INDEX

記号

* （アスタリスク）
  - ポート セキュリティ ワイルドカード 45-11
  - 最初の動作ポート 36-16
  - 自動学習済みエントリ 45-15

1 ギガビット速度
  - 設定 5-6

A

AAA
  - DHCHAP 認証 44-9
  - MSCHAP 認証のイネーブル化 16-9
  - TACACS+ サーバ グループ 17-15, 18-8, 18-15
  - TACACS+ サーバのモニタリング 18-3
  - アカウンティング 16-2
  - 許可 16-2
  - 認証 16-2
  - 制約事項 16-6
  - 設定 16-6, 16-12
  - 設定の確認 16-13
  - 設定プロセス 16-7
  - 設定例 16-13
  - 説明 16-1
  - 前提条件 16-5
  - 注意事項 16-6
  - デフォルト設定 16-13
  - フィールドの説明 16-1
  - ユーザ ログイン プロセス 16-4
  - 利点 16-2

AAA アカウンティング
  - 規則を削除する方法 16-1
  - 規則を整理する方法 16-1
  - 規則を追加する方法 16-1
  - 規則を変更する方法 16-1
  - デフォルトの方式の設定 16-10

AAA アカウンティング ログ
  - 消去 16-12
  - 表示 16-12

AAA サーバ
  - SNMPv3 パラメータの指定 16-11, 16-12
  - VSA 内でのユーザ ロールの指定 16-11
  - ユーザ ロールの指定 16-12

AAA サーバ グループ
  - 説明 16-3

AAA サービス
  - セキュリティ 16-1
  - 設定オプション 16-3
  - リモート 16-2

AAA 認証規則
  - 削除する方法 16-1
  - 整理する方法 16-1
  - 追加する方法 16-1
  - 変更する方法 16-1

AAA プロトコル
  - RADIUS 16-1
  - TACACS+ 16-1

AAA ログイン
  - 認証失敗メッセージのイネーブル化 16-8

AAA ログイン認証
  - コンソール方式の設定 16-7
  - デフォルトの方式の設定 16-8

auto ポート モード
  - 説明 32-4

auto モード
設定 32-10

B

BB_credit
情報の表示 32-17
設定 32-13
説明 32-6
理由コード 32-7
BPDU ガード
「STP BPDU ガード」を参照 10-3
Brocade
ネイティブ interop モード 43-9
Buffer-to-Buffer credit.「BB_credit」を参照 32-7
Build Fabric フレーム 33-3
説明 33-3

C

Call Home
説明 26-1, 27-1
メッセージ フォーマット オプション 26-2
call home
smart call home の機能 26-5
Call Home 宛先プロファイル
属性 26-10
call home 通知
syslog の XML 形式 26-21
syslog のフルテキスト形式 26-20
Call Home メッセージ
フォーマット オプション 26-2
レベルの設定 26-5
CDP
設定 5-7
CFS
NTP 用の設定 3-18
cisco-av-pair
AAA ユーザ パラメータの指定 16-11, 16-12
CIST リージョナル ルート
「MSTP」を参照 9-5
CIST ルート
「MSTP」を参照 9-6

D

DHCHAP
「FC-SP」も参照 44-1
AAA 認証 44-9
AAA 認証の設定 44-9
イネーブル化 44-3, 44-4
グループ設定 44-6
セキュリティ情報の表示 44-9
設定 44-3
設定例 44-9
説明 44-2
タイムアウト値 44-8
他の NX-OS 機能との互換性 44-3
デフォルト設定 44-11
認証モード 44-4
ハッシュ アルゴリズム 44-5
ローカル スイッチのパスワード 44-6
Diffie-Hellman Challenge Handshake Authentication Protocol.「DHCHAP」を参照 44-1
Domain Manager
分離 32-7

E

EFMD
ファブリック バインディング 46-1
ファブリック バインディングの開始 46-3
統計情報の表示 46-7
EISL
ポート チャネル リンク 36-1
Ethanalyzer 50-3

Exchange Fabric Membership Data.「EFMD」を参照 46-1
Exchange Link Parameter.「ELP」を参照 32-7
E ポート
FCS サポート 47-1
FSPF トポロジ 40-1
設定 32-10
トランキングの設定 35-4
ファブリック バインディング検査 46-2
分離 32-7
リンク分離からの回復 38-14
E ポート モード
サービス クラス 32-3
説明 32-3

F

Fabric-Device 管理インターフェイス .「FDMI」を参照 41-4
Fabric Configuration Server.「FCS」を参照 47-1
Fabric Shortest Path First.「FSPF」を参照 40-1
FC-SP
「DHCHAP」も参照 44-1
ISL 上でのイネーブル化 44-9
イネーブル化 44-4
認証 44-1
fcdomain
CFS 配信の設定 33-10, 33-13
イネーブル化 33-5
オーバーラップ分離 32-7
開始 33-5
再起動 33-3
自動再構成のイネーブル化 33-6
情報の表示 33-18, 33-19
スイッチ プライオリティ 33-4
説明 33-1
着信 RCF 33-5
ディセーブル化 33-5
デフォルト設定 33-20
統計情報の表示 33-20
ドメイン ID 33-7
ドメイン マネージャの高速再起動 33-3
マージされたファブリックの自動再構成 33-6
FC ID
FC エイリアス メンバの設定 38-10
HBA への割り当て 43-6
永続的 33-14
説明 33-14
デフォルトの企業 ID リストの割り当て 43-7
割り当て 33-1, 43-6
fcping
スイッチ接続の確認 50-6
デフォルト設定 50-16
呼び出し 50-6
FCS
情報の表示 47-3
説明 47-1
デバイス マネージャを使用したファブリック ポートの表示 47-4
デバイス マネージャを使用したプラットフォームの作成 47-4
デフォルト設定 47-4
特性 47-2
名前の設定 47-2
fctimer
設定された値の表示 43-4
配布 43-3
fctrace
デフォルト設定 50-16
呼び出し 50-5
FC エイリアス
作成 38-10
ゾーンに対する設定 38-10
名前の変更 38-16
複製 38-16
使用 39-8
FDMI
説明 41-4

データベース情報の表示 41-4
Fibre Channel Security Protocol.「FC-SP」を参照 44-1
FLOGI
詳細の表示 41-1
説明 41-1
FSCN
データベースの表示 42-3
FSPF
hello タイム インターバルの設定 40-6
Link State Record のデフォルト 40-3
VSAN カウンタのクリア 40-5
VSAN での設定 40-4
イネーブル化 40-5
インターフェイスでの設定 40-5
インターフェイスでのディセーブル化 40-8
カウンタのクリア 40-9
グローバル情報の表示 40-16
グローバル設定 40-3
再コンバージェンス タイム 40-2
再送信インターバル 40-7
順序どおりの配信 40-10
冗長リンク 40-2
設定のリセット 40-4
説明 40-1
相互運用性 43-11
データベース情報の表示 40-16
ディセーブル化 40-5
デッド タイム インターバル 40-6
デフォルト設定 40-16
デフォルトへのリセット 40-4
トポロジ例 40-2
フォールトトレラント ファブリック 40-2
リンク コストの計算 40-6
リンク コストの設定 40-6
ルーティング サービス 40-1
ルーティング プロトコルのディセーブル化 40-5
FSPF ルート
設定 40-9
説明 40-9
fWWN
FC エイリアス メンバの設定 38-10
Fx ポート
VSAN メンバーシップ 37-4
F ポート
「Fx ポート」も参照 32-3
設定 32-10
説明 32-3
F ポート モード
サービス クラス 32-4
説明 32-3

G

GOLD 診断
拡張モジュール 24-3
設定 24-3
ヘルス モニタリング 24-2
ランタイム 24-2

H

HBA
FC ID の割り当て 43-6
HBA ポート
エリア FCID の設定 33-16
hello タイム
MSTP 9-21
hello タイム インターバル
FSPF の設定 40-6
説明 40-6

I

ID
シスコのベンダー ID 16-12, 17-3
シリアル ID 26-18

IEEE 802.1w
「RSTP」を参照 9-2
interop モード
説明 43-9
デフォルト設定 43-16
モード 1 の設定 43-10
IOD.「順序どおりの配信」を参照 40-10
ISL
ポート チャネル リンク 36-1

L

LACP 11-2, 11-11
システム ID 11-6
LACP の設定 11-11
Link Aggregation Control Protocol 11-2
LUN
検出された SCSI ターゲットの表示 42-3

M

MAC アドレス
セカンダリの設定 43-6
MAC アドレス リダクション 8-3
McData
ネイティブ interop モード 43-9
mgmt0 インターフェイス
設定 3-21
説明 3-21
Microsoft チャレンジ ハンドシェイク認証プロトコル .「MSCHAP」を参照 16-9
MSCHAP
認証のイネーブル化 16-9
MST
CIST リージョナル ルート 9-5
デフォルト値に設定 9-14
MSTP
CIST、説明 9-4
CIST リージョナル ルート 9-5
CIST ルート 9-6
CST
定義 9-4
リージョン間の動作 9-5
IEEE 802.1s
用語 9-6
IST
定義 9-4
マスター 9-5
リージョン内の動作 9-5
MST リージョン
CIST 9-4
IST 9-4
サポートされるスパニングツリー インスタンス 9-2
設定 9-13
説明 9-2
ホップ カウント メカニズム 9-7
VLAN と MST インスタンスのマッピング 9-14
境界ポート
説明 9-7
設定
hello タイム 9-21
MST リージョン 9-13
最大エージング タイム 9-22
最大ホップ カウント 9-22
スイッチ プライオリティ 9-20
セカンダリ ルート スイッチ 9-18
転送遅延時間 9-21
ポート プライオリティ 9-18, 9-19
ルート スイッチ 9-16
モードのイネーブル化 9-13

N

NPIV
イネーブル化 32-15
説明 32-14
NPV、設定 34-6

NPV の設定 34-6
NP ポート 34-1
NP リンク 34-3
NTP
CFS 配信の設定 3-18
設定 3-16
設定時の注意事項 3-17
N ポート
「Nx ポート」も参照 38-2
FCS サポート 47-1
fctrace 50-5
ゾーンの適用 38-12
ゾーン メンバーシップ 38-2
ハード ゾーン分割 38-12
N ポート ID 仮想化 .「NPIV」を参照 32-14

P

PLOGI
ネーム サーバ 41-3
PortChannel
show tech-support port-channel コマンド 50-14
デフォルト設定 36-17
設定の確認 36-16, 36-17
PortChannel プロトコル
自動作成グループの手動設定への変換 36-15
PortFast BPDU フィルタリング
「STP PortFast BPDU フィルタリング」を参照 10-3
Port World Wide Name。「pWWN」を参照 38-2
pWWN
FC エイリアス メンバの設定 38-10
重複の拒否 41-3
ゾーン メンバーシップ 38-2

R

RADIUS
VSA 17-3
グローバルな事前共有キーの設定 17-6
サーバの設定 17-4, 17-13
設定の確認 17-14
設定例 17-15
説明 17-1, 17-4
前提条件 17-4
送信の再試行回数の設定 17-9
タイムアウト間隔の設定 17-9
デフォルト設定 17-15
動作 17-2
ネットワーク環境 17-1
ログイン時にサーバを指定 17-9
RADIUS サーバ
アカウンティング属性の設定 17-11
事前共有キーの設定 17-7
手動モニタリング 17-13
設定の確認 17-14
設定例 17-15
送信の再試行回数の設定 17-10
タイムアウト間隔の設定 17-10
定期的モニタリングの設定 17-12
デッドタイム間隔の設定 17-13
統計情報の表示 17-14
認証属性の設定 17-11
ホストの削除 17-13
ホストの設定 17-5
モニタリング 17-2
RADIUS サーバ グループ
設定 17-8
RBAC
デフォルト設定 22-10
RCF
説明 33-3
着信 33-5
着信の拒否 33-6

Reconfigure Fabric フレーム .「RCF」を参照 33-3
Registered State Change Notification.「RSCN」を参照 41-1
RSCN
情報の表示 41-5
説明 41-4
デフォルト設定 41-11
統計情報のクリア 41-6
ドメイン フォーマット SW-RSCN の抑制 41-6
複数ポート ID 41-5
RSCN タイマー
CFS を使用した設定の配布 41-8
設定 41-7
設定の表示 41-7
RSTP
「MSTP」も参照 9-2
BPDU
処理 8-14
アクティブ トポロジ 8-10
高速コンバージェンス 8-7
ポイントツーポイント リンク 8-7
ルート ポート 8-7
指定スイッチ、定義 8-10
指定ポート、定義 8-10
提案合意ハンドシェイク プロセス 8-7
ルート ポート、定義 8-10

S

SCSI
LUN 検出結果の表示 42-3
SCSI LUN
カスタマイズ検出 42-2
検出の開始 42-1
情報の表示 42-2
ターゲットの検出 42-1
SD ポート
設定 32-10
SD ポート モード
インターフェイス モード 32-4
説明 32-4
SFP
トランスミッタ タイプ 32-15
トランスミッタ タイプの表示 32-17
Small Computer System Interface。「SCSI」を参照 42-1
smart call home
Transport Gateway（TG）集約ポイント 26-6
説明 26-5
登録要件 26-6
SMARTnet
smart call home の登録 26-6
SNMP
CLI でのユーザの同期 27-4
LinkUp/LinkDown 通知の設定 27-10, 27-11
アクセス グループ 27-5
グループベースのアクセス 27-4
サーバ担当者名 26-7
バージョン 3 セキュリティ機能 27-2
場所の割り当て 27-11
連絡先の割り当て 27-11
SNMP（シンプル ネットワーク管理プロトコル）
バージョン
セキュリティ モデルとセキュリティ レベル 27-2
SNMPv3
AAA サーバのパラメータの指定 16-12
AAA パラメータの指定 16-11
セキュリティ機能 27-2
複数のロールの割り当て 27-6
SPAN
出力送信元 49-1
モニタリングの送信元 49-1
SPAN 宛先ポート モード .「SD ポート モード」を参照 32-4
SPAN 送信元
出力 49-1
入力 49-1

SPF
計算ホールド タイム 40-3
SSH
サーバ キー ペアの生成 19-1
STP
PortFast 8-7, 10-2
エッジ ポート 8-7, 10-2
概要
ラーニング ステート 8-12
ディセーブル ステート 8-13
フォワーディング ステート 8-12
ブロッキング ステート 8-12
ルート ブリッジ選択 8-5
ネットワーク ポート 10-2
標準ポート 10-2
ポート タイプ 10-2
ポート チャネル 11-1
STP ブリッジ ID 8-3
STP ルート ガード 10-5
sWWN
ファブリック バインディングの設定 46-4

T

TACACS+
RADIUS と比較しての利点 18-1
イネーブル化 18-5
グローバルな事前共有キー 18-3
グローバルな事前共有キーの設定 18-6
グローバルなタイムアウト間隔の設定 18-10
事前共有キー 18-3
制約事項 18-4
設定 18-4, 18-14
設定の確認 18-14
設定例 18-15
説明 18-1
前提条件 18-3
ディセーブル化 18-14
統計情報の表示 18-14
フィールドの説明 18-15
ユーザ ログイン時の動作 18-2
ログイン時に TACACS+ サーバを指定 18-9
TACACS+ サーバ
TCP ポートの設定 18-11
サーバ グループの設定 18-8, 18-15, 17-15
事前共有キーの設定 18-7
手動でのモニタリング 18-13
設定の確認 18-14
設定プロセス 18-4
タイムアウト間隔の設定 18-10
定期的モニタリングの設定 18-11
デッドタイム間隔の設定 18-13
統計情報の表示 18-14
フィールドの説明 18-15
ホストの設定 18-5, 18-14
モニタリング 18-3
TCP ポート
TACACS+ サーバ 18-11
TE ポート
FCS サポート 47-1, 47-2
fctrace 50-5
FSPF トポロジ 40-1
相互運用性 43-11
トランキングの制限事項 35-1
ファブリック バインディング検査 46-2
リンク分離からの回復 38-14
TE ポート モード
サービス クラス 32-4
説明 32-4
TOV
VSAN に対する設定 43-2
すべての VSAN の設定 43-1
相互運用性 43-10
デフォルト設定 43-16
範囲 43-1

U

UDLD
アグレッシブ モード 5-3
設定 5-5
定義 5-2
非アグレッシブ モード 5-3

V

VLAN
VTP ドメイン 6-3
拡張範囲 6-2
予約範囲 6-2
VSA
形式 16-12
サポートの説明 16-11
プロトコル オプション 16-12, 17-4
VSAN
allowed-active リストの設定 35-6
DHCHAP との互換性 44-3
FC ID 37-1
FCS サポート 47-1
FSPF 40-4
FSPF 接続 40-1
FSPF の設定 40-3
interop モード 43-10
TE ポート モード 32-4
TOV 43-2
機能 37-1
キャッシュ内容 33-19
許可アクティブ 35-1
削除 37-9
使用状況の表示 37-11
ステート 37-5
設定 37-6
設定の表示 37-11
説明 37-1
ゾーンとの比較（表） 37-4
タイマー設定 43-2
デフォルト VSAN 37-8
デフォルト設定 37-12
動作ステート 37-9
独立 37-8
ドメイン ID 自動再構成 33-6
トラフィックの分離 37-3
トランキング ポート 37-7
トランク許可 35-1
トランク許可リストの設定 35-4, 35-6
名前 37-5
ネーム サーバ 41-2
不一致 32-7
複数のゾーン 38-5
フロー統計情報 40-14
ポート トラッキング 48-5
ポート メンバーシップ 37-6
メンバーシップの表示 37-7
利点 37-3
ロード バランシング 37-10
ロード バランシング属性 37-6
VSAN ID
VSAN メンバーシップ 37-4
許可リスト 35-7
説明 37-5
トラフィックの多重化 32-4
範囲 37-4
VTP
ドメイン
VLAN 6-3

W

World Wide Name.「WWN」を参照 43-5
WWN
情報の表示 43-5
セカンダリ MAC アドレス 43-6
設定 43-5
中断された接続 32-7

ポート セキュリティ 45-11
リンク初期化 43-6

あ

アカウンティング
説明 16-2
アクティブ ゾーン セット
考慮事項 38-4
配信のイネーブル化 38-13
宛先 ID
エクスチェンジ ベース 36-3
順序どおりの配信 40-10
パス選択 37-10
フロー ベース 36-3
アドレス割り当てキャッシュ
説明 33-19

い

一意のエリア FC ID
設定 33-16
説明 33-16
インターフェイス
1 ギガビット速度
設定 5-6
CDP
設定 5-7
FC エイリアス メンバの設定 38-10
SFP 情報の表示 32-17
SFP タイプ 32-15
UDLD
設定 5-5
定義 5-2
VSAN への割り当て 37-7
VSAN メンバーシップ 37-6
受信データ フィールド サイズの設定 32-12
情報の表示 32-16
説明の設定 32-10
デバウンス タイマー
設定 5-7
ポート チャネルからの削除 36-11
ポート チャネルへの強制追加 36-10
ポート チャネルへの追加 36-9, 36-10
隔離状態 36-10
中断状態 36-10
インターフェイス速度 5-4
インターフェイスの統計情報
説明 32-16

え

エージング タイム
アクセラレーション
MSTP の 9-21
最大
MSTP 9-22
永続的 FC ID
イネーブル化 33-15
設定 33-15
説明 33-14
表示 33-19

か

拡張ゾーン
イネーブル化 38-20
基本ゾーンからの変更 38-19
基本ゾーンと比較しての利点 38-18
情報の表示 38-24
スイッチ全体のデフォルト ゾーン ポリシーの設定 38-23
説明 38-18
データベースの変更 38-20
データベースのマージ 38-21
デフォルト設定 38-25
デフォルトのフル データベース配信の設定 38-23

デフォルト ポリシーの設定 38-23
拡張範囲 VLAN
「VLAN」を参照 6-2
拡張ポート モード .「E ポート モード」を参照 32-3
仮想ファイバ チャネル インターフェイス
デフォルト設定 32-18
間接リンク障害
回復 48-1
管理インターフェイス
シャットダウン時の force オプションの使用 3-22
情報の表示 3-22
管理インターフェイス .「mgmt0 インターフェイス」を参照 3-21
管理者
デフォルト パスワード 3-10
管理ステート
設定 32-9
説明 32-5
管理速度
設定 32-10
管理操作
説明 3-13

き

企業 ID
FC ID の割り当て 43-7
許可
説明 16-2
ユーザ ログイン 16-4

こ

交換 ID
順序どおりの配信 40-10
パス選択 37-10
ロード バランシング 50-5
高速スパニングツリー プロトコル
「RSTP」を参照 9-2
コミュニティ VLAN 7-2, 7-3
コミュニティ ポート 7-3
コンソール
AAA ログイン認証方式の設定 16-7

さ

サーバ ID
説明 26-18
サーバ グループ .「AAA サーバ グループ」を参照 16-3
再送信インターバル
FSPF の設定 40-7
説明 40-7
最大エージング タイム
MSTP 9-22
最大ホップ カウント、MSTP 9-22
サマータイム
調整 3-15

し

シスコ
ベンダー ID 16-12, 17-3
事前共有キー
TACACS+ 18-3
主要スイッチ
設定 33-9
ドメイン ID の割り当て 33-9
順序どおりの配信
VSAN に対するイネーブル化 40-13
グローバルなイネーブル化 40-12
ステータスの表示 40-13
注意事項 40-12
ドロップ遅延時間の設定 40-14
ネットワーク フレームの順番再設定 40-11
ポート チャネル フレームの順番再設定 40-11
冗長性
VSAN 37-4

冗長物理リンク
例（図） 40-2
シリアル ID
説明 26-18
診断
拡張モジュール 24-3
設定 24-3
デフォルト設定 24-4
ヘルス モニタリング 24-2
ランタイム 24-2

す

スイッチド ポート アナライザ .「SPAN」を参照 49-1
スイッチ プライオリティ
MSTP 9-20
設定 33-4
説明 33-4
デフォルト 33-4
スイッチ ポート
属性のデフォルト値の設定 32-14
スケーラビリティ
VSAN 37-4
スタティック ルート
ランタイム チェック 40-9
ストレージ デバイス
アクセス制御 38-1

せ

セカンダリ MAC アドレス
設定 43-6
セカンダリ VLAN 7-2
セッションの実行 23-3
セッション マネージャ 23-3
ACL セッションの設定（例） 23-3
ACL の設定 23-2
制限事項 23-1
セッションの確認 23-3
セッションのコミット 23-3
セッションの作成 23-2
セッションの廃棄 23-3
セッションの保存 23-3
設定の確認 23-4
説明 23-1
注意事項 23-1

そ

ゾーン
「拡張ゾーン」も参照 38-18
「ゾーン分割」も参照 38-2
「デフォルト ゾーン」も参照 38-9
「ハード ゾーン分割」も参照 38-12
FC エイリアスの設定 38-10
pWWN を使用したメンバーシップ 37-4
show tech-support zone コマンド 50-12
VSAN との比較（表） 37-4
アクセス制御 38-8
エイリアスの設定 38-10
拡張ゾーンからの変更 38-20
機能 38-1, 38-4
情報の表示 38-17, 38-18
制限の適用 38-12
ゾーン メンバの追加 38-8
ダウングレードのための圧縮 38-24
データベースのインポート 38-14
データベースのエクスポート 38-14
デバイス エイリアスとの比較（表） 39-2
デフォルト設定 38-25
デフォルト ポリシー 38-3
名前の変更 38-16
バックアップ（手順） 38-16
復元（手順） 38-16
複製 38-16
フル ゾーン データベースの編集 38-8
分析 38-24

マージ障害 32-7
ゾーン エイリアス
インポート 39-8
デバイス エイリアスへの変換 39-8
ゾーン サーバ データベース
クリア 38-17
ゾーン セット 38-1, 38-2
「アクティブ ゾーン セット」も参照 38-8, 38-5
「ゾーン」も参照 38-2
アクティブ化 38-8
インポート 38-15
エクスポート 38-15
機能 38-1
考慮事項 38-4
コピー 38-15
作成 38-8
情報の表示 38-17, 38-18
設定 38-8
設定の配信 38-12
データベースのインポート 38-14
データベースのエクスポート 38-14
デフォルト設定 38-25
名前の変更 38-16
配信のイネーブル化 38-13
複製 38-16
分析 38-24
リンク分離からの回復 38-14
ワンタイム配信 38-13
ゾーン属性グループ
複製 38-16
ゾーン データベース
MDS 以外のデータベースの移行 38-17
ロックの解除 38-21
ゾーン分割 38-2
実装 38-4
説明 38-1
例 38-3
ゾーン メンバ
情報の表示 38-9
ゾーンへの追加 38-8
ゾーン分割
「ゾーン」も参照 38-1
相互運用性
interop モード 1 の設定 43-10
VSAN 37-11
ステータスの確認 43-12
説明 43-9
送信元 ID
call home イベント フォーマット 26-18
エクスチェンジ ベース 36-3
順序どおりの配信 40-10
パス選択 37-10
フロー ベース 36-3
速度自動検知 32-11
ソフト ゾーン分割 38-12
「ゾーン分割」も参照 38-12
説明 38-12

た

タイムアウト値 .「TOV」を参照 43-2
単方向リンク検出 .「UDLD」を参照。 5-2

て

デッド タイム インターバル
FSPF の設定 40-7
説明 40-6
デバイス ID
call home フォーマット 26-18
デバイス エイリアス
ゾーン エイリアスの変換 39-8
ゾーン セット情報の表示 39-9
ゾーンとの比較（表） 39-2
データベースの変更 39-2
デフォルト設定 39-10
レガシー ゾーン エイリアスのインポート 39-8

拡張モード 39-4
作成 39-3
作成（手順） 39-6
使用 39-8
情報の表示 39-9
説明 39-1
特徴 39-1
要件 39-2
デバイス エイリアス データベース
ファブリックのロック 39-6
ファブリックへの配布 39-5
ファブリック ロックの上書き 39-7
マージ 39-9
配布のイネーブル化 39-7
配布のディセーブル化 39-7
変更のコミット 39-6
変更の廃棄 39-6
デバウンス タイマー 5-4
設定 5-7
デフォルト VSAN
説明 37-8
デフォルト設定
AAA 16-13
RBAC 22-10
ロールバック 23-4
デフォルト ゾーン
アクセス権限の設定 38-9
設定 38-9
説明 38-9
相互運用性 43-10
ポリシー 38-9
ポリシーの設定 38-8
デフォルトのユーザ
説明 3-9
電子メール通知
Call Home 26-1
転送遅延時間
MSTP 9-21

と

統計情報
TACACS+ 18-14
動作ステート
説明 32-5
ファイバ チャネル インターフェイスでの設定 32-10
独立 VLAN 7-2, 7-3
独立 VSAN
説明 37-8
メンバーシップの表示 37-9
独立ポート 7-3
ドメイン ID
CFS 配信の設定 33-10, 33-13
FC エイリアス メンバの設定 38-10
許可リスト 33-9
許可リストの設定 33-10
スタティック 33-9
説明 33-7
相互運用性 43-10
配信 33-1
優先 33-9
連続割り当て 33-13
連続割り当てのイネーブル化 33-13
割り当て障害 32-7
ドメイン マネージャ
高速再起動機能 33-3
トラッキング対象ポート
動作バインディング 48-3
トラップ通知 27-2
トラフィックの分離
VSAN 37-4
トラブルシューティング
fcping 50-6
fctrace 50-5
show tech-support コマンド 50-8
スイッチ接続の確認 50-6
テクニカル サポートの出力の収集 50-8

トランキング
情報の表示 35-6
制限事項 35-1
設定に関する考慮事項 35-1
説明 35-1
相互運用性 43-10
デフォルト設定 35-7
トラフィックのマージ 35-2
ポート チャネルとの比較 36-2
モードの設定 35-3
リンク ステート 35-4
トランキング E ポート モード .「TE ポート モード」を参照 32-4
トランキング プロトコル
説明 35-2
デフォルト ステート 35-2
デフォルト設定 35-7
ポート分離の検出 35-2
トランキング ポート
VSAN との対応 37-7
トランク許可 VSAN リスト
説明 35-4
トランク ポート
情報の表示 35-7
トランク モード
管理者用のデフォルト 32-14
設定 35-3, 35-4
デフォルト設定 35-7
ドロップ遅延時間
順序どおりの配信での FSPF の設定 40-14
情報の表示 40-14
設定 40-14

な

永続的 FC ID
消去 33-18
夏時間
調整 3-15

に

認証
説明 16-2
ファブリック セキュリティ 44-1
方式 16-3
ユーザ ログイン 16-4
リモート 16-2
ローカル 16-2
認証、許可、アカウンティング。「AAA」を参照 16-1

ね

ネーム サーバ
LUN 情報 42-1
重複 pWWN の拒否 41-3
相互運用性 43-11
データベース エントリの表示 41-3
プロキシ機能 41-2
プロキシ登録 41-2
ネットワーク タイム プロトコル .「NTP」を参照。 3-16

は

ハード ゾーン分割
説明 38-12
パスワード
DHCHAP 44-6
管理者 3-9
管理者用のデフォルト 3-10
管理者用のデフォルトの設定 3-10
強力な特性 22-2

ひ

ビット エラー
　理由　32-12
ビット エラーしきい値
　設定　32-12
　説明　32-12

ふ

ファイバ チャネル
　TOV　43-2
　タイムアウト値　43-1
　ファブリック バインディング用の sWWN　46-4
ファイバ チャネル インターフェイス
　「インターフェイス」も参照　32-4
　auto ポート モードの設定　32-10
　BB_credit　32-6
　VSAN メンバーシップの表示　37-8
　イネーブル化　32-9
　管理ステート　32-5
　情報の表示　32-16
　ステート　32-4
　設定　32-8
　説明の設定　32-10
　速度の設定　32-10
　ディセーブル化　32-9
　デフォルト設定　32-18
　動作ステート　32-5
　ビット エラーしきい値の設定　32-12
　フレームのカプセル化の設定　32-11
　ポート チャネルからの削除　36-11
　ポート モードの設定　32-10
　理由コード　32-5
ファイバ チャネル ドメイン .「fcdomain」を参照　33-1
ファブリック
　「Build Fabric フレーム」も参照　33-3
ファブリック .「RCF」を参照　33-3
ファブリック pWWN
　ゾーン メンバーシップ　38-2
ファブリック WWN。「fWWN」を参照　38-10
ファブリック セキュリティ
　デフォルト設定　44-11
　認証　44-1
ファブリックの再設定
　fcdomain のフェーズ　33-1
ファブリック バインディング
　DHCHAP との互換性　44-3
　EFMD　46-1
　EFMD 統計情報の表示（手順）　46-6
　E ポートの検査　46-2
　sWWN リスト　46-4
　TE ポートの検査　46-2
　アクティブ データベースの表示（手順）　46-6
　アクティブ化　46-5
　イネーブル化　46-3
　コンフィギュレーション データベースからの削除（手順）　46-6
　コンフィギュレーション データベースの作成（手順）　46-6
　コンフィギュレーション データベースへのコピー　46-5
　コンフィギュレーション データベースへの保存　46-5
　コンフィギュレーション ファイルへのコピー（手順）　46-6
　ステータスの確認　46-4
　データベースの削除　46-6
　ディセーブル化　46-4
　デフォルト設定　46-7
　ポート セキュリティとの比較　46-1
　ライセンスの要件　46-1
　違反の表示（手順）　46-6
　開始プロセス　46-3
　強制的なアクティブ化　46-5
　強制的な非アクティブ化　46-6
　実行　46-2
　説明　46-1

統計情報のクリア 46-6
ファブリック ポート モード .「F ポート モード」を参照 32-3
ファブリック ログイン .「FLOGI」を参照 41-1
フィールドの説明
AAA 16-1
TACACS+ 18-15
フォールトトレラント ファブリック
例（図） 40-2
プライベート VLAN
エンド ステーション アクセス 7-5
隔離 VLAN 7-2, 7-3
コミュニティ VLAN 7-2, 7-3
セカンダリ VLAN 7-2
プライマリ VLAN 7-2
ポート
コミュニティ 7-3
独立 7-3
無差別 7-3
プライマリ VLAN 7-2
ブリッジ ID
「STP ブリッジ ID」を参照 8-3
フル ゾーン セット 38-5
考慮事項 38-4
配信のイネーブル化 38-13
フレームのカプセル化
設定 32-11
フロー統計情報
カウント 40-15
クリア 40-15
説明 40-14
表示 40-15
ブロードキャスト ストーム
「トラフィック ストーム制御」を参照 15-1
プロキシ
ネーム サーバの登録 41-2
ブロッキング ステート、STP 8-12

へ

ヘルス モニタリング診断
情報 24-2
ベンダー固有属性 .「VSA」を参照 16-11

ほ

ポート
VSAN メンバーシップ 37-6
ポート セキュリティ
CFS 配信の設定 45-12
DHCHAP との互換性 44-3
WWN の識別 45-11
アクティブ化 45-6
アクティベーション 45-3
アクティベーションの拒否 45-6
アクティベーションの強制 45-7
イネーブル化 45-5
データベースからのエントリの削除（手順） 45-12
ディセーブル化 45-5
デフォルト設定 45-21
ファブリック バインディングとの比較 46-1
ライセンス要件 45-2
違反の表示（手順） 45-8
許可済みのペアの追加 45-12
自動学習 45-2
自動学習せずに手動設定 45-10
実行メカニズム 45-2
設定の表示 45-20
設定の表示（手順） 45-8
設定時の注意事項 45-3
統計情報の表示（手順） 45-8
非アクティブ化 45-6
不正アクセスの防止 45-1
ポート セキュリティ データベース
コピー 45-18

コンフィギュレーション データベースへのアクティブ データベースのコピー（手順） 45-8
シナリオ 45-16
マージに関する注意事項 45-15
再アクティブ化 45-7
削除 45-19
手動設定時の注意事項 45-5
消去 45-19
設定の表示 45-20
相互作用 45-16
ポート セキュリティ自動学習
CFS を使用しない設定の注意事項 45-4
CFS 使用時の設定の注意事項 45-3
イネーブル化 45-8
ディセーブル化 45-9
デバイスの許可 45-9
許可の例 45-9
設定の配信 45-14
説明 45-2
ポート速度
設定 32-10
ポート チャネリング 11-2
ポート チャネル
DHCHAP との互換性 44-3
STP 11-1
インターフェイスの強制追加 36-10
インターフェイスの削除 36-11
インターフェイスの追加 36-9, 36-10
インターフェイス状態 36-10
管理上のダウン 32-7
順序保証 40-12
相互運用性 43-11
トランキングとの比較 36-2
ファイバ チャネル ルートの設定 40-9
リンク障害 40-2
リンクの変更 40-12
ロード バランシング 36-2
互換性チェック 36-9
誤設定エラー検出 36-6
削除 36-8
設定 36-8
設定時の注意事項 36-6
説明 36-1
ポート チャネル プロトコル
チャネル グループの作成 36-12
自動作成 36-13
自動作成のイネーブル化 36-15
自動作成の設定 36-15
説明 36-12
ポート チャネル モード
説明 36-6
ポート トラッキング
VSAN 内のポートのモニタリング 48-5
イネーブル化 48-3
情報の表示 48-7
説明 48-1
注意事項 48-2
デフォルト設定 48-7
複数ポート 48-4
ポートを強制的にシャットダウン 48-6
ポート プライオリティ
MSTP 9-18, 9-19
ポート モード
auto 32-4
ホスト ポート
種類 7-3

ま

マージされたファブリック
自動再構成 33-6
マニュアル
関連資料 1-2
追加資料 1-2
マルチキャスト ストーム
「トラフィック ストーム制御」を参照 15-1

む

無差別ポート 7-3

ゆ

ユーザ
説明 22-1
ユーザ アカウント
パスワードの特性 22-2
ユーザ ロール
AAA サーバでの指定 16-11, 16-12
ユーザ ログイン
AAA ログイン認証方式の設定 16-8
許可プロセス 16-4
認証プロセス 16-4
猶予期間のアラート
ライセンス 4-8
ユニキャスト ストーム
「トラフィック ストーム制御」を参照 15-1

よ

読み取り専用ゾーン
デフォルト設定 38-25
予約範囲 VLAN
「VLAN」を参照 6-2

ら

ライセンス
PAK 4-2
アンインストール 4-6
インストール オプション 4-2
永久 4-2
キー ファイルのインストール 4-4
キー ファイルの取得 4-4
欠落 4-2
権利証明書 4-1
更新 4-8
差分 4-2
手動インストール 4-3
使用中の機能の識別 4-6
情報の表示 4-5
スイッチ間の移動 4-9
ノードロック 4-1
バックアップ 4-6
評価 4-2
プレインストールの入手 4-3
ホスト ID 4-1
猶予期間 4-2
猶予期間のアラート 4-8
猶予期間の終了 4-9
用語 4-1
ライセンス キー ファイル
キー ファイルのインストール 4-5
更新 4-4
説明 4-2
ランタイム診断
情報 24-2
ランタイム チェック
スタティック ルート 40-9

り

理由コード
説明 32-5
リンク コスト
FSPF の設定 40-6
説明 40-6
リンク障害
回復 48-1
単一方向の検出 8-15, 9-8

る

ルート ガード
「STP ルート ガード」を参照 10-5
ルート コスト
計算 40-6
ルート スイッチ
MSTP 9-16

れ

例
AAA の設定 16-13
連続ドメイン ID 割り当て
概要 33-13

ろ

ロード バランシング
VSAN の属性 37-6
設定 37-10
説明 37-10
属性 37-10
ポート チャネル 36-1
保証 37-11
説明 36-2
ロール
認証 22-1
ロールバック
コンフィギュレーション例 23-1
制限事項 23-1
設定の確認 23-4
説明 23-1
チェックポイント コピー 23-1
チェックポイント コピーの作成 23-1
チェックポイント ファイルの削除 23-1
チェックポイント ファイルまでの復元 23-1
注意事項 23-1
デフォルト設定 23-4
ハイ アベイラビリティ 23-1
ロールバックの実装 23-1
論理ユニット番号。「LUN」を参照 42-1

はじめに

ここでは、『*Cisco Nexus 5000 シリーズ CLI 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。また、関連マニュアル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、Cisco Nexus 5000 シリーズ スイッチの設定および保守を担当する、経験豊富なネットワーク管理者を対象としています。

マニュアルの構成

このマニュアルは、次の章で構成されています。

章	タイトル	説明
第 1 章	製品概要	Cisco Nexus 5000 シリーズ スイッチの概要について説明します。
第 1 部	設定の基礎	CLI の使用法およびスイッチの初期設定などについて説明します。
第 2 部	LAN スイッチング	イーサネット インターフェイス、VLAN、STP、ポート チャネル、トランク、MAC アドレス テーブル、IGMP スヌーピングの設定方法などについて説明します。
第 3 部	スイッチ セキュリティ機能	AAA、RADIUS、TACACS+、SSH/Telnet、ACL の設定方法などについて説明します。
第 4 部	システム管理	CFS、RBAC、システム メッセージ ロギング、Call Home、SNMP、RMON、ネットワーク管理インターフェイス、ストーム制御、SPAN の設定方法などについて説明します。
第 5 部	Fibre Channel over Ethernet	FCoE および仮想インターフェイスの設定方法などについて説明します。
第 6 部	QoS	QoS の設定方法に関する章が含まれます。

章	タイトル	説明
第 7 部	SAN スイッチング	ファイバ チャネル インターフェイスおよびファイバ チャネル機能（NPV、SAN ポート チャネル、ゾーン、DDAS、FSPF、セキュリティ機能など）の設定方法などについて説明します。
第 8 部	トラブルシューティング	基本的なトラブルシューティングの実行方法に関する章が含まれます。

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*」を意味します。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

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

関連資料

Cisco Cisco Nexus 5000 シリーズ スイッチのマニュアルは、次の URL で入手できます。

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

関連する Cisco Nexus 5000 シリーズのドキュメンテーションは、次のとおりです。

『Cisco Nexus 5000 Series Release Notes』

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

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

『Cisco Nexus 5000 Series System Messages Reference』

『Cisco Nexus 5000 Series Command Reference, Release 4.0』

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

『Cisco Nexus 5000 Series MIBs Reference, Release 4.0』

マニュアルの入手方法およびテクニカル 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 Really Simple Syndication（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

製品概要

Cisco Nexus 5000 シリーズ は、データセンター用のトップオブラック スイッチ ファミリです。Cisco Nexus 5000 シリーズ では、高速イーサネット スイッチングを実現し、Fibre Channel over Ethernet（FCoE）をサポートしてデータセンターの I/O Consolidation（IOC）を可能にします。

Nexus 5010 スイッチは 20 個の固定イーサネット ポートを備えた 1 ラック ユニット（RU）スイッチ で、Nexus 5020 スイッチは 40 個の固定イーサネット ポートを備えた 2 RU スイッチです。オプションの拡張モジュールは、ネイティブ ファイバ チャネル ポートと追加のイーサネット ポートを備えています。

この章では Cisco Nexus 5000 シリーズ スイッチについて説明します。具体的な内容は次のとおりです。

- Cisco Nexus 5000 シリーズ の新しいテクノロジー（1-1 ページ）
- Cisco Nexus 5000 シリーズ スイッチ ハードウェア（1-3 ページ）
- Cisco Nexus 5000 シリーズ スイッチ ソフトウェア（1-5 ページ）
- 一般的な配置トポロジ（1-8 ページ）
- サポートされる規格（1-11 ページ）

Cisco Nexus 5000 シリーズ の新しいテクノロジー

Cisco Nexus 5000 シリーズ スイッチでは新しいテクノロジーが導入されました。ここではその新しいテクノロジーについて説明します。

- Fibre Channel over Ethernet（1-1 ページ）
- IOC（1-2 ページ）
- 仮想インターフェイス（1-3 ページ）

Fibre Channel over Ethernet

FCoE は、物理イーサネット リンク上でファイバ チャネル トラフィックをカプセル化する方法を提供します。FCoE フレームでは固有のイーサタイプが使用されるので、FCoE トラフィックおよび標準イーサネット トラフィックを同一リンクで伝送できます。

ファイバ チャネル トラフィックには、ロスレス トランスポート層が必要です。ネイティブ ファイバ チャネルでは、バッファ間クレジット システムを用いてロスレス サービスが実装されます。FCoE トラフィックの場合、イーサネット リンクでロスレス サービスを提供する必要があります。

Cisco Nexus 5000 シリーズ スイッチのイーサネット リンクは、リンク レベル フロー制御とプライオリティ フロー制御という 2 つのメカニズムを提供し、FCoE トラフィックのロスレス トランスポートを可能にします。

IEEE 802.3x リンクレベル フロー制御により、輻輳したレシーバは遠端に信号を発信し、データ送信を短時間一時停止させます。この一時停止機能はリンク上のすべてのトラフィックに適用されます。

プライオリティ フロー制御（PFC）機能は、イーサネット リンク上の特定のトラフィック クラスにポーズ機能を適用します。たとえば、PFC は FCoE トラフィックにロスレス サービスを、標準イーサネット トラフィックにベストエフォート サービスを提供します。PFC は、（IEEE 802.1p トラフィック クラスを使用して）特定のイーサネット トラフィック クラスに、さまざまなレベルのサービスを提供することができます。

IOC

I/O Consolidation（IOC）により、IP トラフィック、SAN トラフィック、IPC トラフィックを単一のネットワーク テクノロジーで伝送できるようになります。

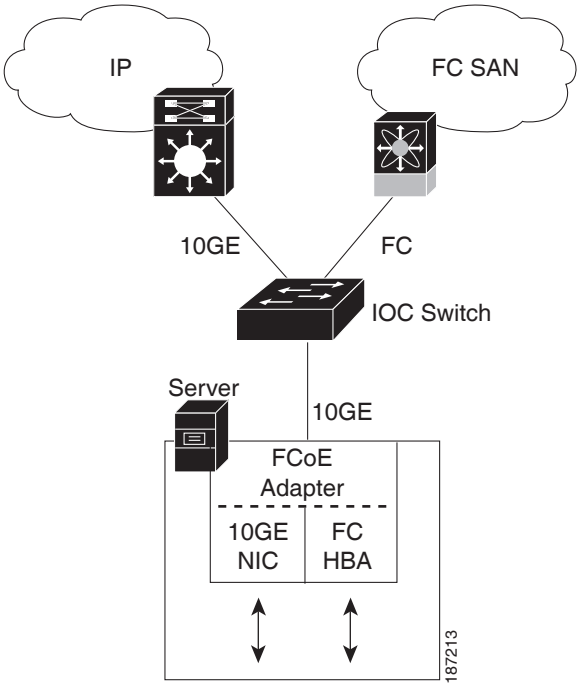
FCoE を使用すると、IOC への漸進的なアプローチが可能になります。上部のファイバ チャネル レイヤは同じであるため、ファイバ チャネル動作モデルが維持されます。FCoE ネットワーク管理と設定は、ネイティブのファイバ チャネル ネットワークと同様です。

Cisco Nexus 5000 シリーズ スイッチでは FCoE が使用され、スイッチとサーバ間の同一物理イーサネット接続でファイバ チャネル トラフィックとイーサネット トラフィックが伝送されます。サーバでは、接続が Converged Network Adapter（CNA）で終端します。このアダプタは、イーサネット NIC インターフェイスおよびファイバ チャネル HBA インターフェイスという 2 つのインターフェイスをサーバのオペレーティング システム（OS）に提示します。サーバの OS は FCoE カプセル化を認識しません（図 1-1 を参照）。

スイッチでは、着信イーサネット ポートがイーサネット トラフィックおよびファイバ チャネル トラフィックを分離します（イーサタイプを使用してフレームを区別）。イーサネット フレームおよびファイバ チャネル フレームは、それぞれのネットワーク側インターフェイスにスイッチングされます。

Cisco Nexus 5000 シリーズ スイッチは、スイッチ間でファイバ チャネル トラフィック用にロスレス サービスを確保する Quality of Service（QoS）機能を提供します。すべてのイーサネット トラフィックにベストエフォート サービスを適用したり、特定クラスのイーサネット トラフィックにさまざまな QoS レベルを設定したりできます。

図 1-1　　IOC



仮想インターフェイス

FCoE をイネーブルにすると、物理イーサネット ケーブルは論理ファイバ チャネル接続のトラフィックを伝送します。

Cisco Nexus 5000 シリーズ スイッチでは仮想インターフェイスを使用して、論理ファイバ チャネル接続を行います。仮想ファイバ チャネル インターフェイスは、設定のために物理イーサネット インターフェイスのレイヤ 2 サブインターフェイスとして実装されます。

イーサネット機能（リンク デバウンス タイマーおよび VLAN メンバーシップなど）は、物理イーサネット インターフェイスで設定します。VSAN メンバーシップなどの論理ファイバ チャネル機能は、仮想ファイバ チャネル インターフェイスで設定します。

Cisco Nexus 5000 シリーズ スイッチ ハードウェア

Cisco Nexus 5000 シリーズには Nexus 5010 スイッチと Nexus 5020 スイッチがあります。ここでは、Cisco Nexus 5000 シリーズ スイッチ ハードウェアについて説明します。

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

シャーシ

Nexus 5010 スイッチは 1 RU シャーシで、Nexus 5020 スイッチは2 RU シャーシです。それぞれラックマウント用に設計されています。シャーシでは、冗長ファンおよび電源装置がサポートされます。

Cisco Nexus 5000 シリーズ スイッチング ファブリックは低遅延でノンブロッキングであり、64 ～ 9216 バイトのイーサネット フレーム サイズがサポートされます。

拡張モジュール

オプションの拡張モジュール用のスロットは、Nexus 5010 スイッチには 1 つ、Nexus 5020 スイッチには 2 つあります。次の拡張モジュールを使用できます。

- 4 個の 10 ギガビット イーサネット ポートおよび 4 個の 1/2/4 Gb ファイバ チャネル ポートを備えた N5K-M1404
- 6 個の 10 ギガビット イーサネット ポートを備えた N5K-M1600
- 8 個の 1/2/4 Gb ファイバ チャネル ポートを備えた N5K-M1008

拡張モジュールは現場交換可能ユニット（FRU）であり、活性挿抜（OIR）をサポートします。

イーサネット インターフェイス

Nexus 5010 スイッチでは、20 個の固定 10 ギガビット イーサネット ポートに SFP+ インターフェイス アダプタが装備されています。最初の 8 個のポートは、スイッチ可能な 1 ギガビット/10 ギガビット ポートです。拡張モジュールでは、さらに最大 6 個の 10 ギガビット イーサネット ポートが使用可能です。

Nexus 5020 スイッチでは、40 個の固定 10 ギガビット イーサネット ポートに SFP+ インターフェイス アダプタが装備されています。最初の 16 個のポートは、スイッチ可能な 1 ギガビット/10 ギガビット ポートです。拡張モジュールでは、さらに最大 12 個の 10 ギガビット イーサネット ポートが使用可能です。

すべての 10 ギガビット イーサネット ポートで FCoE がサポートされます。それぞれのポートは、サーバに接続されたダウンリンクとして、またはデータセンター LAN へのアップリンクとして使用できます。

ファイバ チャネル インターフェイス

Cisco Nexus 5000 シリーズ スイッチではファイバ チャネル ポートがオプションになっています。拡張モジュールを使用する場合、使用可能なファイバ チャネル ポートは、Nexus 5010 スイッチで最大 8 個、Nexus 5020 スイッチで最大 16 個です。

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

管理インターフェイス

Cisco Nexus 5000 シリーズ スイッチには 2 個の専用管理インターフェイスがあります（シリアル コンソール ポート 1 個と 10/100/1000 イーサネット インターフェイス 1 個）。

Cisco Nexus 5000 シリーズ スイッチ ソフトウェア

Cisco Nexus 5000 シリーズ スイッチは、Cisco Nexus オペレーティング システム（NX-OS）が実行されるレイヤ 2 デバイスです。ここでは、Cisco Nexus 5000 シリーズ スイッチ ソフトウェアについて説明します。

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

イーサネット スイッチング

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

- IEEE 802.1D-2004 高速スパニングツリー プロトコル（RSTP）およびマルチ スパニングツリー プロトコル（802.1w および 802.1s）
- IEEE 802.1Q VLAN およびトランク
- IEEE 802.3ad リンク アグリゲーション
- プライベート VLAN
- トラフィック抑制（ユニキャスト、マルチキャスト、ブロードキャスト）

FCoE およびファイバ チャネル スイッチング

Cisco Nexus 5000 シリーズ スイッチでは、FCoE インターフェイスをサーバに、ネイティブ ファイバ チャネル インターフェイスを SAN に提供して、データセンターの I/O Consolidation（IOC）をサポートします。

FCoE およびファイバ チャネル スイッチングには次の機能が含まれます。

- シスコ ファブリック サービス
- N ポート バーチャライゼーション
- VSAN および VSAN トランキング
- ゾーニング
- DDAS
- SAN ポート チャネル

ライセンス

Cisco Nexus 5000 シリーズ スイッチはライセンスがインストールされた状態で出荷されます。このスイッチには、ライセンスを管理して追加ライセンスをインストールするためのコマンドがあります。

QoS

Cisco Nexus 5000 シリーズ スイッチには、出力インターフェイスにおけるトラフィックの優先順位付けおよび帯域割り当てなどの Quality of Service（QoS）機能があります。

スイッチのデフォルト QoS 設定では、ファイバ チャネル トラフィックと FCoE トラフィックにロスレス サービスが提供されます。イーサネット トラフィックのサービス クラス（CoS）を追加するよう QoS を設定できます。

サービスアビリティ

Cisco Nexus 5000 シリーズ スイッチのサービスアビリティ機能ではネットワーク プランニング用のデータが提供され、問題解決の時間を短縮できます。

この項では、次のトピックについて取り上げます。

- スイッチド ポート アナライザ（1-6 ページ）
- Ethanalyzer（1-6 ページ）
- Call Home（1-6 ページ）
- オンライン診断（1-7 ページ）

スイッチド ポート アナライザ

スイッチド ポート アナライザ（SPAN）機能により、管理者は外部アナライザが接続されている SPAN 宛先ポートに、セッションに影響を与えることなく SPAN セッション トラフィックを転送して、ポート間のすべてのトラフィックを分析できます。

Ethanalyzer

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

Call Home

Call Home は、ハードウェア コンポーネントとソフトウェア コンポーネントを継続的にモニタリングし、重要なシステム イベントを E メールで通知する機能です。さまざまなメッセージ フォーマットが用意されており、ポケットベル サービス、標準の E メール、および XML ベースの自動解析アプリケーションに対応します。この機能では、アラート グルーピング機能およびカスタマイズ可能な宛先プロファイルが提供されます。この機能の利用方法には、ネットワーク サ

ポート技術者を直接ポケットベルで呼び出す、ネットワーク オペレーション センター（NOC）に E メール メッセージを送信する、およびCisco AutoNotify サービスを採用して Cisco Technical Assistance Center（TAC）へ問題を直接送信する、などの方法があります。自律システム運用に向けたこの機能により、問題発生時にネットワーキング デバイスから IT 部門への通知が可能になり、問題を迅速に解決できるようになります。

オンライン診断

Cisco Generic Online Diagnostics（GOLD）は一連の診断機能であり、ハードウェアと内部データ パスが設計どおりに動作していることを確認できます。Cisco GOLD フィーチャ セットには、起動時診断、継続監視、オンデマンド テスト、スケジュール テストが含まれます。GOLD では障害を迅速に特定し、システムを継続的に監視できます。

スイッチ管理

この項では、次のトピックについて取り上げます。

- 簡易ネットワーク管理プロトコル（1-7 ページ）
- RBAC（1-7 ページ）
- 設定メソッド（1-7 ページ）

簡易ネットワーク管理プロトコル

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

RBAC

ロールベース アクセス コントロール（RBAC）では、ユーザにロールを割り当ててスイッチ操作へのアクセスを制限できます。管理者はアクセスをカスタマイズし、必要なユーザにそのアクセスを限定できます。

設定メソッド

直接ネットワーク設定方式または Fabric Manager サーバでホスティングされる Web サービスを使用して、Cisco Nexus 5000 シリーズ スイッチを設定できます。

この項では、次のトピックについて取り上げます。

- CLI、XML 管理インターフェイス、または SNMP による設定（1-7 ページ）
- Cisco MDS Fabric Manager での設定（1-8 ページ）

CLI、XML 管理インターフェイス、または SNMP による設定

コマンドライン インターフェイス（CLI）、SSH による XML 管理インターフェイス、または SNMP のうちいずれかを使用し、次のように Cisco Nexus 5000 シリーズ スイッチを設定できます。

- CLI：SSH セッション、Telnet セッション、またはコンソール ポートから CLI を使用してスイッチを設定できます。SSH ではデバイスへの安全な接続が提供されます。

- SSH による XML 管理インターフェイス：CLI 機能を補完する NETCONF プロトコルに基づくプログラミング インターフェイスである XML 管理インターフェイスを使用し、スイッチを設定できます。詳細については、『*Cisco NX-OS XML Management Interface User Guide*』Release 4.0 を参照してください。
- SNMP：MIB を使用してスイッチを設定できます。

Cisco MDS Fabric Manager での設定

Fabric Manager クライアントを使用して Cisco Nexus 5000 シリーズ スイッチを設定できます。Fabric Manager クライアントは、ローカル PC 上で稼働し、Fabric Manager サーバを使用します。

ネットワーク セキュリティ機能

Cisco NX-OS Release 4.0 には次のセキュリティ機能が含まれます。

- 認証、許可、アカウンティング（AAA）および TACACS+
- RADIUS
- SSH プロトコル バージョン 2
- 簡易ネットワーク管理プロトコル バージョン 3（SNMPv3）
- ポートベース ACL（PACL）および VLAN ベース ACL（VACL）を含む MAC ACL および IP ACL

VDC

Cisco NX-OS では、仮想デバイスをエミュレートする Virtual Device Context（VDC）に、オペレーティング システムおよびハードウェア リソースを分割できます。Cisco Nexus 5000 シリーズ スイッチでは複数の VDC はサポートされません。すべてのスイッチ リソースはデフォルト VDC で管理されます。

一般的な配置トポロジ

このリリースにおける Cisco Nexus 5000 シリーズ スイッチの一般的な配置トポロジは、次のとおりです。

- イーサネット TOR スイッチ トポロジ（1-8 ページ）
- IOC トポロジ（1-10 ページ）

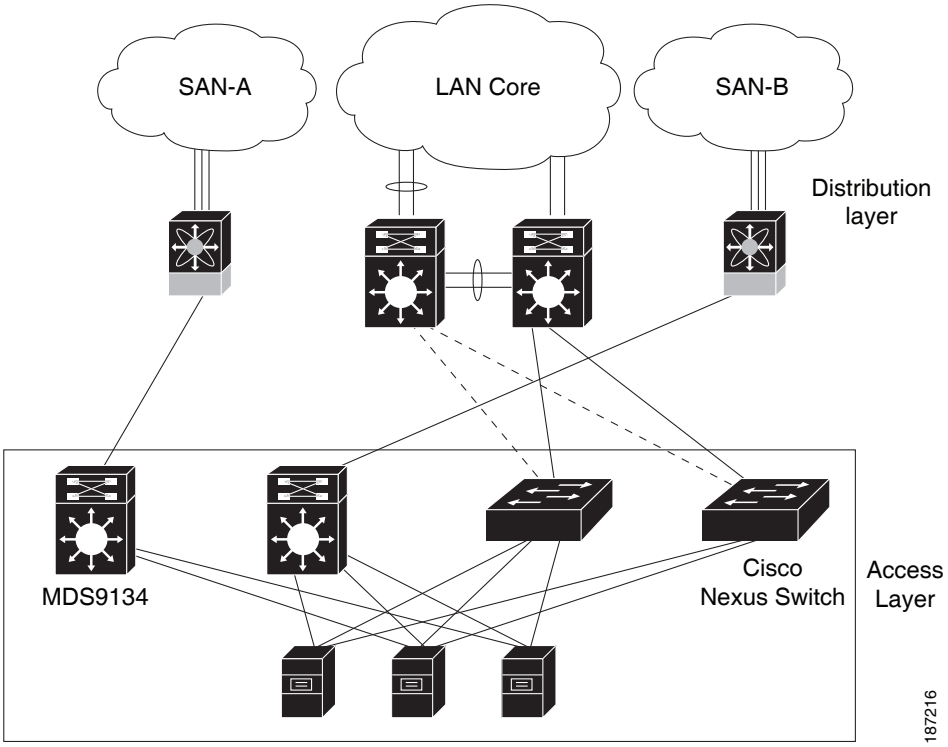
イーサネット TOR スイッチ トポロジ

Cisco Nexus 5000 シリーズ スイッチは、データセンターの LAN 配信レイヤ スイッチへのアップリンクを搭載した、10 ギガビット イーサネット Top-Of-Rack（TOR）スイッチとして配置できます。図 1-2に、構成例を示します。

この例では、ブレード サーバ ラックにブレード スイッチが組み込まれ、Cisco Nexus 5000 シリーズ スイッチへの 10 ギガビット イーサネット アップリンクがサポートされます。ブレード スイッチは FCoE をサポートしないので、Cisco Nexus 5000 シリーズ スイッチには FCoE トラフィックおよびファイバ チャネル ポートがありません。

この構成例の Cisco Nexus 5000 シリーズ スイッチには、2 つの Catalyst スイッチへのイーサネット アップリンクがあります。データセンター LAN で STP をイネーブルにしている場合、どちらかのスイッチへのリンクは STP 対応となり、その他のスイッチへのリンクでは STP がブロックされます。

図 1-2　　イーサネット TOR スイッチ トポロジ



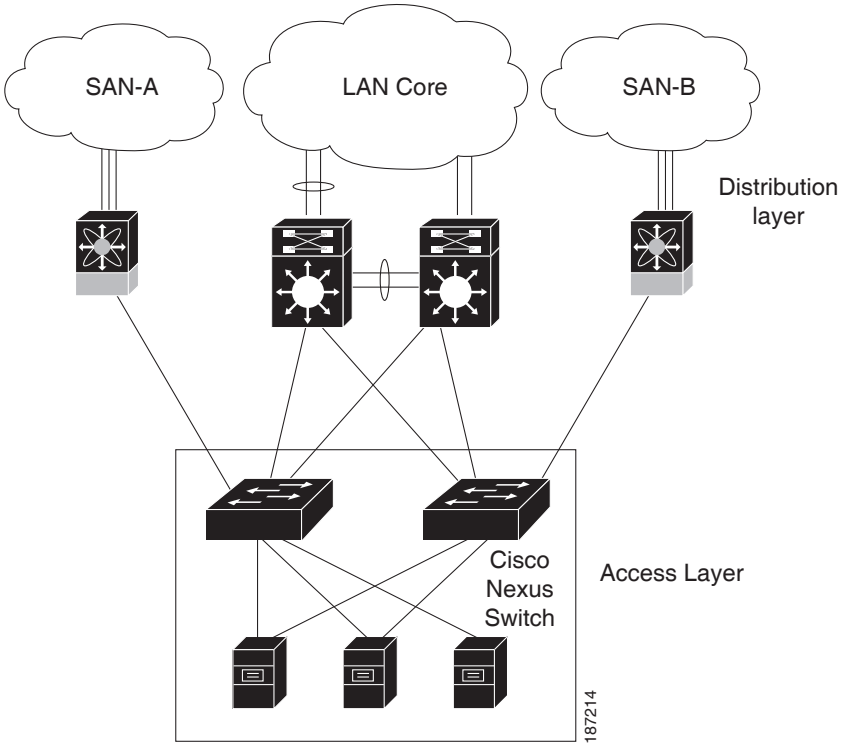
Cisco Nexus 5000 シリーズ スイッチのサーバ側ポートはすべて、標準イーサネットを実行しています。FCoE は不要なので、サーバ ポートは 10 ギガビット イーサネット NIC で接続されます。

サーバは、MDS 9134 SAN スイッチでデータセンター SAN に接続されます。サーバのファイバ チャネル ポートでは、標準ファイバ チャネル HBA が必要です。

IOC トポロジ

図 1-3 に、Cisco Nexus 5000 シリーズ スイッチの一般的な I/O Consolidation（IOC）シナリオを示します。

図 1-3　IOC トポロジ



Cisco Nexus 5000 シリーズ スイッチは、FCoE でサーバ ポートに接続します。サーバのポートでは CNA が必要です。冗長性を確保するために、各サーバは両方のスイッチに接続します。この目的のためにはデュアルポート CNA アダプタを使用できます。CNA は active-passive モードで設定されます。また、サーバではサーバベース フェールオーバーをサポートする必要があります。

Cisco Nexus 5000 シリーズ スイッチでは、イーサネット ネットワーク側ポートを 2 つの Catalyst 6500 スイッチに接続します。必要なアップリンク トラフィック量により、各 Catalyst 6500 スイッチに複数のポートが接続されてポート チャネルとして設定されることがあります。データセンター LAN で STP をイネーブルにしている場合、どちらかのスイッチへのリンクは STP 対応となり、その他のスイッチへのリンクでは STP がブロックされます。

Cisco Nexus 5000 シリーズ スイッチの SAN ネットワーク側ポートは、Cisco MDS 9000 ファミリ スイッチに接続されます。必要なトラフィック量により、各 MDS 9000 ファミリ スイッチに複数のファイバ チャネル ポートが接続されて SAN ポート チャネルとして設定されることがあります。

サポートされる規格

表 1-1 に、Cisco Nexus 5000 シリーズ スイッチでサポートされる標準を示します。

表 1-1　IEEE への準拠

規格	説明
802.1D	MAC ブリッジ
802.1s	マルチ スパニングツリー プロトコル
802.1w	高速スパニングツリー プロトコル
802.3ad	LACP によるリンク集約
802.3ae	10 ギガビット イーサネット
802.1Q	VLAN タギング
802.1p	イーサネット フレームのサービス クラス（CoS）タギング

CHAPTER 2

コマンドライン インターフェイスの使用

この章では、コマンドライン インターフェイス（CLI）および CLI コマンド モードについて説明します。内容は次のとおりです。

- コマンドライン インターフェイスへのアクセス（2-1 ページ）
- CLI の使用（2-2 ページ）
- コマンドの使用方法（2-6 ページ）
- CLI 変数の使用（2-9 ページ）
- コマンド エイリアスの使用（2-10 ページ）
- コマンド エイリアスの定義（2-11 ページ）
- コマンド スクリプト（2-11 ページ）

コマンドライン インターフェイスへのアクセス

このスイッチには、コンソール ポートに設置されている端末を使用して接続できます。コンソール ポート パラメータの設定方法については、コンソール設定（3-3 ページ）を参照してください。

Telnet または SSH でスイッチに接続することもできます。このスイッチでは、同時に最大 8 つの Telnet 接続および SSH 接続がサポートされます。Telnet または SSH で接続するには、スイッチのホスト名または IP アドレスが必要になります。

スイッチへの Telnet 接続を確立する手順は、次のとおりです。

	コマンド	目的
ステップ 1	**telnet** {*hostname* | *ip_addr*}	ホストからアクセスするスイッチへの Telnet 接続を確立します。
ステップ 2	Login: **admin** Password: ***password***	認証を開始します。 **（注）** パスワードが設定されていない場合は、Return を押します。
ステップ 3	switch# **exit**	セッションを終了します。

スイッチへの SSH 接続を確立する手順は、次のとおりです。

コマンド	目的
ssh {*hostname* | *ip_addr*}	ホストからアクセスするスイッチへの SSH 接続を確立します。

CLI の使用

ここでは、次の内容について説明します。

- CLI コマンド モードの使用方法 (2-2 ページ)
- CLI コマンド階層構造 (2-3 ページ)
- EXEC モード コマンド (2-3 ページ)
- コンフィギュレーション モード コマンド (2-5 ページ)

CLI コマンド モードの使用方法

Cisco Nexus 5000 シリーズ のスイッチには、ユーザ EXEC モードとコンフィギュレーション モードという主に 2 つのコマンド モードがあります。利用できるコマンドは、現在のモードによって異なります。それぞれのモードで使用可能なコマンドのリストを取得するには、システム プロンプトで疑問符 (**?**) を入力します。

表 2-1 に、一般的に使われる 2 つのモードと、そのモードの開始方法、およびそこから返されるシステム プロンプトを示します。システム プロンプトから、現在実行しているモードを識別して、そのモードで使用できるコマンドを判断できます。

表 2-1　一般的なスイッチのコマンド モード

モード	説明	開始方法	プロンプト
EXEC	端末の設定を一時的に変更したり、基本的なテストを実行できます。また、システム情報も表示できます。 **(注)**　このモードで行う変更は通常保存されないため、システム リセット後には反映されません。	スイッチ プロンプトに、必要な EXEC モード コマンドを入力します。	`switch#`
コンフィギュレーション モード	システム全体に影響を及ぼす機能を設定できます。 **(注)**　このモードで行う変更はシステム リセット後にも保存されます (設定を保存した場合)。	EXEC モードで **configure terminal** コマンドを入力します。	`switch(config)#`

コマンドを入力する際、他のコマンドと区別がつく文字数だけを入力して、コマンドおよびキーワードを省略できます。たとえば、**configure terminal** コマンドを **conf t** に省略できます。

コマンド モードの変更

コンフィギュレーション モード（別名、端末コンフィギュレーション モード）には、いくつかのサブモードがあります。これらの各サブモードを使用すると、プロンプトのより下の階層で作業できます。**exit** を入力すると、スイッチは現在のレベルを 1 つ前に戻すため、ユーザは前回のレベルに戻ることができます。**end** を入力すると、スイッチはユーザ EXEC レベルに戻ります。**end** を入力する代わりに、コンフィギュレーション モードで **Ctrl+Z** を押しても同様です。

各コマンド モードで使用可能なコマンドの一覧表示

スイッチ プロンプトで疑問符（**?**）を入力すると、任意のコマンド モードで使用できるコマンドを表示できます。

CLI コマンド階層構造

CLI コマンドは、同じような機能を実行するコマンドを同じレベルに集めた階層構造で編成されています。たとえば、システム、設定、またはハードウェアに関する情報を表示するコマンドはすべて **show** コマンドとしてグループ化されています。また、スイッチを設定できるコマンドはすべて **configure terminal** コマンドとしてグループ化されています。

コマンドを実行するには、階層の最上位から始めてコマンドを入力します。たとえば、インターフェイスを設定するには、**config terminal** コマンドを使用します。次に、コンフィギュレーション モードが開始されるので、**interface** コマンドを入力します。インターフェイス サブモードが開始され、使用できるコマンドを調べることができます。

次に、インターフェイス サブモードで使用できるコマンドを確認する例を示します。

```
switch# configure terminal
switch(config)# interface fc 3/1
switch(config-if)# ?
  channel-group   add to/remove from a san-port-channel
  description     Enter description of maximum 80 characters
  exit            Exit from command interpreter
  fcdomain        Configure fcdomain parameters
  fspf            Configure FSPF parameters
  no              Negate a command or set its defaults
  out-of-service  Put an interface out of service.
  shutdown        Enable/disable an interface
  switchport      Configure switchport parameters
```

EXEC モード コマンド

スイッチ上でセッションを開始する場合、最初は EXEC モードから始めます。この EXEC モードから、コンフィギュレーション モードを開始できます。EXEC コマンドの大半は、現在の設定状態を表示する **show** コマンドのような 1 回限りのコマンドです。

次のコマンドは EXEC モードで使用できます。

```
switch# ?
  callhome          callhome commands
  cd                Change current directory
  clear             Reset functions
  cli               CLI commands
  clock             Manage the system clock
  configure         Enter configuration mode
  copy              Copy from one file to another
```

```
debug             Debugging functions
debug-filter      Enable filtering for debugging functions
delete            delete a file
dir               list files in a directory
discover          discover information
end               Exit configuration mode
ethanalyzer       Configure cisco fabric analyzer
exit              Exit from command interpreter
fcping            Ping an N-Port
fctrace           Trace the route for an N-Port.
file              File management commands
find              Find a file below the current directory
format            Format disks
gunzip            Uncompresses LZ77 coded files
gzip              Compresses file using LZ77 coding
install           upgrade software
ip                Configure IP features
license           Enter the license configuration mode
logit             Add syslog message
mkdir             Create new directory
move              Move files
no                Negate a command or set its defaults
ntp               Execute NTP commands
ping              Test network reachability
purge             Deletes unused data
pwd               View current directory
reload            Reboot the entire box
replace           Discard the entire configuration and load the entire configuration in
                  <filename>
rmdir             delete a directory
run-script        Run shell scripts
san-port-channel  Port-Channel related commands
send              Send message to open sessions
session           Configure session preferences
setup             Run the basic SETUP command facility
show              Show running system information
sleep             Sleep for the specified number of seconds
ssh               SSH to another system
syslog            Execute a logging command
system            System management commands
tac-pac           save tac information to a specific location
tail              Display the last part of a file
telnet            Telnet to another system
terminal          Set terminal line parameters
terminate         Terminates a config session
test              test command
traceroute        Traceroute to destination
undebug           Disable Debugging functions (See also debug)
unmount           unmount compact flash disk or usb drive
update            Update license
write             Write current configuration
xml               xml agent
zone              Execute Zone Server commands
zoneset           Execute zoneset commands
```

コンフィギュレーション モード コマンド

コンフィギュレーション モードでは、既存の設定を変更できます。変更した設定を保存すると、スイッチの再起動後も変更内容が保存されます。コンフィギュレーション モードでは、インターフェイス コンフィギュレーション モード、ゾーン コンフィギュレーション モード、およびプロトコルに特化したさまざまなモードを開始できます。コンフィギュレーション モードは、すべてのコンフィギュレーション コマンドの開始点です。

次のコマンドはコンフィギュレーション モードで使用できます。

```
switch# configure terminal
switch(config)# ?
  aaa                 Configure aaa functions
  arp                 ARP
  banner              Configure banner message
  boot                Configure boot variables
  callhome            Enter the callhome configuration mode
  cdp                 CDP Configuration parameters
  cfs                 CFS configuration commands
  class-map           Configure class-map
  cli                 Configure CLI aliases
  clock               Configure time-of-day clock
  device-alias        Device-alias configuration commands
  diagnostic          Diagnostic commands
  end                 Exit configuration mode
  exit                Exit from command interpreter
  fabric              Switch fabric information
  fabric-binding      Fabric Binding configuration
  fc                  FCoE/FC feature
  fcalias             Fcalias configuration commands
  fcdomain            Enter the fcdomain configuration mode
  fcdroplatency       configure switch or network latency
  fcflow              Configure fcfloww
  fcid-allocation     Add/remove company id(or OUIs) from auto area list
  fcinterop           Interop commands
  fcns                name server configuration
  fcroute             Configure FC routes
  fcs                 Configure Fabric Config Server
  fcsp                Config commands for FC-SP
  fctimer             configure fibre channel timers
  fdmi                config commands for FDMI
  feature             Command to enable/disable features
  fspf                Configure fspf
  hostname            Configure system's host name
  hw-module           Enable/Disable OBFL information
  in-order-guarantee  set in-order delivery guarantee
  interface           Configure interfaces
  ip                  Configure IP features
  ipv6                Configure IPv6 features
  line                Configure a terminal line
  lldp                Configure global LLDP parameters
  logging             Modify message logging facilities
  mac                 MAC configuration commands
  mac-address-table   MAC Address Table
  monitor             Ethernet SPAN
  no                  Negate a command or set its defaults
  npiv                Nx port Id Virtualization (NPIV) feature enable
  npv                 Config commands for FC N_port Virtualizer
  ntp                 NTP Configuration
  pm                  packet manager
  policy-map          Configure policy-map
  port-channel        Add to/remove from a port-channel
  port-security       Configure Port Security
```

```
  port-track          Configure Switch port track config
  privilege           Command privilege parameters
  prompt              Define default prompt
  radius-server       Configure RADIUS related parameters
  resequence          Resequence a list with sequence numbers
  rib                 Configure RIB parameters
  rlir                config commands for RLIR
  rmon                Remote Monitoring
  role                Configure roles
  rscn                config commands for RSCN
  scsi-target         scsi-target configuration
  show                Show running system information
  snmp-server         Configure snmp server
  spanning-tree       Spanning Tree Subsystem
  ssh                 Configure SSH parameters
  svi                 svi configuration commands
  switchname          Configure system's host name
  system              system config command
  system              Configure system
  tacacs+             Enable tacacs+
  telnet              Enable telnet
  track               Object tracking configuration commands
  trunk               Configure Switch wide trunk protocol
  username            Configure user information.
  vlan                Vlan commands
  vrf                 Configure VRF parameters
  vsan                Enter the vsan configuration mode
  wwn                 Set secondary base MAC addr and range for additional WWNs
  xml                 xml agent
  zone                Zone configuration commands
  zoneset             Zoneset configuration commands
```

コマンドの使用方法

CLI を 2 つの方法で機能するように設定できます。この 2 つの方法は、CLI プロンプトでコマンドを入力してインタラクティブに設定する方法、またはスイッチ設定情報を含む ASCII ファイルを作成する（CLI を使用してファイルを編集し、アクティブ化する）方法です。

コマンドおよび構文の一覧表示

すべてのコマンド モードで、疑問符（?）を入力することにより、使用できるコマンドのリストを表示できます。

```
switch# ?
```

特定の文字シーケンスで始まるコマンドの一覧を表示するには、それらの文字を入力した後に疑問符（?）を入力します。疑問符の前にスペースを入れないでください。

```
switch# co?
configure copy
```

キーワードまたは引数のリストを表示するには、キーワードまたは引数の代わりに疑問符を入力します。疑問符の前にスペースを 1 つ入れてください。この形式のヘルプをコマンド構文ヘルプと呼びます。入力したコマンド、キーワード、および引数に基づいて、使用できるキーワードまたは引数を表示するためです。

```
switch# # configure ?
  <CR>
  terminal  Configure the system from terminal input
```

ヒント　コマンドを入力してエラーになる場合は、システム プロンプトをチェックし、疑問符（**?**）を入力して使用可能なコマンドの一覧を表示してください。コマンド モードが間違っているか、間違った構文を使用している可能性があります。

コマンド文字列の入力

どのコマンド モードでも、特定のコマンドの文字列を入力して、すぐに **Tab** キーを押すと残りのコマンドを完了させることができます。

```
switch (config)# ro<Tab>
switch (config)# role <Tab>
switch (config)# role name
```

この形式のヘルプをコマンド補完機能と呼びます。この機能はコマンドの文字を補完します。入力した文字に対して複数のオプションがある場合、それらの文字に一致するすべてのオプションが表示されます。

取り消しまたはデフォルト値/条件の復元

すべてのコマンドで **no** 形式を入力して、次の操作を実行できます。

- 誤って入力したコマンドを取り消す

  zone member コマンドを入力した場合、このコマンドの結果を次のようにして取り消すことができます。

  ```
  switch(config)# zone name test vsan 1
  switch(config-zone)# member pwwn 12:12:12:12:12:12:12:12
  switch(config-zone)# no member pwwn 12:12:12:12:12:12:12:12
  WARNING: Zone is empty.Deleting zone test.Exit the submode.
  switch(config-zone)#
  ```

- 作成したファシリティを削除する

  作成したゾーンを削除する場合は次のようになります。

  ```
  switch(config)# zone name test vsan 1
  switch(config-zone)# exit
  switch(config)# no zone name test vsan 1
  switch(config)#
  ```

  ゾーン コンフィギュレーション サブモードをまだ終了していない場合、test というゾーン ファシリティは削除できません。最初にゾーン サブモードを終了し、コンフィギュレーション モードに戻る必要があります。

- デフォルト値に戻す

  zone merge-control restrict vsan コマンドを入力した場合、このコマンドの結果を次のようにして取り消すことができます。

  ```
  switch(config)# zone merge-control restrict vsan 10
  switch(config)# no zone merge-control restrict vsan 10
  switch(config)#
  ```

キーボード ショートカットの使用方法

コンフィギュレーション モードまたはサブモードのプロンプトから、EXEC モードのコマンドを実行することができます。コンフィギュレーション モード内のすべてのサブモードから、このコマンドを入力できます。コンフィギュレーション モード（または任意のサブモード）で、必要な EXEC モードコマンドとともに **do** コマンドを入力します。コマンドは EXEC レベルで実行され、その後、プロンプトが現在のモード レベルに戻って再開されます。

```
switch(config)# do terminal session-timeout 0
switch(config)#
```

上記の例の **terminal session-timeout** は EXEC モードのコマンドです。EXEC モード コマンドを、コンフィギュレーション モードの **do** コマンドを使用して入力したことになります。

do コマンドは、**end** および **exit** コマンド以外のすべての EXEC モード コマンドに適用されます。また、EXEC コマンドとともに **do** コマンドを入力する場合は、EXEC コマンドのヘルプ（?）機能およびコマンドの補完（**Tab**）機能を使用することもできます。

表 2-2 に、EXEC モードおよびコンフィギュレーション モードの両方で使用できる便利なコマンド キーを示します。

表 2-2　　便利なコマンド キー

コマンド	説明
Ctrl+P	履歴を上へ
Ctrl+N	履歴を下へ
Ctrl+X+H	履歴の一覧表示
Alt+P	履歴を後方へ検索 **（注）** Tab キーによるコマンド補完機能と Alt+P キーまたは Alt+N キーの違いは、Tab キーが現在のワードを補完するのに対し、Alt+P キーおよび Alt+N キーは前に入力したコマンドを完成させる点です。
Alt+N	履歴を前方へ検索
Ctrl+G	終了
Ctrl-Z	終了
Ctrl+L	セッションのクリア

表 2-3 では、一般的に使用するコンフィギュレーション サブモードについて説明します。

表 2-3　　一般的なコンフィギュレーション サブモード

サブモード名	コンフィギュレーション モードからの入力例	サブモードのプロンプト
Call Home	**callhome**	switch(config-callhome)#
FCS 登録	**fcs register**	switch(config-fcs-register)#
	FCS 登録サブモードから **platform name** *name* **vsan** *vsan-id*	switch(config-fcs-register-attrib)#
ファイバ チャネル エイリアス	**fcalias name** *name* **vsan** *vsan-id*	switch(congif-fcalias)#

表 2-3　一般的なコンフィギュレーション サブモード（続き）

サブモード名	コンフィギュレーション モードからの入力例	サブモードのプロンプト
FSPF	**fspf config vsan** *vsan-id*	switch(config-(fspf-config))#
インターフェイス コンフィギュレーション	**interface** *type slot/port*	switch(config-if)#
ライン コンソール	**line console**	switch(config-console)
仮想端末回線	**line vty**	switch(config-line)#
ロール	**role name**	switch(config-role)#
VLAN	**vlan**	switch(config-vlan)#
VSAN データベース	**vsan database**	switch(config-vsan-db)#
ゾーン	**zone name** *string* **vsan** *vsan-id*	switch(config-zone)#
ゾーン セット	**zoneset name** *name* **vsan** *vsan-id*	switch(config-zoneset)#

CLI 変数の使用

Cisco Nexus 5000 シリーズ CLI パーサーは CLI コマンドでの変数の定義および使用をサポートします。CLI 変数は次のように使用できます。

- コマンドラインで直接入力する。
- **run-script** コマンドを使用して開始された子スクリプトに渡す。

  親シェルで定義した変数は子 **run-script** コマンド プロセスで使用できます（「スクリプトで指定されたコマンドの実行」セクション（2-11 ページ）を参照）。
- **run-script** コマンドのコマンドライン引数として渡す（「スクリプトで指定されたコマンドの実行」セクション（2-11 ページ）を参照）。

CLI 変数には、次の特性があります。

- 入れ子状態の参照を使用して、別の変数から変数は参照できません。
- スイッチを再起動しても使用できる固定変数を定義できます。
- 参照できるのは 1 つの定義済みシステム変数、TIMESTAMP 変数だけです。

ユーザ定義の固定 CLI 変数

EXEC モードで **cli var name** コマンドを使用すると、CLI セッションの間だけ有効な CLI セッション変数を定義できます。CLI セッション変数は定期的に実行するスクリプトに役立ちます。

次に、ユーザ定義の CLI セッション変数を作成する例を示します。

```
switch# cli var name testinterface fc 1/1
```

$(variable) 構文を使用して変数を参照できます。次に、ユーザ定義の CLI セッション変数を参照する例を示します。

```
switch# show interface $(testinterface)
fc2/1 is up
Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
```

```
Port WWN is 20:01:00:0d:ec:0e:1d:00
Admin port mode is auto, trunk mode is on
snmp traps are enabled
Port mode is F, FCID is 0x01000b
Port vsan is 1
Speed is 2 Gbps
Transmit B2B Credit is 7
Receive B2B Credit is 16
Receive data field Size is 2112
Beacon is turned off
5 minutes input rate 256 bits/sec, 32 bytes/sec, 1 frames/sec
5 minutes output rate 256 bits/sec, 32 bytes/sec, 1 frames/sec
  232692 frames input, 7447280 bytes
    0 discards, 0 errors
    0 CRC,  0 unknown class
    0 too long, 0 too short
  232691 frames output, 7448692 bytes
    0 discards, 0 errors
  0 input OLS, 0 LRR, 0 NOS, 0 loop inits
  1 output OLS, 1 LRR, 0 NOS, 1 loop inits
  16 receive B2B credit remaining
  7 transmit B2B credit remaining
```

ユーザ定義の CLI セッション変数を表示するには、**show cli variables** コマンドを使用します。次に、ユーザ定義の CLI セッション変数を表示する例を示します。

```
switch# show cli variables
VSH Variable List
-----------------
TIMESTAMP="2005-10-24-21.29.33"
testinterface="fc 1/1"
```

ユーザ定義の CLI セッション変数を削除するには、**cli no var name** コマンドを使用します。次に、ユーザ定義の CLI セッション変数を削除する例を示します。

```
switch# cli no var name testinterface
```

コマンド エイリアスの使用

コマンド エイリアスには、次の特性があります。

- コマンド エイリアスはすべてのユーザ セッションに対してグローバルです。
- コマンド エイリアスは再起動後も保存されます。
- エイリアスを付けたコマンドは省略せずに完全に入力する必要があります。
- コマンド エイリアス変換は常にすべてのコンフィギュレーション モードまたはサブモードのすべてのキーワードの中で最優先されます。
- コマンド エイリアスのサポートはスイッチング モジュールではなく、スーパーバイザ モジュールでだけ利用できます。
- コマンド エイリアスの設定は他のユーザ セッションに対してただちに有効になります。
- デフォルトのコマンド エイリアス **alias** を変更できません。これは **show cli alias** コマンドのエイリアスです。
- コマンド エイリアスのネスティングは最大深度 1 まで可能です。1 つのコマンド エイリアスは、有効なコマンドを参照する必要がある別のコマンド エイリアスを参照できますが、その他のコマンド エイリアスは参照できません。

- コマンド エイリアスは必ず、コマンドラインの最初のコマンド キーワードを置き換えます。
- すべてのコンフィギュレーション サブモードまたは EXEC モードで、コマンドのコマンド エイリアスを定義できます。

コマンド エイリアスの定義

コマンド エイリアスは、コンフィギュレーション モードで **cli alias name** コマンドを使用して定義できます。

次に、コマンド エイリアスを定義する例を示します。

```
switch# configure terminal
switch(config)# cli alias name eth interface ethernet
switch(config)# cli alias name shintbr show interface brief
switch(config)# cli alias name shfcintup shintbr | include up | include fc
```

スイッチで定義されたコマンド エイリアスは、デフォルトのコマンド エイリアス **alias** を使用して表示できます。

次に、スイッチに定義されたコマンド エイリアスを表示する例を示します。

```
switch# alias
CLI alias commands
==================
alias      :show cli alias
gigint     :interface gigabitethernet
shintbr    :show interface brief
shfcintup  :shintbr | include up | include fc
```

コマンド スクリプト

この項では、次のトピックについて取り上げます。

- スクリプトで指定されたコマンドの実行（2-11 ページ）
- スクリプトでの CLI 変数の使用（2-12 ページ）
- 遅延時間の設定（2-13 ページ）

スクリプトで指定されたコマンドの実行

run-script コマンドは、ファイルに指定されたコマンドを実行します。このコマンドを使用する場合、ファイルが作成され、正しい順番でコマンドが指定されていることを確認してください。

（注） スイッチ プロンプトでスクリプト ファイルは作成できません。外部装置上でスクリプト ファイルを作成し、bootflash: ディレクトリにコピーすることはできます。ここでは、スクリプト ファイルが bootflash: ディレクトリにすでにあることを前提としています。

このコマンドの構文は、**run-script** *filename* です。

次に、bootflash: ディレクトリにある testfile に指定されている CLI コマンドを表示する例を示します。

```
switch# show file bootflash:testfile
configure terminal
interface fc 3/1
no shutdown
end
show interface fc 3/1
```

次に、testfile の内容を実行した **run-script** コマンドの出力結果を示します。

```
switch# run-script bootflash:testfile
'configure terminal'
Enter configuration commands, one per line.End with CNTL/Z.
'interface fc 3/1'
'shutdown'
'end'
'show interface fc 3/1'
fc3/1 is trunking
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:81:00:0d:ec:6b:cd:c0
    Peer port WWN is 20:01:00:0d:ec:0d:d0:00
    Admin port mode is auto, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
    Speed is 2 Gbps
    Transmit B2B Credit is 255
    Receive B2B Credit is 16
    Receive data field Size is 2112
    Beacon is turned off
    Trunk vsans (admin allowed and active) (1)
    Trunk vsans (up)                       (1)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
    5 minutes input rate 96 bits/sec, 12 bytes/sec, 0 frames/sec
    5 minutes output rate 64 bits/sec, 8 bytes/sec, 0 frames/sec
      77423 frames input, 6708868 bytes
        0 discards, 0 errors
        0 CRC,  0 unknown class
        0 too long, 0 too short
      77302 frames output, 4184976 bytes
        0 discards, 0 errors
      1 input OLS, 2 LRR, 0 NOS, 0 loop inits
      1 output OLS, 0 LRR, 1 NOS, 0 loop inits
      16 receive B2B credit remaining
      255 transmit B2B credit remaining
```

スクリプトでの CLI 変数の使用

cli var コマンドで定義された CLI 変数（「CLI 変数の使用」セクション（2-9 ページ）を参照）、または **run-script** コマンドで引数として渡された CLI 変数を使用できます。

次に、**run-script** コマンドで使用されるスクリプト ファイル内での CLI セッション変数の使用例を示します。

```
switch# cli var name testinterface fc 1/1
switch# show file bootflash:test1.vsh
show interface $(testvar)
switch# run-script bootflash:test1.vsh
```

```
`show interface $(testvar)`
fc2/1 is down (SFP not present)
Hardware is Fibre Channel
Port WWN is 20:01:00:05:30:00:8e:1e
Admin port mode is auto, trunk mode is on
Port vsan is 1
Receive data field Size is 2112
Beacon is turned off
5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
1 frames input, 128 bytes
0 discards, 0 errors
0 CRC, 0 unknown class
0 too long, 0 too short
1 frames output, 128 bytes
0 discards, 0 errors
0 input OLS, 0 LRR, 0 NOS, 0 loop inits
0 output OLS, 0 LRR, 0 NOS, 0 loop inits
0 receive B2B credit remaining
0 transmit B2B credit remaining
```

次に、CLI セッション変数を子 **run-script** コマンド プロセスへの引数として渡す例を示します。

```
switch# show file bootflash:test1.vsh
show interface $(var1) $(var2)
switch# run bootflash:test2.vsh var1="fc2/1" var2="brief"
`show interface $(var1) $(var2)`
--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                          Mode  Speed  Channel
                         Mode                                 (Gbps)
--------------------------------------------------------------------------------
fc2/1 1 auto on sfpAbsent -- -- -- \
```

遅延時間の設定

sleep コマンドは、指定の秒数の間、特定のアクションを遅延させます。

このコマンドの構文は、**sleep** *seconds* です。

```
switch# sleep 30
```

この場合、30 秒後にスイッチ プロンプトが再表示されます。このコマンドはスクリプト内で役立ちます。たとえば、次のような test-script というコマンド スクリプトを作成しているとします。

```
switch# show file bootflash:test-script
discover scsi-target remote
sleep 10
show scsi-target disk
switch# run-script bootflash:test-script
```

test-script コマンド スクリプトを実行すると、スイッチ ソフトウェアは **discover scsi-target remote** コマンドを実行した後、10 秒待機してから、**show scsi-target disk** コマンドを実行します。

CHAPTER 3

スイッチの設定

この章では、基本的なスイッチ設定機能について説明します。この章は、次の項で構成されています。

- スイッチのイメージ ファイル(3-1 ページ)
- スイッチのアップグレード (3-4 ページ)
- 以前のリリースへのダウングレード (3-7 ページ)
- 初期設定(3-8 ページ)
- スイッチへのアクセス(3-13 ページ)
- スイッチのその他の設定(3-13 ページ)
- NTP 設定(3-16 ページ)
- 管理インターフェイスの設定(3-21 ページ)
- スイッチ コンフィギュレーションの管理(3-23 ページ)
- スイッチ ファイル システムの使用(3-24 ページ)

スイッチのイメージ ファイル

Cisco Nexus 5000 シリーズ スイッチには次のイメージがあります。

- 1 つのファイルに組み合わされた BIOS イメージおよびローダ イメージ
- キックスタート イメージ
- アップグレード可能な BIOS イメージを含むシステム イメージ

このスイッチにはフラッシュ メモリがあり、次の 2 つのフラッシュ部分から構成されています。

- 2 つの BIOS イメージおよびローダ イメージを保持する、2 MB のフラッシュ部分
- 設定ファイル、キックスタート イメージ、システム イメージ、その他のファイルを保持する、1 GB のフラッシュ部分

アップグレード可能な BIOS およびゴールデン BIOS は、2 MB のフラッシュ部分にプログラムされています。ゴールデン BIOS はアップグレードできません。

キックスタート イメージとシステム イメージの新しいペアをダウンロードすると、新しい BIOS イメージも取得されます。BIOS イメージがシステム イメージに組み込まれているからです。キックスタート イメージ、システム イメージ、アップグレード可能 BIOS イメージをアップグレードするには、**install all** コマンドを使用します。

この項では、次のトピックについて取り上げます。

- スイッチの起動（3-2 ページ）
- ブート シーケンス（3-2 ページ）

スイッチの起動

Cisco Nexus 5000 シリーズ スイッチでは、電源コードを A/C 電源に差し込むとすぐにブート プロセスが始まります。このスイッチには電源スイッチがありません。

ブート シーケンス

スイッチを起動すると、ゴールデン BIOS がアップグレード可能 BIOS のチェックサムを検証します。チェックサムが有効である場合、制御はアップグレード可能 BIOS イメージに移ります。アップグレード可能 BIOS はキックスタート イメージを開始し、キックスタート イメージはシステム イメージを開始します。アップグレード可能 BIOS のチェックサムが有効でない場合は、ゴールデン BIOS がキックスタート イメージを開始し、キックスタート イメージがシステム イメージを開始します。

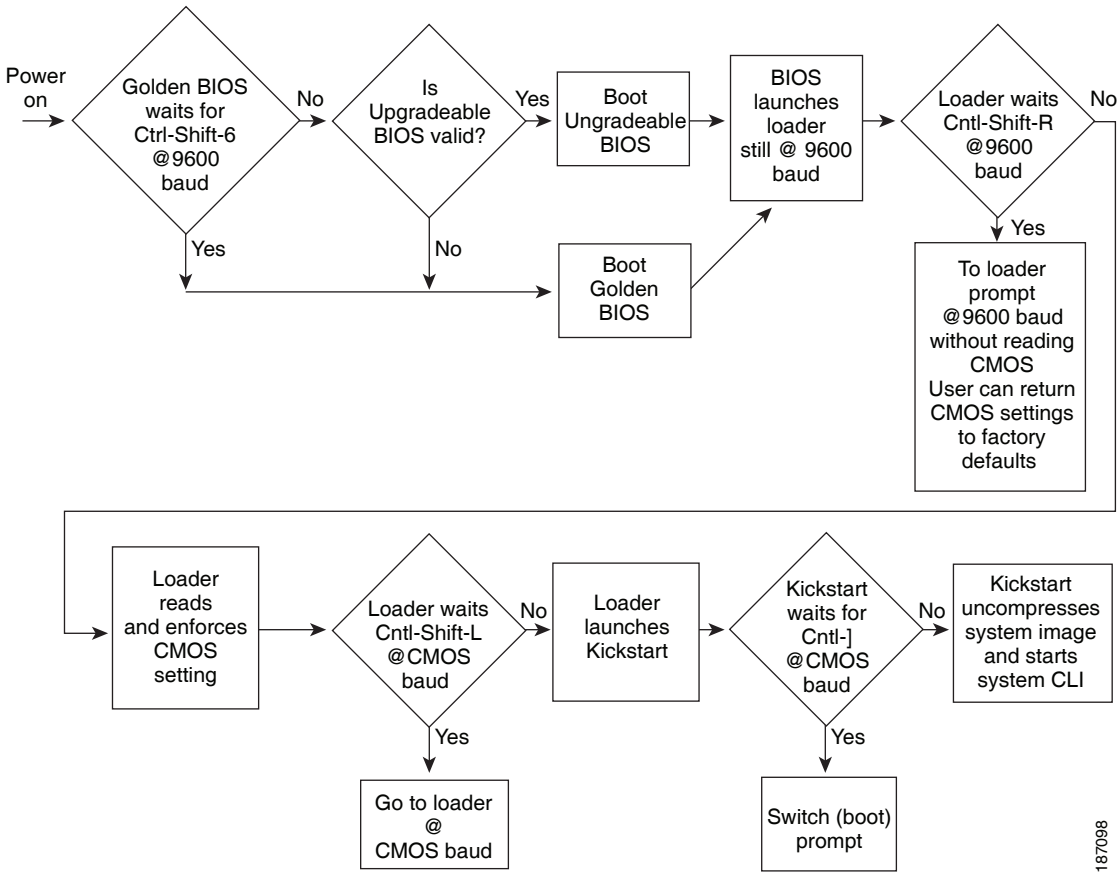
スイッチにアップグレード可能 BIOS を迂回させて、その代わりにゴールデン BIOS を使用させることができます。スイッチの電源を入れてから 2 秒以内に **Ctrl-Shift-6** を押すと、アップグレード可能 BIOS のチェックサムが有効であっても、ゴールデン BIOS が使用されてキックスタート イメージが開始されます。

（注）　**Ctrl-Shift-6** を押すときには、コンソール設定をデフォルトの 9600 ボー、8 データ ビット、パリティなし、1 ストップ ビットに設定する必要があります。

ブート シーケンスが始まる前に、BIOS はスイッチの内部テストを実行します。テストで不合格となった場合、ローダは制御を取得しません。その代わりに BIOS イメージが制御を保持し、30 秒ごとに 9600 ボーでコンソールにメッセージを出力して障害があることを示します。

図 3-1 に、正常なブート シーケンスおよび回復ブート シーケンスを示します。

図 3-1　　ブート シーケンス



回復手順の詳細については、第 50 章「トラブルシューティング」を参照してください。

コンソール設定

ローダ イメージ、キックスタート イメージ、システム イメージのデフォルト コンソール設定は次のとおりです。

- 速度:9600 ボー
- データビット:1 バイトごとに 8 ビット
- ストップビット:1 ビット
- パリティ:なし

この設定はスイッチに保存されており、3 つすべてのイメージは、保存されているコンソール設定を使用します。

コンソール設定を変更するには、コンフィギュレーション モードで **line console** コマンドを使用します。次の例ではライン コンソールを設定し、その端末ラインのオプションを設定しています。

```
switch# configure terminal
switch(config)# line console
switch(config-console)# databits 7
switch(config-console)# exec-timeout 30
switch(config-console)# parity even
switch(config-console)# stopbits 2
```

BIOS コンソール設定は変更できません。この設定は、デフォルトのコンソール設定と同じです。

スイッチのアップグレード

（注） network-admin ロールを持つユーザは、スイッチのソフトウェア イメージをアップグレードできます。

この項では、次のトピックについて取り上げます。

- アップグレード手順の概要（3-4 ページ）
- アップグレードの詳細手順（3-4 ページ）

アップグレード手順の概要

次の手順の概要では、スイッチ ソフトウェアのアップグレード方法について説明します。

ステップ 1　スーパーバイザ モジュールのコンソール ポートにログインします。

ステップ 2　Cisco.com にログインし、キックスタート イメージおよびシステム イメージをサーバにダウンロードします。

ステップ 3　**copy** コマンドを使用し、キックスタート イメージおよびシステム イメージをスイッチにダウンロードします。

ステップ 4　**install all** コマンドを使用し、イメージをインストールします。

注意　スイッチがインストールを実行している間、スイッチを通過するすべてのトラフィックは中断されます。

アップグレードの詳細手順

注意　Cisco Nexus 5000 シリーズ スイッチをアップグレードすると、スイッチを通過するすべてのトラフィックは中断されます。

スイッチのソフトウェアをアップグレードする手順は、次のとおりです。

ステップ 1　コンソール ポート接続でスイッチにログインします。

ステップ 2　Cisco.com にログインし、Software Download Center にアクセスします。Cisco.com にログインするには、http://www.cisco.com/ を表示してページ最上部の [Log In] をクリックします。シスコ ユーザ名およびパスワードを入力してください。

（注）　Cisco.com に登録していないユーザは、このマニュアルに記載されているリンクにアクセスできません。

ステップ 3　次の URL を使用し、Software Download Center にアクセスします。

http://www.cisco.com/kobayashi/sw-center/index.shtml

ステップ 4　Cisco Nexus 5000 シリーズ スイッチのソフトウェア ダウンロード ページに移動します。

スイッチのダウンロード イメージへのリンクが表示されます。

ステップ 5　関連イメージ ファイルのリリース ノートを参照します。

ステップ 6　キックスタート ソフトウェア ファイルおよびシステム ソフトウェア ファイルを選択し、サーバにダウンロードします。

ステップ 7　イメージ ファイルをコピーするために必要なスペースが bootflash: ディレクトリにあることを確認します。

```
switch# dir bootflash:
       5910     Jun 17 14:48:28 2008  config0617
        453     Jan 01 00:12:13 2005  ent-fm.lic
        453     Jan 01 20:50:55 2005  ent-fm123.lic
        453     Jan 01 20:58:49 2005  ent-fm123456.lic
        215     Jan 01 00:13:50 2005  enterprise.lic
        221     Jan 01 04:25:43 2005  eth-mod.lic
        219     Jan 01 04:26:14 2005  eth-port.lic
        216     Jan 01 00:21:48 2005  fc-feature.lic
      49152     Jul 28 09:42:51 2008  lost+found/
   21581824     Jul 08 10:11:14 2008  n5000-uk9-kickstart.4.0.0.N1.1.445.bin
   21573632     Jul 28 09:38:33 2008  n5000-uk9-kickstart.4.0.0.N1.1.47.bin
   20062208     Jul 28 09:43:05 2008  n5000-uk9-kickstart.4.0.0.N1.2.467.bin
   77139580     Jul 08 10:10:45 2008  n5000-uk9.4.0.0.N1.1.445.bin
   75270834     Jul 28 09:38:33 2008  n5000-uk9.4.0.0.N1.1.47.bin
   76924383     Jul 28 09:44:01 2008  n5000-uk9.4.0.0.N1.2.467.bin
       4096     Jan 01 00:07:37 2005  routing-sw/
       3697     Apr 30 14:53:07 2008  startup-config
       4096     Aug 08 12:49:09 2008  test/
          0     Jan 03 04:19:13 2005  thttpd_output
     782893     Jan 21 16:56:14 2005  zone-scale-config.out
     126927     Jan 21 16:55:45 2005  zoneset-scale-config.out

Usage for bootflash://sup-local
  855547904 bytes used
 6942613504 bytes free
 7798161408 bytes total
```

ヒント　新しいイメージ ファイルが正常にロードしない場合に使用できるように、最低でも 1 つ前のソフトウェア リリースのキックスタート イメージ ファイルおよびシステム イメージ ファイルを保存しておいてください。

ステップ 8　アクティブ スーパーバイザ モジュール ブートフラッシュにさらに多くのスペースが必要な場合、不要なファイルを削除して使用できるスペースを作ります。

```
switch# delete bootflash:n5000-uk9-kickstart.4.0.0.N1.1.445.bin
switch# delete bootflash:n5000-uk9.4.0.0.N1.1.445.bin
```

ステップ 9　転送プロトコルを使用し、キックスタート イメージおよびシステム イメージをスーパーバイザ モジュールのブートフラッシュにコピーします。**ftp:**、**tftp:**、**scp:**、または **sftp:** を使用できます。この手順の例では、**scp:** を使用しています。

```
switch# copy scp://user@scpserver.cisco.com//downloads/n5000-uk9-kickstart.4.0.0.N1.2.bin
bootflash:n5000-uk9-kickstart.4.0.0.N1.2.bin
switch# copy scp://user@scpserver.cisco.com//downloads/n5000-uk9.4.0.0.N1.2.bin
bootflash:n5000-uk9.4.0.0.N1.2.bin
```

ステップ 10　ステップ 9 でダウンロードした新しいイメージ名を指定し、新しいイメージをインストールします。

```
switch(config)# install all kickstart bootflash:n5000-uk9-kickstart.4.0.0.N1.2.bin system
bootflash:n5000-uk9.4.0.0.N1.2.bin
```

install コマンドは次の処理を実行します。

- 指定したイメージの互換性チェック（**show incompatibility** コマンドに相当）を実行します。互換性の問題がある場合はエラー メッセージが表示され、インストールは中断されます。
- 互換性チェックの結果を表示し、インストールを中断するかどうかを表示します。
- プロンプトが表示され、インストールの継続または中断を行うことができるようになります。

（注）　インストールを中断すると、スイッチの再起動中にトラフィックが中断されます。

- 指定イメージを参照するようにブート変数を更新し、スタートアップ コンフィギュレーション ファイルに設定を保存します。

ステップ 11　スイッチでインストールが完了したらログインし、必要なソフトウェア バージョンをスイッチが実行していることを確認します。

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2008, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software may be covered under the GNU Public
License or the GNU Lesser General Public License.A copy of
each such license is available at
http://www.gnu.org/licenses/gpl.html and
http://www.gnu.org/licenses/lgpl.html

Software
  BIOS:      version 1.2.0
  kickstart: version 4.0(0)N1(2)
  system:    version 4.0(0)N1(2)

  BIOS compile time:       2008/06/19
  kickstart image file is: bootflash:/n5000-uk9-kickstart.4.0.0.N1.2.467.bin
  kickstart compile time:  2008/07/28 2:00:00 [2008/07/28 9:41:24]
  system image file is:    bootflash:/n5000-uk9.4.0.0.N1.2.467.bin
  system compile time:     2008/07/28 2:00:00 [2008/07/28 10:09:17]
```

```
ハードウェア
  cisco Nexus5020 Chassis ("40x10GE/Supervisor")
  Intel(R) Celeron(R) M CPU   with 2074164 kB of memory.
  Processor Board ID JAB120600AY

  bootflash:  7864320 kB

nms-eugene-02   kernel uptime is 11 days 3 hours 15 minute(s) 19 second(s)

  Last reset at 63897 usecs after Mon Jul 28 09:46:39 2008
    Reason: Reset by installer
    System version: 4.0(0)N1(1)
    [Service]:
```

以前のリリースへのダウングレード

（注） ソフトウェア イメージをダウングレードできるのは、network-admin ロールに属するユーザだけです。

スイッチをダウングレードする手順はスイッチのアップグレードと同じですが、ロードするイメージ ファイルは、スイッチで現在実行しているイメージよりも前のリリースになります。

（注） 特定リリースにダウングレードする前に、スイッチにインストールされている現在のリリースのリリース ノートを確認し、ハードウェアにその特定リリースとの互換性があることを確認してください。

スイッチのソフトウェアをダウングレードする手順は、次のとおりです。

ステップ 1　**dir bootflash:** コマンドを入力し、ダウングレードに使用するイメージ ファイルを特定します。

イメージ ファイルがブートフラッシュ メモリに保存されていない場合は、Cisco.com からファイルをダウンロードします。ソフトウェア アップグレード手順の 1 ～ 9 を使用してください。

ステップ 2　新しいイメージをインストールします。

```
switch(config)# install all kickstart bootflash:n5000-uk9-kickstart.4.0.0.N1.1a.bin system
bootflash:n5000-uk9.4.0.0.N1.1a.bin
```

install all コマンドは次の処理を実行します。

- 指定したイメージの互換性チェック（**show incompatibility** コマンドに相当）を実行します。互換性の問題がある場合はエラー メッセージが表示され、インストールは中断されます。
- 互換性チェックの結果を表示し、インストールを中断するかどうかを表示します。
- プロンプトが表示され、インストールの継続または中断を行うことができるようになります。

（注） インストールを中断すると、スイッチの再起動中にトラフィックが中断されます。

- 指定イメージを参照するようにブート変数を更新し、スタートアップ コンフィギュレーション ファイルに設定を保存します。

ステップ 3　スイッチでインストールが完了したらログインし、必要なソフトウェア バージョンをスイッチが実行していることを確認します。

```
switch# show version
```

初期設定

ここでは、次の内容について説明します。

- 設定要件（3-8 ページ）
- 初期設定（3-9 ページ）
- スイッチの設定準備（3-9 ページ）
- デフォルトのログイン（3-9 ページ）
- スイッチの設定（3-10 ページ）
- 初期設定の変更（3-13 ページ）

設定要件

ハードウェア インストレーションに必要な作業が完了しているかどうかを次の手順で再確認してください。これらの作業を完了しないと、スイッチを設定できません。

次の手順を実行したあとに、スイッチを設定できます。

ステップ 1　新しい Cisco Nexus 5000 シリーズ スイッチの次の物理接続を確認します。

- コンピュータ端末（または端末サーバ）にコンソール ポートが物理的に接続されている。
- 管理イーサネット ポート（mgmt0）が外部のハブ、スイッチ、またはルータに接続されている

詳細については、該当する製品の『*Cisco Nexus 5000 シリーズ Hardware Installation Guide*』を参照してください。

ヒント　後で使用するためにホスト ID 情報を控えておいてください（たとえば、ライセンス機能をイネーブルにする場合など）。ホスト ID 情報は、スイッチに同梱されている Proof of Purchase 文書に記載されています。

ステップ 2　デフォルトのコンソール ポートのパラメータが、スイッチ コンソール ポートに接続されたコンピュータ端末（または端末サーバ）のパラメータと同じであることを確認します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

初期設定

Cisco Nexus 5000 シリーズ スイッチに初めてアクセスすると、セットアップ プログラムが実行され、イーサネット インターフェイス経由で通信するために必要な IP アドレスおよびその他の情報の入力を要求するプロンプトが表示されます。この情報は、スイッチを設定および管理するために必要です。

（注） IP アドレスは、CLI からだけ設定できます。スイッチの初回の起動時には、IP アドレスを割り当てる必要があります。この手順の実行後、コンソール ポートを介して Cisco MDS 9000 Family Fabric Manager からスイッチにアクセスできるようになります。

スイッチの設定準備

Cisco Nexus 5000 シリーズ スイッチを初めて設定する前に、次の情報を確認してください。

- 管理者パスワード。

（注） パスワードが弱い（短く、解読されやすい）場合、パスワード設定が拒否されます。必ず強固なパスワードを設定するようにしてください。

- 管理インターフェイスに IPv4 アドレスを使用する場合は、次の情報が必要です。
  - スイッチの管理インターフェイスの IPv4 サブネット マスク
  - デフォルト ゲートウェイの IPv4 アドレス（任意）
- スイッチの SSH サービス（任意）

  このサービスをイネーブルにするには、SSH のキー タイプ（dsa/rsa/rsa1）とキーのビット数（768 ～ 2048）を選択します。
- NTP サーバの IPv4 アドレス（任意）
- SNMP コミュニティ ストリング（任意）
- スイッチ名（任意）

  スイッチのプロンプトになります。
- 追加ログイン アカウントおよびパスワード（任意）

（注） IPv4 を使用する場合、SNMP アクセスを有効にするには、必ず IPv4 ルート、IPv4 デフォルト ネットワーク アドレス、および IPv4 デフォルト ゲートウェイ アドレスを設定してください。

デフォルトのログイン

スイッチには必ず、デフォルトのユーザであるネットワーク管理者（admin）が設定されています。デフォルトのユーザはどの時点でも変更できません。

デフォルトのパスワードはないので、強固なパスワードを明示的に設定する必要があります。パスワードが簡潔である場合（短く、解読しやすい場合）、パスワード設定は拒否されます。必ず強固なパスワードを設定するようにしてください。新しいパスワードを設定した後に忘れてしまった場合は、このパスワードを回復することもできます。

（注）　**write erase** コマンドを入力してスイッチをリロードした場合、設定手順を使用して、デフォルトのユーザ（admin）パスワードを再設定する必要があります。

スイッチの設定

ここでは、スイッチの初期設定の方法について説明します。

（注）　プロンプトで Ctrl+C キーを押すことによって、残りの設定オプションを省略し、この時点までの設定で先に進めます。管理者用の新規パスワードの入力は必須で、省略はできません。

ヒント　事前に設定された質問に応答しない場合、または任意の質問の回答を省略する場合は、Enter を押します。デフォルトの回答が見つからない場合（たとえば、スイッチ名）、スイッチは以前の設定を使用して、次の質問にスキップします。

スイッチを初めて設定する手順は、次のとおりです。

ステップ 1　スイッチの電源が入っていることを確認します。Cisco Nexus 5000 シリーズ のスイッチは自動的に起動します。

ステップ 2　管理者の新しいパスワードを入力します。

```
Enter the password for admin: password
```

ヒント　パスワードが弱い（短く、解読されやすい）場合、パスワード設定が拒否されます。必ず強固なパスワードを設定するようにしてください。パスワードでは大文字と小文字が区別されます。

ステップ 3　**yes** と入力すると、セットアップ モードが開始されます。

```
This setup utility will guide you through the basic configuration of
the system.Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present.So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog.Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes
```

セットアップ ユーティリティでは、手順に従って、基本的な設定プロセスを完了できます。どのプロンプトでも、Ctrl を押した状態で C を押すと、設定プロセスが終了します。

ステップ 4　管理者の新しいパスワードを入力します（デフォルトは admin）。

```
Enter the password for admin: admin
```

ステップ 5　**yes** と入力すると（デフォルトは no）、追加アカウントを作成できます。

```
Create another login account (yes/no) [n]: yes
```

初回のセットアップ時に、管理者のアカウントのほかにもう 1 つユーザ アカウント（network-admin ロール）を作成できます。デフォルトのロールおよび権限については、「RBAC の設定」セクション（22-5 ページ）を参照してください。

a. ユーザ ログイン ID を入力します。

```
Enter the user login ID: user_name
```

b. ユーザ パスワードを入力します。

```
Enter the password for user_name: user-password
```

ステップ 6　**yes** と入力して（デフォルトは yes）、読み取り専用の SNMP コミュニティ ストリングを作成します。

```
Configure read-only SNMP community string (yes/no) [n]: yes

SNMP community string: snmp_community
```

ステップ 7　スイッチの名前を入力します。

（注）　スイッチの名前は、英数字 32 文字以内で指定してください。デフォルトは **switch** です。

```
Enter the switch name: switch_name
```

ステップ 8　**yes** と入力し（デフォルトは yes）、帯域外管理を設定します。

```
Continue with Out-of-band (mgmt0) management configuration? [yes/no]: yes
```

a. mgmt0 の IPv4 アドレスを入力します。

```
Mgmt0 IPv4 address: ip_address
```

ステップ 9　**yes** と入力して（デフォルトは yes）、IPv4 デフォルト ゲートウェイを設定します（推奨）。

```
Configure the default-gateway: (yes/no) [y]: yes
```

a. デフォルト ゲートウェイの IPv4 アドレスを入力します。

```
IPv4 address of the default-gateway: default_gateway
```

ステップ 10　**yes** と入力して（デフォルトは yes）、Telnet サービスをイネーブルにします。

```
Enable the telnet service? (yes/no) [y]: yes
```

ステップ 11　**yes** と入力して（デフォルトは no）、SSH サービスをイネーブルにします。

```
Enabled SSH service? (yes/no) [n]: yes
```

ステップ 12　生成する SSH のキー タイプを入力します。

```
Type the SSH key you would like to generate (dsa/rsa/rsa1)? dsa
```

ステップ 13　指定範囲内でキーのビット数を入力します。

```
Enter the number of key bits? (768 to 2048): 768
```

ステップ 14　**yes** と入力して（デフォルトは no）、NTP サーバを設定します。

```
Configure NTP server? (yes/no) [n]: yes
```

a. NTP サーバの IPv4 アドレスを入力します。

```
NTP server IP address: ntp_server_IP_address
```

ステップ 15　**yes** と入力して（デフォルトは yes）、基本的なファイバ チャネル設定を設定します。

```
Enter basic FC configurations (yes/no) [n]: yes
```

ステップ 16　**shut** と入力して（デフォルトは shut）、デフォルトのファイバ チャネル スイッチ ポート インターフェイスを shut（ディセーブル）ステートに設定します。

```
Configure default physical FC switchport interface state (shut/noshut) [shut]: shut
```

ステップ 17　**on** と入力して（デフォルトは on）、スイッチ ポート トランク モードを設定します。

```
Configure default physical FC switchport trunk mode (on/off/auto) [on]: on
```

ステップ 18　**permit** と入力して（デフォルトは deny）、デフォルトのゾーン ポリシー設定を拒否します。

```
Configure default zone policy (permit/deny) [deny]: permit
```

デフォルト ゾーンのすべてのメンバへのトラフィック フローを許可します。

（注）　**write erase** コマンドを入力した後でセットアップ スクリプトを実行する場合、スクリプト終了後、次のコマンドを使用してデフォルトのゾーン ポリシーを明示的に変更し、VSAN（仮想 SAN）1 を許可する必要があります。

```
switch(config)# zone default-zone permit vsan 1
```

ステップ 19　**yes** と入力して（デフォルトは no）、フル ゾーン セット配信をイネーブルにします。

```
Enable full zoneset distribution (yes/no) [n]: yes
```

フル ゾーン セットの配信機能に対するスイッチ全体のデフォルトを上書きします。

新しい設定を参照します。ここまでに入力した設定を確認して修正します。

ステップ 20　設定に問題がなければ、**no** と入力します（デフォルトは no）。

```
The following configuration will be applied:
  username admin password <user-password> role network-admin
  snmp-server community snmp_community ro
  switchname switch
  telnet server enable
  ssh key dsa 768 force
  ssh server enable
  system default switchport shutdown san
  system default switchport trunk mode on
  system default zone default-zone permit
  system default zone distribute full

Would you like to edit the configuration? (yes/no) [n]: no
```

ステップ 21　**yes** と入力すると、この設定を保存して使用できます（デフォルトは yes）。

```
Use this configuration and save it? (yes/no) [y]: yes
```

注意　ここで、設定を保存しておかないと、次回のスイッチ再起動時に設定が更新されません。**yes** と入力して新しい設定を保存します。この操作によって、キックスタート イメージとシステム イメージも自動的に設定されます（「スイッチのイメージ ファイル」セクション（3-1 ページ）を参照）。

初期設定の変更

初期設定を後で変更する場合、EXEC モードで **setup** コマンドを入力します。

```
switch# setup

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system.Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present.So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog.Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes
```

セットアップ ユーティリティでは、手順に従って、基本的な設定プロセスを完了できます。

スイッチへのアクセス

初期設定のあと、次のように多くの方法でスイッチにアクセスできます。

- シリアル コンソール アクセス：シリアル ポート接続を使用して CLI にアクセスできます。
- アウトオブバンド アクセス：Telnet または SSH を使用して Cisco Nexus 5000 シリーズ スイッチにアクセスするか、Cisco MDS 9000 Fabric Manager アプリケーションを使用し、SNMP を使用してスイッチに接続します。

スイッチのその他の設定

この項では、次のトピックについて取り上げます。

- スイッチ名の割り当て（3-14 ページ）
- 日付、時刻、およびタイム ゾーンの設定（3-14 ページ）
- 夏時間への調整（3-15 ページ）

スイッチ名の割り当て

ネットワークの各スイッチには、一意の名前を付ける必要があります。物理的な位置、ネットワークのアソシエーションまたは配置された組織からスイッチを簡単に識別できる名前を割り当てることができます。割り当てられた名前は、コマンドライン プロンプトで表示されます。スイッチの名前は英数字 20 文字以内で指定してください。

（注）　このマニュアルでは、Cisco Nexus 5000 シリーズ スイッチを*スイッチ*として表し、switch# プロンプトを使用します。

スイッチ名を変更する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# switchname myswitch1` `myswitch1(config)#`	指定どおりにスイッチ名のプロンプトを変更します（myswitch1）。
ステップ 3	`myswitch1(config)# no switchname` `switch(config)#`	スイッチ名のプロンプトをデフォルト（switch#）に戻します。

日付、時刻、およびタイム ゾーンの設定

Cisco Nexus 5000 シリーズ スイッチは、GMT（グリニッジ標準時）と同一の UTC（協定世界時）を使用します。スイッチのデフォルトの時刻を変更する手順は、次のとおりです。

コマンド	目的
`switch# clock set HH:MM:SS DD Month YYYY`	スイッチのデフォルトの時刻を設定します。HH は 24 時間制の時（午後 3 時は 15）、MM は分（58）、SS は秒（09）、DD は日付（29）、Month は英単語の月（February）、YYYY は年（2008）を表します。

次の例ではスイッチの時刻が設定されます。

```
switch# clock set 15:58:09 29 February 2008
Mon Feb 20 15:58:09 UTC 2008
```

（注）　**clock** コマンドによる変更は、システムをリセットしても保存されます。

スイッチのタイム ゾーンを指定できます。夏時間機能なしのローカル タイムを指定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# clock timezone timezone hours_offset minutes_offset`	タイム ゾーンを設定します。timezone は 3 文字で表すタイム ゾーン（太平洋標準時は PST）、hours_offset は UTC からのオフセット（PST オフセットの場合は -8）を表します。minutes_offset は、ニューファンドランド標準時（NST）やインド標準時（IST）などのタイム ゾーンで必要となります。
ステップ 3	`switch(config)# exit`	EXEC モードに戻ります。
ステップ 4	`switch# show clock`	タイム ゾーンの設定を確認します。
ステップ 5	`switch# show run`	タイム ゾーン設定に加えられた変更とその他の設定情報を表示します。

次の例では、タイム ゾーンを Pacific Standard Time（PST）に設定し、UTC 時間からのオフセットをマイナス 8 時間と 0 分にします。

```
switch# configure terminal
switch(config)# clock timezone PST -8 0
```

ローカル時間設定をディセーブルにする手順は、次のとおりです。

`switch(config)# no clock timezone`	タイム ゾーン調整機能をディセーブルにします。

夏時間への調整

スイッチは夏時間へ調整するよう設定できます。デフォルトでは、Cisco NX-OS は自動的に夏時間に調整しません。したがって、スイッチを夏時間に調整するよう手動で設定する必要があります。

たとえば、米国標準（2005 年に成立した「エネルギー政策法」で定義）に従い、3 月の第 2 日曜日午前 2 時にスイッチのクロックを 1 時間進め、11 月の第 1 日曜日午前 2 時にまた 1 時間戻すといった調節を行います。または、開始日時、終了日時、毎年時間調整が繰り返されるか否かを明示的に指定できます。

夏時間調整をイネーブルにするには、次の手順を行います。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# clock summer-time` *`timezone start_week start_day start_month start_time end_week end_day end_month end_time offset`*	指定されたタイム ゾーンに夏時間を設定します。 開始および終了値は次のとおりです。 • 週の範囲は、1 ～ 5 です。 • 曜日の範囲は、Sunday から Saturday です。 • 月の範囲は、January から December です。 夏時間オフセットの範囲は 1 ～ 1440 分で、開始時間に追加され、終了時間で削除されます。
	`switch(config)# no clock summer-time`	夏時間調整機能をディセーブルにします。
ステップ 3	`switch(config)# exit` `switch#`	EXEC モードに戻ります。
ステップ 4	`switch# show running-config | include summer-time`	タイム ゾーンの設定を確認します。

次の例では、3 月第 2 日曜日の午前 2 時から 11 月第 1 日曜日午前 2 時までの期間、米国太平洋標準時のサマータイムを 60 分調節します。

```
switch# configure terminal
switch(config)# clock summer-time PDT 1 Sunday March 02:00 1 Sunday November 02:00 60
```

NTP 設定

ネットワーク タイム プロトコル（NTP）サーバは、ラジオ クロックまたは原子時計などの正確なタイム ソースをネットワーク装置のシステム クロックに同期化させます。NTP は、ユーザ データグラム プロトコル/IP 上でトランスポートされます。すべての NTP 通信は UTC を使用します。NTP サーバは、タイム サーバに接続されたラジオ クロックまたは原子時計などの基準タイム ソースから時刻を受け取ります。NTP はこの時刻をネットワーク全体に配信します。

ここでは、次の内容について説明します。

- NTP について（3-16 ページ）
- NTP 設定時の注意事項（3-17 ページ）
- NTP の設定（3-18 ページ）
- NTP CFS の配信（3-18 ページ）

NTP について

規模の大きい企業ネットワークでは、複数の装置間で記録される相互作用イベントのアソシエーションを試みる場合、すべてのネットワーク装置で 1 つの時間基準を持つことは、管理レポーティングおよびイベント ロギング機能において重要です。重要なネットワークを保有する多くの企業のお客様は、独自のストラタム 1 NTP ソースを保持しています。

クライアントとサーバ間で複数のフレームが交換されたときに時刻の同期化が行われます。クライアント モードにあるスイッチは、1 つまたは複数の NTP サーバのアドレスを認識します。NTP サーバはタイム ソースとして動作し、クライアントの同期要求を受け取ります。

ピアとして IP アドレスを設定し、スイッチは必要に応じて時刻を入手して提供できます。ピアでは、独自に時刻を提供することができ、サーバが設定されている場合も対応できます。これらの両方のインスタンスが別のタイム サーバに指定される場合、NTP サービスがより信頼性の高いものになります。アクティブ サーバ リンクが失われた場合でも、ピアの存在によって正確な時間を保つことができます。

ヒント　アクティブ サーバに障害が発生する場合、設定されたピアが NTP 時刻の提供に役立ちます。アクティブ サーバに障害が発生した場合のバックアップ サポートを確保するには、直接的な NTP サーバ アソシエーションを指定して、ピアを設定します。

ピアだけを設定すると、最も正確なピアが NTP サーバの役割を引き受け、他のピアがピアとして動作します。

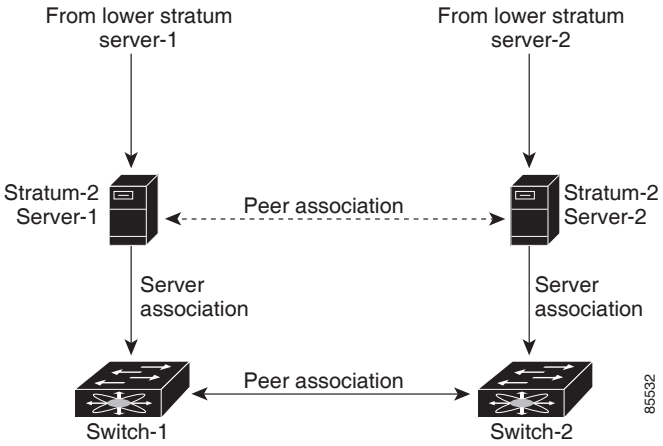
NTP 設定時の注意事項

すべての NTP 設定に次の注意事項が適用されます。

- 時計が信頼できる状態の場合にだけ、別のスイッチにピア アソシエーションを適用する必要があります(つまり、ユーザが信頼できる NTP サーバのクライアントである場合)。
- ピアだけが設定されている場合、そのピアがサーバの役割を引き受け、バックアップとして使用される必要があります。2 つのサーバが存在する場合、複数のスイッチが 1 つのサーバを指定し、残りのスイッチが別のサーバを指定するようにできます。この 2 つのセットの間でピア アソシエーションを設定すると、クロックの信頼性がさらに高まります。
- サーバが 1 つしかない場合は、すべてのスイッチがそのサーバに対してクライアント アソシエーションを持つことを推奨します。

ネットワーク内に適切に設定されているスイッチはサーバのダウンタイムにも影響されません。図 3-2 に、2 つの NTP ストラタム 2 サーバおよび 2 つのスイッチを含むネットワークを示します。

図 3-2　NTP のピアおよびサーバ アソシエーション



この設定では、スイッチは次のように設定されています。

- ストラタム 2 サーバ 1
  - IPv4 アドレス：10.10.10.10
  - ストラタム 2 サーバ 2
  - IPv4 アドレス：10.10.10.9
- スイッチ 1 の IPv4 アドレス - 10.10.10.1
- スイッチ 1 NTP コンフィギュレーション コマンド
  - **ntp server 10.10.10.10**
  - **ntp peer 10.10.10.2**
- スイッチ 2 の IPv4 アドレス - 10.10.10.2
- スイッチ 2 NTP コンフィギュレーション コマンド
  - **ntp server 10.10.10.9**
  - **ntp peer 10.10.10.1**

NTP の設定

IPv4 アドレス、IPv6 アドレス、またはドメイン ネーム サービス（DNS）名のいずれかを使用して NTP を設定できます。NTP アソシエーションを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configure terminal`**	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`ntp server`** {*ip-address* | *ipv6-address* | *dns-name*}	1 つのサーバと 1 つのサーバ アソシエーションを形成します。
ステップ 3	`switch(config)#` **`ntp peer`** {*ip-address* | *ipv6-address* | *dns-name*}	1 つのピアと 1 つのピア アソシエーションを形成します。複数のアソシエーションを指定できます。
ステップ 4	`switch(config)#` **`exit`**	EXEC モードに戻ります。
ステップ 5	`switch#` **`copy running-config startup-config`**	設定の変更内容を不揮発性 RAM（NVRAM）に保存します。 **ヒント**　これは、NTP 設定の変更結果の保存先の一例です。いつでもこのコマンドを入力できます。
ステップ 6	`switch#` **`show ntp peers`**	設定されたサーバおよびピア アソシエーションを表示します。

NTP CFS の配信

Cisco Fabric Services（CFS）を使用して、ファブリック内のすべての Cisco Nexus 5000 シリーズ スイッチに対して NTP ファブリック配信をイネーブルにできます。NTP 設定を実行し、配信がイネーブルにされている場合、サーバまたはピアの設定の全体がファブリック内のすべてのスイッチに配信されます。

スイッチで配信をイネーブルにしたあとで最初のコンフィギュレーション コマンドを入力すると、ファブリック全体のロックが自動的に有効になります。NTP アプリケーションは、有効データベースと保留データベース モデルを使用し、使用中のコンフィギュレーションに基づいてコマンドを格納または実行します。変更は保留データベースに格納され、有効データベースにコミットされます。

CFS アプリケーションの詳細については、「CFS について」セクション（21-1 ページ）を参照してください。

ここでは、次の内容について説明します。

- NTP 配信のイネーブル化（3-19 ページ）
- NTP 設定変更のコミット（3-19 ページ）
- NTP セッション ステータスの確認（3-20 ページ）
- データベース結合に関する注意事項（3-20 ページ）
- NTP セッション ステータスの確認（3-20 ページ）

NTP 配信のイネーブル化

NTP 設定ファブリックの配信をイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# ntp distribute`	NTP 設定の配信をファブリック内のすべてのスイッチでイネーブルにします。ファブリックのロックを取得して、その後の設定変更をすべて保留データベースに格納します。
	`switch(config)# no ntp distribute`	NTP 設定の配信をファブリック内のすべてのスイッチでディセーブル（デフォルト）にします。

NTP 設定変更のコミット

NTP 設定変更をコミットすると、有効なデータベースが保留中のデータベース内の設定変更によって上書きされて、ファブリック内のすべてのスイッチが同じ設定を受信します。セッション機能を実装しないで NTP 設定変更をコミットする場合、NTP 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。

NTP 設定変更をコミットする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# ntp commit`	NTP 設定変更をファブリック内のすべてのスイッチに配信し、ロックを解除します。保留データベースに対する変更を有効データベースに上書きします。

NTP 設定変更の廃棄

設定を変更したあとで、設定変更を廃棄したりコミットできます。いずれの場合でも、ロックは解除されます。

NTP 設定変更を廃棄する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# ntp abort`	保留中のデータベースの NTP 設定変更を廃棄し、ファブリック ロックを解除します。

ファブリック セッション ロックの解除

NTP ファブリック作業を実行して、変更のコミットまたは廃棄を行ってロックを解除するのを忘れた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこの操作を行うと、ユーザによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。

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

管理者権限を使用して、ロックされた NTP セッションを解除するには、**clear ntp session** コマンドを使用します。

```
switch# clear ntp session
```

データベース結合に関する注意事項

2 つのファブリックを結合する場合は、次の注意事項に従ってください。

- 結合とは、ファブリック内の各スイッチの既存および受信されたデータベースの合体を意味していることを認識しておいてください。
- IP アドレスを 1 つのスイッチ上のサーバとして、また別のスイッチのピアとして設定しないでください。この設定が存在すると、結合が失敗する可能性があります。
- データベースの合体が 64 の最大数を超えていないかどうか確認します。

NTP セッション ステータスの確認

NTP セッションのステータスを確認するには、**show ntp session-status** コマンドを使用します。

```
switch# show ntp session-status
last-action : Distribution Enable    Result : Success
```

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は、同時に複数の Telnet または SNMP セッションを許可します。スイッチは、管理インターフェイス（mgmt0）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まず一部の IP パラメータを設定しておく必要があります。CLI から手動で管理インターフェイスを設定できます。

ここでは、次の内容について説明します。

- mgmt0 インターフェイスの概要（3-21 ページ）
- 管理インターフェイスの設定（3-21 ページ）
- 管理インターフェイスの設定の表示（3-22 ページ）
- 管理インターフェイスのシャットダウン（3-22 ページ）

mgmt0 インターフェイスの概要

Cisco NX-OS デバイス上の mgmt0 インターフェイスではアウトオブバンド管理を行え、IPv4 アドレスまたは IPv6 アドレスでデバイスを管理できます。mgmt0 インターフェイスは 10/100/1000 イーサネットを使用します。

（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。

管理インターフェイスの設定

管理（mgmt0）イーサネット インターフェイスを設定して IP 上で接続する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface mgmt 0`	スイッチの管理イーサネット インターフェイスを選択し、インターフェイス コンフィギュレーション サブモードを開始します。
ステップ 3	`switch(config-if)# ip address ipv4-address[/length]`	IPv4 アドレスとそのサブネット マスクを設定します。
	`switch(config-if)# ip address ipv4-address [subnet-mask]`	IPv4 アドレスとそのサブネット マスクを設定するもう 1 つの方法です。
	`switch(config-if)# ipv6 address ipv6-address[/length]`	IPv6 アドレスとそのサブネット マスクを設定します。
ステップ 4	`switch(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 5	`switch(config-if)# exit`	コンフィギュレーション モードに戻ります。
ステップ 6	`switch(config)# vrf context management`	VRF コンテキスト管理コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 7	switch(config-vrf)# **ip route** *ipv4-prefix*[/*length*] *ipv4-nexthop-address*	ネクスト ホップの IPv4 アドレスを設定します。
	switch(config-vrf)# **ipv6 route** *ipv6-prefix*[/*length*] *ipv6-nexthop-address*	ネクスト ホップの IPv6 アドレスを設定します。
ステップ 8	switch(config-vrf)# **exit**	EXEC モードに戻ります。
ステップ 9	switch# **copy running-config startup-config**	(任意)ファイル システムへの設定の変更を保存します。

スイッチ インターフェイスが管理上のシャットダウン状態である場合があります。**show interface mgmt 0** コマンドを使用して、いつでもインターフェイスのステータスを確認できます。

管理インターフェイスの設定の表示

管理インターフェイスの設定を表示するには、**show interface mgmt 0** コマンドを使用します。

```
switch# show interface mgmt0
mgmt0 is up
    Hardware is GigabitEthernet, address is 000d.ec8f.cb00 (bia 000d.ec8f.cb00)
    Internet Address is 172.16.131.202/24
    MTU 1500 bytes, BW 0 Kbit, DLY 0 usec,
       reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA
    full-duplex, 1000 Mb/s
    Input flow-control is off, output flow-control is off
    8540 packets input, 2835036 bytes
    5202 multicast frames, 0 compressed
    0 input errors, 0 frame, 0 overrun, 0 fifo
    570 packets output, 85555 bytes
    0 underrun, 0 output errors, 0 collisions
    0 fifo, 0 carrier errors
switch#
```

管理インターフェイスのシャットダウン

管理インターフェイス(mgmt0)をシャットダウンするには、**shutdown** コマンドを使用します。システム プロンプトにより、コマンドの実行前に処理を確認するように要求されます。**force** オプションを使用して、この確認を省略できます。次に、**force** オプションを使用せずに、管理インターフェイスをシャットダウンする例を示します。

```
switch# configure terminal
switch(config)# interface mgmt 0
switch(config-if)# shutdown
Shutting down this interface will drop all telnet sessions.
Do you wish to continue (y/n)? y
```

次に、**force** オプションを使用して、管理インターフェイスをシャットダウンする例を示します。

```
switch# configure terminal
switch(config)# interface mgmt 0
switch(config-if)# shutdown force
```

スイッチ コンフィギュレーションの管理

この項では、次のトピックについて取り上げます。

- スイッチ コンフィギュレーションの表示（3-23 ページ）
- コンフィギュレーションの保存（3-23 ページ）
- コンフィギュレーションのクリア（3-23 ページ）

スイッチ コンフィギュレーションの表示

必要に応じて、コンフィギュレーション ファイルを ASCII 形式で表示できます。EXEC プロンプトから現在の設定ツリーを表示させるには、**show running-config** コマンドを入力します。実行コンフィギュレーションがスタートアップ コンフィギュレーションと異なり、また再起動後に **copy running-config startup-config** コマンドを入力していない場合、**show startup-config** コマンドを入力して、スイッチの起動に使用された現在のスタートアップ コンフィギュレーションの ASCII バージョンを表示します。現在のスタートアップ コンフィギュレーションの内容を表示するには、**show startup-config** コマンドを使用します。

また、スイッチ全体の特定の情報を収集するには、それに関連する **show** コマンドを入力します。指定した機能、インターフェイス、モジュール、または VSAN に基づいてコンフィギュレーションが表示されます。各機能に対して使用できる **show** コマンドをここで簡単に説明し、さらに各章の最後に一覧表示しています。

コンフィギュレーションの保存

不揮発性ストレージに新しいコンフィギュレーションを保存するには、**copy running-config startup-config** コマンドを使用します。このコマンドを入力すると、実行中および起動時の設定が同一の内容になります。

コンフィギュレーションのクリア

スタートアップ コンフィギュレーションをクリアするには、**write erase** コマンドを使用します。このコマンドを実行すると、スイッチのスタートアップ コンフィギュレーションが工場出荷時（デフォルト）の状態に戻ります。実行コンフィギュレーションに影響はありません。

注意　**write erase** コマンドは起動時の設定を、ローダ機能に影響する設定以外、すべて削除します。

write erase boot コマンドは、ローダ機能に影響する設定だけを削除します。ローダ機能コンフィギュレーションには、ブート変数と mgmt0 IP コンフィギュレーション情報（IP アドレス、ネットマスク、デフォルト ゲートウェイ）が含まれています。

```
switch# write erase boot
```

このコマンドにより、インターフェイス mgmt0 のブート変数および IP 設定が削除されます。

スイッチ ファイル システムの使用

この項では、次のトピックについて取り上げます。

- カレント ディレクトリの設定（3-24 ページ）
- カレント ディレクトリの表示（3-24 ページ）
- ディレクトリ内のファイルの一覧表示（3-25 ページ）
- ディレクトリの作成（3-25 ページ）
- 既存のディレクトリの削除（3-25 ページ）
- ファイルの移動（3-26 ページ）
- ファイルのコピー（3-26 ページ）
- ファイルの削除（3-26 ページ）
- ファイル内容の表示（3-27 ページ）
- コマンド出力のファイルへの保存（3-27 ページ）
- ファイルの圧縮および圧縮解除（3-27 ページ）

カレント ディレクトリの設定

cd コマンドを使用することで、カレント ディレクトリ レベルを指定のディレクトリ レベルに変更できます。CLI のデフォルトでは、volatile: ファイル システムになります。このコマンドにはディレクトリ名を入力する必要があります。

volatile: ファイル システムに保存されているファイルは、スイッチの再起動時に削除されます。

このコマンドの構文は、**cd** *directory name* です。

次に、bootflash: ファイル システム上のルート ディレクトリにカレント ディレクトリを変更する例を示します。

```
switch# cd bootflash:
```

次に、カレント ディレクトリにある mystorage ディレクトリをカレント ディレクトリにする例を示します。

```
switch# cd mystorage
```

カレント ディレクトリの表示

pwd コマンドを使用して、カレント ディレクトリの場所を表示します。次に、ディレクトリを変更し、カレント ディレクトリを表示する例を示します。

```
switch# cd bootflash:
switch# pwd
bootflash:
```

ディレクトリ内のファイルの一覧表示

dir コマンドを使用して、カレント ディレクトリ、または指定のディレクトリの内容を表示します。このコマンドの構文は、**dir** *directory* または **dir** *filename* です。

次に、デフォルトの volatile: ファイル システム上にあるファイルを一覧表示する例を示します。

```
switch# dir
          Usage for volatile: filesystem
                        0 bytes total used
                 20971520 bytes free
                 20971520 bytes available
```

ディレクトリの作成

mkdir コマンドを使用することで、カレント ディレクトリ レベルまたは指定のディレクトリ レベルに、新しいディレクトリを作成できます。

このコマンドの構文は、**mkdir** *directory name* です。

次に、bootflash: ディレクトリに新しいディレクトリ test を作成する例を示します。

```
switch# mkdir bootflash:test
```

次に、カレント ディレクトリ レベルに新しいディレクトリ test を作成する例を示します。

```
switch# mkdir test
```

既存のディレクトリの削除

rmdir コマンドを使用すると、カレント ディレクトリ レベルまたは指定のディレクトリ レベルで、既存のディレクトリを削除できます。削除対象のディレクトリは空である必要があります。

このコマンドの構文は、**rmdir** *directory name* です。

次に、bootflash ディレクトリにあるディレクトリ test を削除する例を示します。

```
switch# rmdir bootflash:test
This is a directory.Do you want to continue (y/n)?  [y] y
```

delete コマンドでは、空のディレクトリおよび空でないディレクトリも削除できます。このコマンドを入力する場合、ディレクトリを削除する意思を確認する警告が表示されます。

次に、カレント ディレクトリ レベルにある test ディレクトリを削除する例を示します。

```
switch# delete test
This is a directory.Do you want to continue (y/n)?  [y] y
```

カレント ディレクトリが bootflahs:mydir である場合、このコマンドでは bootflash:mydir/test ディレクトリが削除されます。

ファイルの移動

move コマンドを使用することで、ソース ディレクトリからファイルを削除し、宛先ディレクトリにそのファイルを配置することができます。

注意　宛先ディレクトリに同名のファイルがすでに存在する場合は、そのファイルは移動対象のファイルによって上書きされます。

次に、samplefile というファイルをルート ディレクトリから mystorage ディレクトリに移動する例を示します。

```
switch# move bootflash:samplefile bootflash:mystorage/samplefile
```

次に、カレント ディレクトリ レベルからファイルを移動する例を示します。

```
switch# move samplefile mystorage/samplefile
```

カレント ディレクトリが bootflash:mydir の場合、このコマンドは bootflash:mydir/samplefile を bootflash:mydir/mystorage/samplefile に移動します。

ファイルのコピー

スイッチ内のファイル システム間でファイルをコピーするには、**copy** コマンドを使用します。

（注）　**dir** コマンドを使用して、コピー先のファイル システムに十分な領域があることを確認します。十分な領域が残っていない場合は、**delete** コマンドを使用して不要なファイルを削除します。

次に、samplefile というファイルをルート ディレクトリから mystorage ディレクトリにコピーする例を示します。

```
switch# copy bootflash:samplefile bootflash:mystorage/samplefile
```

次に、カレント ディレクトリ レベルからファイルをコピーする例を示します

```
switch# copy samplefile mystorage/samplefile
```

カレント ディレクトリが bootflash:mydir の場合、このコマンドは bootflash:mydir/samplefile を bootflash:mydir/mystorage/samplefile にコピーします。

ファイルの削除

delete コマンドは、指定したファイル、または指定したディレクトリとその内容を削除します。

次に、現在の作業ディレクトリからファイルを削除する例を示します。

```
switch# delete dns_config.cfg
```

次に、bootflash全体（ディレクトリおよびそのすべての内容）を削除する例を示します。

```
switch# delete bootflash:my-dir
```

注意　1 つのディレクトリを指定している場合、**delete** コマンドではディレクトリ全体とその内容すべてが削除されます。

ファイル内容の表示

show file コマンドを使用して、ファイル システム上の指定のファイルの内容を表示できます。

次に、カレント ディレクトリにあるファイルの内容を表示する例を示します。

```
switch# show file myfile
```

コマンド出力のファイルへの保存

スクリーンに表示される出力結果をすべてファイルに保存するには、コマンドの後ろに > *filename* を指定します。たとえば、EXEC モードのスイッチ プロンプトで **show interface > samplefile** と入力すると、同じディレクトリ レベルに作成された samplefile にインターフェイス コンフィギュレーションが保存されます。EXEC モード スイッチ プロンプトで **dir** コマンドを入力すると、最近保存した *samplefile* をはじめ、このディレクトリにあるすべてのファイルが表示されます。

ファイルの圧縮および圧縮解除

gzip コマンドは、指定のファイルを LZ77 コーディングで圧縮（zip）します。

次に、**show tech-support** コマンドの出力結果をファイル（Samplefile）に出力してそのファイルを zip 圧縮し、volatile: ディレクトリでの消費容量の違いを表示させる例を示します。

```
switch# show tech-support > Samplefile
Building Configuration ...
switch# dir
    1525859     Jul 04 00:51:03 2003 Samplefile
Usage for volatile://
    1527808 bytes used
   19443712 bytes free
   20971520 bytes total
switch# gzip volatile:Samplefile
switch# dir
     266069     Jul 04 00:51:03 2003 Samplefile.gz
Usage for volatile://
     266240 bytes used
   20705280 bytes free
   20971520 bytes total
```

gunzip コマンドは、LZ77 コーディングされたファイルを圧縮解除（unzip）します。

次に、前回の例で圧縮されたファイルを圧縮解除する例を示します。

```
switch# gunzip samplefile
switch# dir
    1525859     Jul 04 00:51:03 2003 Samplefile
Usage for volatile://
    1527808 bytes used
   19443712 bytes free
   20971520 bytes total
```

CHAPTER 4

ライセンスの管理

この章では、Cisco Nexus 5000 シリーズ スイッチでライセンスを管理する方法について説明します。

ライセンスによって、適切なライセンスをインストールしたあと、スイッチの指定されたプレミアム機能へのアクセスが可能になります。この章では、Cisco NX-OS ソフトウェアのライセンスタイプ、オプション、手順、インストール、および管理について説明します。

この章は、次の項で構成されています。

- ライセンス用語(4-1 ページ)
- ライセンス モデル(4-2 ページ)
- ライセンスのインストール(4-3 ページ)
- ライセンス キー ファイルの取得(4-4 ページ)
- ライセンス キー ファイルのインストール(4-5 ページ)
- ライセンス ファイルのバックアップ(4-6 ページ)
- 使用中のライセンス機能の識別(4-6 ページ)
- ライセンスのアンインストール(4-7 ページ)
- ライセンスの更新(4-8 ページ)
- 猶予期間のアラート(4-9 ページ)
- スイッチ間のライセンスの移動(4-10 ページ)
- ライセンスの設定の確認(4-10 ページ)

ライセンス用語

この章では次の用語を使用します。

- ライセンス機能:特定の機能をライセンス ファイル、ハードウェア オブジェクト、または適法契約を介して使用するためのアクセス権。このアクセス権は、ユーザ数、インスタンス数、タイム スパン、および実装されたスイッチに制限されます。
- ライセンス対象アプリケーション:使用するのにライセンスを必要とするソフトウェア機能
- ライセンスの実施:ライセンスを取得していない場合に機能の使用を禁止するメカニズム
- ノードロック ライセンス:スイッチの一意のホスト ID を使用した特定のスイッチだけで使用できるライセンス。
- ホスト ID:各 スイッチ固有の一意なシャーシ シリアル番号。

- Proof of Purchase（購入証明書）：記載された 1 台のスイッチ上で、ライセンス機能を使用する権限を持つ所有者であることを認定する文書。Proof of Purchase 文書は Claim Certificate（権利証明書）とも呼ばれます。
- Product Authorization Key（PAK）：PAK を使用して、Proof of Purchase 文書に掲載されたサイトの 1 つからライセンス キーを入手できます。指定された Web サイトで登録した後、E メールでライセンス キー ファイルとインストールの説明を受け取ります。
- ライセンス キー ファイル：ライセンス機能を明記するスイッチ固有の一意のファイル。各ファイルには、改ざんと変更を防ぐためにデジタル署名が含まれます。ライセンス機能を使用するためには、ライセンス キーが必要です。ライセンス キーは、指定された期間内で効力を発します。
- ライセンスの欠落：ブートフラッシュが破損した場合、またはライセンスのインストール後にスーパバイザ モジュールを交換した場合、そのライセンスは「missing」として示されます。この機能は引き続き機能しますが、ライセンス数が正しくありません。できるだけ早くライセンスを再インストールする必要があります。
- 差分ライセンス：最初のライセンス ファイルになかった追加のライセンス機能。ライセンス キーは追加可能です。一部の機能を現在購入して、あとでさらに購入する場合は、ライセンス ファイルとソフトウェアが指定されたスイッチのすべての機能数の合計を検出します。
- 評価ライセンス：一時的なライセンス。評価ライセンスは期限付きで（指定された日数有効）、ホスト ID（スイッチのシリアル番号）には関連しません。
- 永久ライセンス：期限が定められていないライセンスを、永久ライセンスといいます。
- 猶予期間：ライセンスがなくてもライセンス パッケージ内の機能が引き続き使用できる期間
- サポート：シスコのサポートをシスコのリセラーからご購入された場合は、リセラーに直接お問い合わせください。サポートをシスコから直接ご購入された場合は、次の URL にある Technical Assistance Center（TAC）にご連絡ください。

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

ライセンス モデル

Cisco NX-OS ソフトウェアのライセンス モデルは機能ベースです。機能ベース ライセンスでは、物理スイッチ全体で機能が使用可能になります。表 4-1 に、機能ベース ライセンス パッケージの一覧を示します。

（注）　ストレージ サービス ライセンス パッケージに含まれないすべての機能は Cisco NX-OS ソフトウェアにバンドルされ、追加料金なしでスイッチ ハードウェアで提供されます（表 4-1 のベース サービス パッケージを参照）。

表 4-1　機能ベースのライセンス

機能ライセンス	機能
ベース サービス パッケージ N5000-AS	このパッケージは、追加料金なしでスイッチ ハードウェアに組み込まれています。ストレージ サービス パッケージに明示的に含まれている機能を除く、すべてのイーサネット機能およびシステム機能が含まれます。

表 4-1　機能ベースのライセンス（続き）

機能ライセンス	機能
ストレージ サービス パッケージ N5020-SS	• 1 つの NX5020 システム用に次のサービスが含まれます。 • ネイティブ ファイバ チャネル • FCoE • NPV • FC ポート セキュリティ • ファブリック バインディング
Advanced Services パッケージ N5000-AS	• 今後のリリースで利用可能になります。

ライセンスのインストール

プレインストール ライセンスを取得するか（スイッチの新規発注だけに適用）、ライセンスを手動でインストールできます（ネットワークの既存スイッチに適用）。

この項では、次のトピックについて取り上げます。

- プレインストール ライセンスの入手（4-3 ページ）
- 手動インストールの実行（4-4 ページ）

プレインストール ライセンスの入手

新しい Cisco Nexus 5000 シリーズ スイッチのプレインストール ライセンスを入手できます。

プレインストール ライセンスを取得する手順は、次のとおりです。

ステップ 1　製品を購入されたリセラーまたは代理店に連絡して、このサービスを要求してください。

（注）　シスコのサポートをシスコのリセラーからご購入された場合は、リセラーに直接お問い合わせください。サポートをシスコから直接ご購入された場合は、次の URL にある Technical Assistance Center（TAC）にご連絡ください。

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

必要なライセンスがシステムにインストールされてスイッチが出荷されています。Proof of Purchase 文書は、スイッチと一緒に送られます。

ステップ 2　今後使用するために、Proof of Purchase 文書からホスト ID を入手します。

これでスイッチおよびライセンス機能の使用を開始できるようになりました。

手動インストールの実行

すべてのCisco Nexus 5000 シリーズ ライセンスはプレインストール済みです。手動インストールは不要です。

ライセンス キー ファイルの取得

新規ライセンス キー ファイルまたは更新ライセンス キー ファイルを取得する手順は、次のとおりです。

ステップ 1　**show license host-id** コマンドを使用して、スイッチのシリアル番号を取得します。ホスト ID は、スイッチのシリアル番号ともいいます。

```
switch# show license host-id
License hostid: VDH=FOX064317SQ
```

ヒント　コロン(:)記号の後に表示される ID 全体を使用します。この例では、ホスト ID は VDH=FOX064317SQ です。

ステップ 2　Claim Certificate または Proof of Purchase 文書を入手します。この文書は、すべての Cisco Nexus 5000 シリーズ スイッチに添付されています。

ステップ 3　Claim Certificate または Proof of Purchase 文書から PAK を取得します。

ステップ 4　Claim Certificate または Proof of Purchase 文書から Web サイト URL を検索します。

ステップ 5　スイッチに該当する指定された URL にアクセスし、スイッチのシリアル番号と PAK を入力します。

ライセンス キー ファイルは、E メールによって送信されます。ライセンス キー ファイルは、要求されたスイッチの使用だけを認証するためにデジタル署名されています。指定されたスイッチの Cisco NX-OS ソフトウェアがライセンス キー ファイルにアクセスすると、要求された機能もイネーブルになります。

注意　ライセンス キー ファイルは変更を加えずに、指定された Cisco Nexus 5000 シリーズ スイッチにインストールしてください。

ライセンスは、永久のものと、確定日に終了するもののどちらかとなります。ライセンスを所有しない場合、ライセンスによって提供される機能を初めて使用したときからその機能の使用猶予期間が開始します(「猶予期間のアラート」セクション(4-9 ページ)を参照)。

ステップ 6　EXEC モードで **copy licenses** コマンドを使用して、ライセンス ファイルを 2 つの保存場所、bootflash: ディレクトリまたは volatile: ディレクトリのどちらかに保存します(「ライセンス ファイルのバックアップ」セクション(4-6 ページ)を参照)。

ライセンス キー ファイルのインストール

ヒント　任意のスイッチで複数のライセンスをインストールする必要がある場合は、各ライセンス キー ファイルに一意のファイル名を割り当ててください。

任意のスイッチにライセンス キー ファイルをインストールする手順は、次のとおりです。

ステップ 1　アクティブ スーパーバイザのコンソール ポートを介してスイッチにログインします。

ステップ 2　スイッチ コンソールからアクティブ スーパーバイザ モジュールで **install license** コマンドを入力してインストールを実行します。

```
switch# install license bootflash:license_file.lic
Installing license ..done
```

（注）　ライセンス キー ファイルにターゲット名を指定する場合、ファイルは指定された名前でインストールされます。そうしない場合、ライセンス キー ファイルに指定されたファイル名がライセンスのインストールに使用されます。

ステップ 3　**copy licenses** コマンドを使用して、bootflash: にライセンス ファイルのバックアップを .tar ファイルで作成します。

```
switch# copy licenses bootflash:/Enterprise.tar
Backing up license done
```

ステップ 4　スイッチ コンソールを終了し、**show license** コマンドを使用してスイッチにインストールされたすべてのライセンス ファイルを表示するために新しい端末セッションを開きます。

```
switch# show license
Enterprise.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT ENTERPRISE_PKG cisco 1.0 permanent uncounted \
        HOSTID=VDH=FOX0646S017 \
        NOTICE="<LicFileID></LicFileID><LicLineID>0</LicLineID> \
        <PAK>dummyPak</PAK>" SIGN=EE9F91EA4B64
```

（注）　**install license** コマンドが入力されたときにライセンスがすべてのガイドラインを満たしている場合、設定どおりにすべての機能とモジュールが機能を続行します。

show license brief コマンドを使用して、スイッチにインストールしたライセンス ファイルのリストを表示できます。

```
switch# show license brief
Enterprise.lic
FibreChannel.lic
```

show license file コマンドを使用して、スイッチにインストールした特定ライセンス ファイルに関する情報を表示できます。

```
switch# show license file Enterprise.lic
Enterprise.lic:
SERVER this_host ANY
VENDOR cisco
```

```
INCREMENT ENTERPRISE_PKG cisco 1.0 permanent uncounted \
        HOSTID=VDH=FOX0646S017 \
        NOTICE="<LicFileID></LicFileID><LicLineID>0</LicLineID> \
        <PAK>dummyPak</PAK>" SIGN=EE9F91EA4B64
```

ライセンス ファイルのバックアップ

インストールされたすべてのライセンス ファイルは、ユーザ指定の場所に. tar ファイルでバックアップできます。EXEC モードで **copy licenses** コマンドを使用して、ライセンス ファイルを 2 つの保存場所、bootflash: または volatile: のどちらかに保存します。次の例では、すべてのライセンスを Enterprise.tar ファイルに保存します。

```
switch# copy licenses bootflash:/Enterprise.tar
Backing up license done
```

ヒント　ライセンス ファイルのインストールが終わったらすぐにファイルをバックアップしておき、**write erase** コマンドを実行する前にもバックアップすることを推奨します。

注意　既存のライセンスを消去した場合、**install license** コマンドを使用して再インストールできます。

使用中のライセンス機能の識別

Cisco NX-OS ソフトウェア機能をイネーブルにすると、ライセンス猶予期間が起動する場合があります。特定のライセンスに対してアクティブな機能を識別するには、**show license usage** *license-name* コマンドを使用します。

```
switch# show license usage FC_FEATURES_PKG
アプリケーション
-----------
PFM
-----------
```

show license usage コマンドを使用して、スイッチ上のすべてのアクティブな機能を識別します。

```
switch# show license usage
Feature                      Ins  Lic   Status Expiry Date Comments
                                 Count
--------------------------------------------------------------------------------
FM_SERVER_PKG                 No    -   Unused             -
ENTERPRISE_PKG                No    -   In use             Grace 119D 23H
FC_FEATURES_PKG               Yes   -   In use never       -
--------------------------------------------------------------------------------
```

ライセンスのアンインストール

未使用の永久ライセンスだけをアンインストールできます。現在使用されている永久ライセンスを削除しようとすると、ソフトウェアは要求を拒否し、エラー メッセージを表示します。未使用ライセンスをアンインストールすると、猶予期間が始まります。猶予期間は、ライセンスなしで機能を最初に使用したときから測定され、有効なライセンス ファイルがインストールされるとリセットされます。

（注） 永久ライセンスが使用されている場合は、アンインストールできません。永久ライセンスによって有効になっている機能をまずディセーブルにしてから、ライセンスをアンインストールする必要があります。

ヒント 評価ライセンスを使用していて、新規の永久ライセンスをインストールする場合は、評価ライセンスが終了する前にサービスを中断させることなく行うことができます。評価ライセンスを削除すると、サービスを中断させることなく猶予期間がすぐに始まります。

注意 関連した機能をディセーブルにしてから、ライセンスをアンインストールします。ライセンスが使用されている場合、削除手順は失敗します。

ライセンスをアンインストールする手順は、次のとおりです。

ステップ 1 **copy** コマンドを使用してリモート サーバに実行コンフィギュレーションを保存します（第 3 章「スイッチの設定」を参照）。

ステップ 2 EXEC モードで **show license brief** コマンドを入力して、インストールされたすべてのライセンス キー ファイルのリストを表示し、アンインストールするファイルを指定します。この例では、アンインストールするファイルは FibreChannel.lic です。

```
switch# show license brief
Enterprise.lic
FibreChannel.lic
```

ステップ 3 アンインストールするライセンスによって提供された機能をディセーブルにします。**show license usage** *package_name* コマンドを入力して、指定されたパッケージでイネーブルにされている機能を表示します。

```
switch# show license usage FC_FEATURES_PKG
アプリケーション
-----------
PFM
-----------
```

ステップ 4 **clear license** *filename* コマンドを使用して FibreChannel.lic ファイルをアンインストールします。ここでは、*filename* は、インストールされたライセンス キー ファイルの名前です。

```
switch# clear license FibreChannel.lic
Clearing license FibreChannel.lic:
SERVER this_host ANY
VENDOR cisco
```

ステップ 5 **yes** と入力して（yes がデフォルト）、ライセンスの更新を続けます。

```
Do you want to continue? (y/n) y
```

```
Clearing license ..done
```

これで FibreChannel.lic ライセンス キー ファイルはアンインストールされました。

ライセンスの更新

期間の制約があるライセンスは、更新ライセンスを取得してインストールする必要があります。テクニカル サポートに連絡のうえ、更新ライセンスを要求してください。

（注）シスコのサポートをシスコのリセラーからご購入された場合は、リセラーに直接お問い合わせください。サポートをシスコから直接ご購入された場合は、次の URL にある Technical Assistance Center（TAC）にご連絡ください。

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

ライセンスを更新する手順は、次のとおりです。

ステップ 1　「ライセンス キー ファイルの取得」セクション（4-4 ページ）の説明に従って、更新ライセンス ファイルを取得します。

ステップ 2　**copy** コマンドを使用して、実行コンフィギュレーションをリモート サーバに保存します。

ステップ 3　**show license brief** コマンドを入力して、更新するファイル名を確認します。

```
switch# show license brief
Enterprise.lic:
```

ステップ 4　**update license** *url* コマンドを使用してライセンス ファイルを更新します。*url* は、更新されたライセンス ファイルの bootflash: または volatile: ロケーションを指定します。

```
switch# update license bootflash:Advanced2.lic Advanced1.lic
Updating Advanced1.lic:
SERVER this_host ANY
VENDOR cisco
# An example fcports license
INCREMENT SAN_EXTN_OVER_IP cisco 1.000 permanent 1 HOSTID=VDH=ABCD \
        NOTICE=<LicFileID>Advanced1.lic</LicFileID><LicLineID>0</LicLineID> \
        SIGN=33088E76F668

with bootflash:/Advanced2.lic:
SERVER this_host ANY
VENDOR cisco
# An example fcports license
INCREMENT SAN_EXTN_OVER_IP cisco 1.000 permanent 1 HOSTID=VDH=ABCD \
        NOTICE=<LicFileID>Advanced2.lic</LicFileID><LicLineID>1</LicLineID> \
        SIGN=67CB2A8CCAC2
```

ステップ 5　**yes** と入力して（yes がデフォルト）、ライセンスの更新を続けます。

```
Do you want to continue? (y/n) y
Updating license ..done
switch#
```

これで Enterprise.lic ライセンス キー ファイルが更新されました。

猶予期間のアラート

Cisco NX-OS には 120 日の猶予期間があります。この猶予期間はライセンスをインストールしていない機能の評価中に、開始または継続します。

猶予期間は評価中の機能をディセーブルにすると停止しますが、その機能を有効なライセンスなしで再びイネーブルにすると、停止したところから猶予期間のカウントダウンが継続します。

猶予期間はライセンス パッケージ内のすべての機能に働きます。ライセンス パッケージには複数の機能が含まれていることがあります。機能を猶予期間中にディセーブルにした場合に、まだイネーブルにされているその他の機能がライセンス パッケージにあると、そのライセンス パッケージのカウントダウンは停止しません。ライセンス パッケージの猶予期間カウントダウンを停止するには、そのライセンス パッケージのすべての機能をディセーブルにする必要があります。**show license usage** *license-name* コマンドを使用して、ディセーブルするアプリケーションを判別します。

```
switch# show license usage FC_FEATURES_PKG
アプリケーション
-----------
PFM
-----------
```

Cisco NX-OS ライセンス カウンタは、スイッチのすべてのライセンスを管理します。機能の評価中に猶予期間が開始されると、コンソール メッセージ、SNMP トラップ、システム メッセージ、および Call Home メッセージが毎日表示されます。

猶予期間の最後の 7 日間は、これらのメッセージの頻度が毎時になります。

（注） 猶予期間メッセージの頻度は変更できません。

注意 猶予期間の最後の 7 日間の後、機能が停止し、ネットワーク トラフィックが中断する場合があります。今後のアップグレードはライセンス要件および 120 日間の猶予期間を実施します。

show license usage コマンドを使用して、スイッチの猶予期間情報を表示します。

```
switch# show license usage
Feature                 Installed   License Status  ExpiryDate   Comments
                                    Count
--------------------------------------------------------------------------------------------
FM_SERVER_PKG           Yes         -       Unused   never        license missing
MAINFRAME_PKG           No          -       Unused   never        Grace Period 57days15hrs
ENTERPRISE_PKG          Yes         -       InUse    never        -
SAN_EXTN_OVER_IP        No          0       Unused   never        -
SAN_EXTN_OVER_IP_IPS4   No          0       Unused   never        -
--------------------------------------------------------------------------------------------
```

スイッチ間のライセンスの移動

ライセンスは発行されたスイッチに対して固有であり、その他のスイッチでは無効です。ライセンスをスイッチ間で転送する場合は、購入した代理店にお問い合わせください。

（注）シスコのサポートをシスコのリセラーからご購入された場合は、リセラーに直接お問い合わせください。サポートをシスコから直接ご購入された場合は、次の URL にある Technical Assistance Center（TAC）にご連絡ください。

★DTP: Delete [TAC Escalation Center] Section.

ライセンスの設定の確認

ライセンスの設定情報を表示するには、次のうちいずれかの処理を行います。

コマンド	目的
switch# **show license** [**brief**]	インストールされているすべてのライセンス ファイルの情報を表示します。
switch# **show license file**	特定ライセンス ファイルの情報を表示します。
switch# **show license host-id**	物理スイッチのホスト ID を表示します。
switch# **show license usage**	インストール済みライセンスの使用状況を表示します。

CHAPTER 5

イーサネット インターフェイスの設定

ここでは、Cisco Nexus 5000 シリーズ スイッチにおけるイーサネット インターフェイスの設定について説明します。内容は次のとおりです。

- イーサネット インターフェイスの概要（5-1 ページ）
- イーサネット インターフェイスの設定（5-4 ページ）
- インターフェイス情報の表示（5-9 ページ）

イーサネット インターフェイスの概要

イーサネット ポートは、サーバまたは LAN に接続される標準のイーサネット インターフェイスとして機能します。

イーサネット インターフェイスでは、Fibre Channel over Ethernet（FCoE）もサポートされます。FCoE により、イーサネット トラフィックとファイバ チャネル トラフィックの両方を物理イーサネット リンクで伝送できるようになります。詳細については、第 29 章「FCoE の設定」および第 30 章「仮想インターフェイスの設定」を参照してください。

Cisco Nexus 5000 シリーズ スイッチでは、イーサネット インターフェイスがデフォルトでイネーブルになっています。

この項では、次のトピックについて取り上げます。

- interface コマンドについて（5-1 ページ）
- UDLD パラメータ（5-2 ページ）
- インターフェイス速度（5-4 ページ）
- デバウンス タイマー パラメータについて（5-4 ページ）
- MTU 設定について（5-4 ページ）

interface コマンドについて

interface コマンドを使用すれば、イーサネット インターフェイスのさまざまな機能をインターフェイスごとにイネーブルにできます。**interface** コマンドを入力する際には、次の情報を指定します。

- インターフェイス タイプ：物理イーサネット インターフェイスには、常にキーワード **ethernet** を使用します。

- スロット番号
  - スロット 1 にはすべての固定ポートが含まれます。
  - スロット 2 には上位拡張モジュールのポートが含まれます（実装されている場合）。
  - スロット 3 には下位拡張モジュールのポートが含まれます（実装されている場合）。
- ポート番号
  - グループ内でのポート番号です。

UDLD パラメータ

この項では、次のトピックについて取り上げます。

- UDLD の概要（5-2 ページ）
- UDLD のデフォルト設定（5-3 ページ）
- UDLD アグレッシブ モードと非アグレッシブ モード（5-3 ページ）

UDLD の概要

シスコ独自の単方向リンク検出（UDLD）プロトコルでは、光ファイバまたは銅線（カテゴリ 5 ケーブル配線など）のイーサネット ケーブルで接続されているポートでケーブルの物理的な構成をモニタリングし、単方向リンクの存在を検出できます。スイッチが単方向リンクを検出すると、UDLD は関連する LAN ポートをシャットダウンし、ユーザに警告します。単方向リンクは、スパニングツリー トポロジ ループをはじめ、さまざまな問題を引き起こす可能性があります。

UDLD は、レイヤ 1 プロトコルと協調してリンクの物理ステータスを検出するレイヤ 2 プロトコルです。レイヤ 1 では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバーの ID の検知、誤って接続された LAN ポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 とレイヤ 2 の検出が協調して動作して、物理的な単一方向接続と論理的な単一方向接続を防止し、その他のプロトコルの異常動作を防止できます。

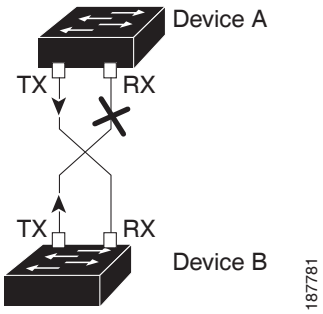
リンク上でローカル デバイスから送信されたトラフィックはネイバーで受信されるのに対し、ネイバーから送信されたトラフィックはローカル デバイスで受信されない場合には常に、単方向リンクが発生します。対になったファイバ ケーブルのうち一方の接続が切断された場合、自動ネゴシエーションがアクティブである限り、そのリンクはアップ状態が維持されなくなります。この場合、論理リンクは不定であり、UDLD は何の処理も行いません。レイヤ 1 で両方の光ファイバが正常に動作している場合は、レイヤ 2 で UDLD が、これらの光ファイルが正しく接続されているかどうか、および正しいネイバー間でトラフィックが双方向に流れているかを調べます。自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは、自動ネゴシエーションでは実行できません。

Cisco Nexus 5000 シリーズ スイッチは、UDLD をイネーブルにした LAN ポート上のネイバー デバイスに UDLD フレームを定期的に送信します。一定の時間内にフレームがエコー バックされてきて、特定の確認応答（echo）が見つからなければ、そのリンクは単一方向のフラグが立てられ、その LAN ポートはシャットダウンされます。UDLD プロトコルにより単方向リンクが正しく識別されその使用が禁止されるようにするためには、リンクの両端のデバイスで UDLD がサポートされている必要があります。

（注）　UDLD は、銅線の LAN ポート上では、このタイプのメディアでの不要な制御トラフィックの送信を避けるために、ローカルでデフォルトでディセーブルになっています。

図 5-1 に、単一方向リンク条件の例を示します。デバイス B はこのポートでデバイス A からのトラフィックを正常に受信していますが、デバイス A は同じポート上でデバイス B からのトラフィックを受信していません。UDLD によって問題が検出され、ポートがディセーブルになります。

図 5-1　　単方向リンク



UDLD のデフォルト設定

表 5-1 に、UDLD のデフォルト設定を示します。

表 5-1　　UDLD のデフォルト設定

機能	デフォルト値
UDLD グローバル イネーブル ステート	グローバルにディセーブル
UDLD アグレッシブ モード	ディセーブル
ポート別の UDLD イネーブル ステート（光ファイバ メディア用）	すべてのイーサネット光ファイバ LAN ポートでイネーブル
ポート別の UDLD イネーブル ステート（ツイストペア（銅製）メディア用）	すべてのイーサネット 10/100 および 1000BASE-TX LAN ポートでディセーブル

デバイスとそのポートの UDLD を設定する方法については、「UDLD モードの設定」セクション（5-5 ページ）を参照してください。

UDLD アグレッシブ モードと非アグレッシブ モード

デフォルトでは、UDLD アグレッシブ モードはディセーブルになっています。UDLD アグレッシブ モードは、UDLD アグレッシブ モードをサポートするネットワーク デバイスの間のポイントツーポイントのリンク上に限って設定できます。UDLD アグレッシブ モードをイネーブルに設定した場合、UDLD 近接関係が設定されている双方向リンク上のポートが UDLD フレームを受信しなくなったとき、UDLD はネイバーとの接続を再確立しようとします。この再試行に 8 回失敗すると、ポートはディセーブルになります。

スパニングツリー ループを防止するため、間隔がデフォルトの 15 秒である非アグレッシブな UDLD でも、（デフォルトのスパニングツリー パラメータを使用して）ブロッキング ポートがフォワーディング ステートに移行する前に、単方向リンクをシャットダウンすることができます。

UDLD アグレッシブ モードをイネーブルにすると、次のようなことが発生します。

- リンクの一方にポート スタックが生じる（送受信どちらも）
- リンクの一方がダウンしているにもかかわらず、リンクのもう一方がアップしたままになる

このような場合、UDLD アグレッシブ モードでは、リンクのポートの 1 つがディセーブルになり、トラフィックが廃棄されるのを防止します。

インターフェイス速度

Cisco Nexus 5000 シリーズ スイッチでは、固定の 10 ギガビットのポートが多数装備され、各ポートには SFP＋ インターフェイス アダプタが装着されています。Nexus 5010 スイッチには 20 個の固定ポートが装備されており、そのうち、最初の 8 個がスイッチ可能な 1 ギガビットおよび 10 ギガビットのポートです。Nexus 5020 スイッチには 40 個の固定ポートが装備されており、そのうち、最初の 16 個がスイッチ可能な 1 ギガビットおよび 10 ギガビットのポートです。

デバウンス タイマー パラメータについて

ポート デバウンス時間は、リンクがダウンしたことをスーパーバイザに通知するためにインターフェイスが待機する時間です。この時間、インターフェイスはリンクがアップ状態に戻ったかどうかを確認するために待機します。待機時間は、トラフィックが停止している時間です。

デバウンス タイマーは各インターフェイスに対してイネーブルにでき、ミリ秒単位で遅延時間を指定できます。

注意　ポート デバウンス タイマーをイネーブルにすると、リンク アップ検出とリンク ダウン検出に遅延が発生するため、デバウンス期間中にトラフィックが一部損失します。トラフィックが損失することにより、一部のプロトコルのコンバージェンスおよび再コンバージェンスに影響を及ぼす場合があります。

MTU 設定について

物理イーサネット インターフェイスごとの最大伝送単位（MTU）はサポートされていません。代わりに、MTU は QoS クラスに従って設定されます。MTU は、ポリシーとクラスのマップを設定することにより変更できます。詳細については、第 31 章「QoS の設定」を参照してください。

インターフェイス設定を表示すると、物理イーサネット インターフェイスの MTU は 1500 と表示され、ファイバ チャネル インターフェイスの受信データ フィールド サイズは 2112 と表示されます。

イーサネット インターフェイスの設定

ここでは、イーサネット インターフェイスを設定する方法を示します。説明する項目は次のとおりです。

- UDLD モードの設定（5-5 ページ）
- インターフェイス速度の設定（5-6 ページ）
- CDP パラメータの設定（5-7 ページ）

- デバウンス タイマーの設定（5-7 ページ）
- 説明パラメータの設定（5-8 ページ）
- イーサネット インターフェイスのディセーブル化と再起動（5-8 ページ）

UDLD モードの設定

単一方向リンク検出（UDLD）を実行するように設定されているデバイス上のイーサネット インターフェイスには、ノーマル モードまたはアグレッシブ モードの UDLD を設定できます。インターフェイスの UDLD モードをイネーブルにするには、そのインターフェイスを含むデバイス上で UDLD を事前にイネーブルにしておく必要があります。UDLD は他方のリンク先のインターフェイスおよびそのデバイスでもイネーブルになっている必要があります。

ノーマル UDLD モードを使用するには、ポートの 1 つをノーマル モードに設定し、他方のポートをノーマル モードまたはアグレッシブ モードに設定する必要があります。アグレッシブ UDLD モードを使用するには、両方のポートをアグレッシブ モードに設定する必要があります。

（注） 設定前に、リンクされている他方のポートとそのデバイスの UDLD をイネーブルにしておかなければなりません。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# feature udld`	デバイスの UDLD をイネーブルにします。
	`switch(config)# no feature udld`	デバイスの UDLD をディセーブルにします。
ステップ 3	`switch(config)# show udld global`	デバイスの UDLD ステータスを表示します。
ステップ 4	`switch(config)# interface ethernet` *slot/port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	`switch(config-if)# udld {enable | disable | aggressive}`	ノーマル UDLD モードをイネーブルにするか、UDLD をディセーブルにするか、またはアグレッシブ UDLD モードをイネーブルにします。
ステップ 6	`switch(config-if)# show udld` *interface*	インターフェイスの UDLD ステータスを表示します。

次の例は、スイッチの UDLD をイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# feature udld
```

次の例は、イーサネット ポートのノーマル UDLD モードをイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# udld enable
```

次の例は、イーサネット ポートのアグレッシブ UDLD モードをイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# udld aggressive
```

次の例は、イーサネット ポートの UDLD をディセーブルにする例を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# udld disable
```

次の例は、スイッチの UDLD をディセーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# no feature udld
```

インターフェイス速度の設定

Nexus 5010 スイッチの最初の 8 個のポートと、Nexus 5020 スイッチの最初の 16 個のポートは、スイッチ可能な 1 ギガビット ポートと 10 ギガビット ポートです。デフォルトのインターフェイス速度は 10 ギガビットです。これらのポートを 1 ギガビット イーサネット用に設定するには、1 ギガビット イーサネット SFP トランシーバを適切なポートに挿入してから、**speed** コマンドを使用して速度を設定します。

1 ギガビット イーサネット ポートを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface type slot/port`	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。このインターフェイスに、1 ギガビット イーサネット SFP+ トランシーバが挿入されている必要があります。
ステップ 3	`switch(config-if)# speed speed`	インターフェイスの速度を設定します。

次に、1 ギガビット イーサネット ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# speed 1000
```

このコマンドは、物理的なイーサネット インターフェイスにしか適用できません。

（注） インターフェイスとトランシーバの速度が一致しない場合に **show interface ethernet** *slot/port* コマンドを実行すると、SFP 検証の失敗を伝えるメッセージが表示されます。たとえば、**speed 1000** と設定せずに 1 ギガビット SFP トランシーバをポートに挿入すると、このエラーが発生します。デフォルトでは、すべてのポートが 10 ギガビットです。

CDP パラメータの設定

イーサネット インターフェイスの Cisco Discovery Protocol（CDP）をイネーブルまたはディセーブルにできます。このプロトコルは、同一リンクの両方のインターフェイスでイネーブルになっている場合にだけ機能します。

インターフェイスに対して CDP をイネーブルにしたりディセーブルにしたりする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface type slot/port`	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# cdp enable`	インターフェイスに対して CDP をイネーブルにします。 正常に機能するには、このパラメータが同一リンク上の両方のインターフェイスでイネーブルになっている必要があります。
	`switch(config-if)# cdp enable`	インターフェイスに対して CDP をディセーブルにします。

次に、イーサネット ポートに対して CDP をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# cdp enable
```

このコマンドは、物理的なイーサネット インターフェイスにしか適用できません。

デバウンス タイマーの設定

イーサネットのデバウンス タイマーは、デバウンス時間（ミリ秒単位）を指定することによりイネーブル化でき、デバウンス時間に 0 を指定することによりディセーブル化できます。

show interface debounce コマンドを使用すれば、すべてのイーサネット ポートのデバウンス時間を表示できます。

デバウンス タイマーをイネーブル/ディセーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface type slot/port`	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# link debounce time milliseconds`	指定した時間（1 ～ 5,000 ミリ秒）でデバウンス タイマーをイネーブルにします。 0 ミリ秒を指定すると、デバウンス タイマーはディセーブルになります。

次の例は、イーサネット インターフェイスでデバウンス タイマーをイネーブルにして、デバウンス時間を 1000 ミリ秒に設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# link debounce time 1000
```

次の例は、イーサネット インターフェイスでデバウンス タイマーをディセーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# link debounce time 0
```

このコマンドは、物理的なイーサネット インターフェイスにしか適用できません。

説明パラメータの設定

イーサネット ポートのインターフェイスのテキストでの説明を提供する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** *type slot/port*	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **description** *test*	インターフェイスの説明を指定します。

次に、インターフェイスの説明を「Server 3 Interface」に設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# description Server 3 Interface
```

イーサネット インターフェイスのディセーブル化と再起動

イーサネット インターフェイスは、シャットダウンして再起動することができます。この操作により、すべてのインターフェイス機能がディセーブル化され、すべてのモニタリング画面でインターフェイスがダウンしているものとしてマークされます。この情報は、すべてのダイナミック ルーティング プロトコルを通じて、他のネットワーク サーバに伝達されます。シャットダウンされたインターフェイスは、どのルーティング アップデートにも含まれません。

インターフェイスをディセーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** *type slot/port*	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **shutdown**	インターフェイスをディセーブルにします。

次に、イーサネット ポートをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# shutdown
```

インターフェイスを再起動する手順は、次のとおりです。

コマンド	目的
switch(config-if)# **no shutdown**	インターフェイスを再起動します。

次に、イーサネット インターフェイスを再起動する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# no shutdown
```

インターフェイス情報の表示

定義済みインターフェイスに関する設定情報を表示するには、次のうちいずれかの手順を実行します。

コマンド	目的
switch# **show interface** *type slot/port*	指定したインターフェイスの詳細設定が表示されます。
switch# **show interface** *type slot/port* **capabilities**	指定したインターフェイスの機能に関する詳細情報が表示されます。このオプションは、物理インターフェイスにしか使用できません。
switch# **show interface** *type slot/port* **transceiver**	指定したインターフェイスに接続されているトランシーバに関する詳細情報が表示されます。このオプションは、物理インターフェイスにしか使用できません。
switch# **show interface brief**	すべてのインターフェイスのステータスが表示されます。
switch# **show interface debounce**	すべてのインターフェイスのデバウンス ステータスが表示されます。
switch# **show interface flowcontrol**	すべてのインターフェイスでフロー制御設定の詳細なリストを表示します。

show interface コマンドは、EXEC モードから呼び出され、インターフェイスの設定を表示します。引数を入力せずにこのコマンドを実行すると、スイッチ内に設定されたすべてのインターフェイスの情報が表示されます。

次に、物理イーサネット インターフェイスを表示する例を示します。

```
switch# show interface ethernet 1/4
Ethernet1/1 is up
  Hardware is 1000/10000 Ethernet, address is 000d.eca3.5f08 (bia 000d.eca3.5f08)
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
```

```
    reliability 255/255, txload 190/255, rxload 192/255
  Encapsulation ARPA
  Port mode is trunk
  full-duplex, 10 Gb/s, media type is 1/10g
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned on
  Rate mode is dedicated
  Switchport monitor is off
  Last clearing of "show interface" counters never
  5 minute input rate 942201806 bytes/sec, 14721892 packets/sec
  5 minute output rate 935840313 bytes/sec, 14622492 packets/sec
  Rx
    129141483840 input packets 0 unicast packets 129141483847 multicast packets
    0 broadcast packets 0 jumbo packets 0 storm suppression packets
    8265054965824 bytes
    0 No buffer 0 runt 0 Overrun
    0 crc 0 Ignored 0 Bad etype drop
    0 Bad proto drop
  Tx
    119038487241 output packets 119038487245 multicast packets
    0 broadcast packets 0 jumbo packets
    7618463256471 bytes
    0 output CRC 0 ecc
    0 underrun 0 if down drop     0 output error 0 collision 0 deferred
    0 late collision 0 lost carrier 0 no carrier
    0 babble
    0 Rx pause 8031547972 Tx pause 0 reset
```

次に、物理イーサネットの機能を表示する例を示します。

```
switch# show interface ethernet 1/3 capabilities
Ethernet1/1
  Model:                 AGD11342302
  Type:                  10Gbase-SR
  Speed:                 1000,10000
  Duplex:                full
  Trunk encap. type:     802.1Q
  Channel:               no
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off/on),tx-(off/on)
  Rate mode:             none
  QOS scheduling:        rx-(6q1t),tx-(1p6q0t)
  CoS rewrite:           no
  ToS rewrite:           no
  SPAN:                  yes
  UDLD:                  yes
  Link Debounce:         yes
  Link Debounce Time:    yes
  MDIX:                  no
```

次に、物理イーサネット トランシーバを表示する例を示します。

```
switch# show interface ethernet 1/3 transceiver
Ethernet1/3
    sfp is present
    name is CISCO-AVAGO
    part number is SFBR-7700SDZ    B4  R
    revision is B4  R
    serial number is AGD1134229V     070823
    nominal bitrate is 0 MBits/sec
    Link length supported for 50/125mm fiber is 0 m(s)
    Link length supported for 62.5/125mm fiber is 0 m(s)
    cisco id is --
    cisco extended id number is 4
```

次に、インターフェイス ステータスの要約を表示する例を示します（出力の一部を割愛してあります）。

```
switch# show interface brief

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
Eth1/1        200    eth  trunk  up      none                       10G(D) --
Eth1/2        1      eth  trunk  up      none                       10G(D) --
Eth1/3        300    eth  access down    SFP not inserted           10G(D) --
Eth1/4        300    eth  access down    SFP not inserted           10G(D) --
Eth1/5        300    eth  access down    Link not connected        1000(D) --
Eth1/6        20     eth  access down    Link not connected         10G(D) --
Eth1/7        300    eth  access down    SFP not inserted           10G(D) --
...
```

次の例は、リンクのデバウンス ステータスの表示方法を示しています（簡潔にするため、一部の出力が削除されています）。

```
switch# show interface debounce

--------------------------------------------------------------------------------
Port          Debounce time   Value(ms)
--------------------------------------------------------------------------------
...
Eth1/1        enable               100
Eth1/2        enable               100
Eth1/3        enable               100
...
```

次に、CDP ネイバーを表示する例を示します。

```
switch# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute


Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID

d5-switch-9.qa.Eth1/40         148     R S I    WS-C6506-E    Ten4/2

dist-row-d               mgmt0           147     R S I    WS-C3560G-48T Gig0/34
```

物理イーサネットのデフォルト設定

次の表に、すべての物理イーサネット インターフェイスのデフォルト設定を示します。

パラメータ	デフォルト設定
デバウンス	イネーブル、100 ミリ秒
Duplex	オート（全二重）
カプセル化	ARPA
MTU[1]	1500 バイト

パラメータ	デフォルト設定
Port Mode	アクセス
速度	オート（10000）

1. MTU を物理イーサネット インターフェイスごとに変更することはできません。MTU の変更は、QoS クラスのマップを選択することにより行います。詳細については、「第 31 章「QoS の設定」」を参照してください。

CHAPTER 6

VLAN の設定

VLAN（仮想 LAN）を使用し、別々の論理領域にネットワークを分割できます。VLAN はブロードキャスト ドメインと見なすこともできます。

どのようなスイッチ ポートでも VLAN に属すことができ、ユニキャスト、ブロードキャスト、マルチキャストのパケットは、その VLAN に属する端末だけに転送またはフラッディングされます。各 VLAN は論理ネットワークと見なされ、VLAN に属さないステーション宛てのパケットはルータで転送する必要があります。

この章は、次の項で構成されています。

- VLAN について（6-1 ページ）
- VLAN の設定（6-4 ページ）
- VLAN 設定の確認（6-6 ページ）

VLAN について

この項では、次のトピックについて取り上げます。

- VLAN の概要（6-1 ページ）
- VLAN 範囲の概要（6-2 ページ）
- VLAN の作成、削除、変更（6-3 ページ）

VLAN の概要

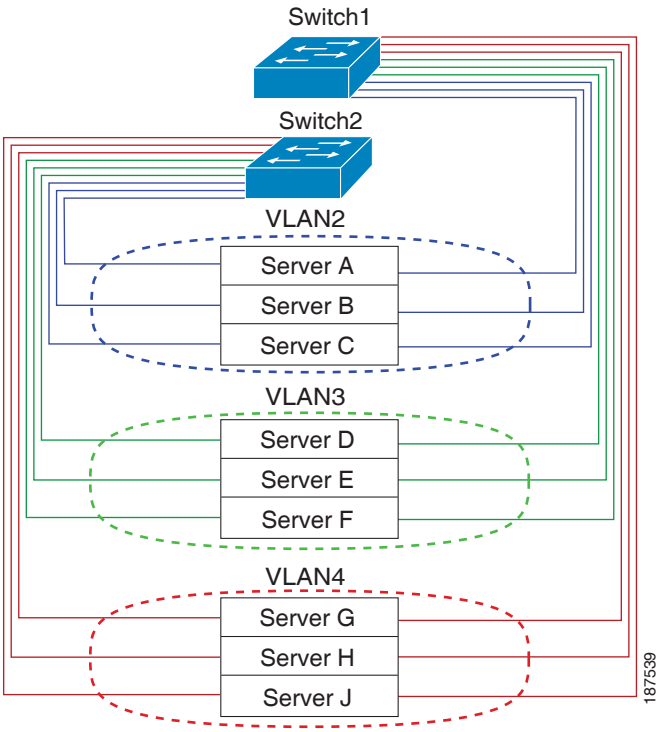
（注） VLAN トランキング プロトコル（VTP）モードはオフです。その他のスイッチで VTP がオンになっている場合に VTP ドメインを分割する Cisco Nexus 5000 シリーズ スイッチのすべてのインターフェイスでは、VTP BPDU がドロップされます。

VLAN は、ユーザの物理的な位置に関係なく、機能、プロジェクト チーム、またはアプリケーションによって論理的にセグメント化されているスイッチド ネットワークの端末のグループです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンド ステーションもグループ化できます。

どのようなポートでも VLAN に属すことができ、ユニキャスト、ブロードキャスト、マルチキャストのパケットは、その VLAN に属する端末だけに転送またはフラッディングされます。各 VLAN は論理ネットワークと見なされます。VLAN に属さないステーション宛てのパケットは、ルータで転送する必要があります。

図 6-1 に、論理ネットワークとしての VLAN を示します。この図では、エンジニアリング部門のステーションはある VLAN に、マーケティング部門のステーションは別の VLAN に、会計部門のステーションはまた別の VLAN に割り当てられています。

図 6-1　　論理的に定義されたネットワークとしての VLAN



VLAN は通常、IP サブネットワークに関連付けられますたとえば、特定の IP サブネットに含まれるエンド ステーションはすべて同じ VLAN に属します。VLAN 間で通信するには、トラフィックをルーティングする必要があります。

デフォルトでは、新しく作成した VLAN は動作状態になります。つまり VLAN は非シャットダウン状態になります。また、トラフィックを通過させるアクティブ ステート、またはパケットを通過させない一時停止ステートに、VLAN を設定することもできます。デフォルトでは、VLAN はアクティブ ステートでトラフィックを通過させます。

VLAN 範囲の概要

Cisco Nexus 5000 シリーズ スイッチでは、IEEE 802.1Q 標準に従って VLAN 番号 1 ～ 4094 がサポートされます。これらの VLAN は、範囲ごとにまとめられています。各範囲は多少違った方法で使用します。スイッチでサポートできる VLAN の数には物理的な制限があります。ハードウェアは、この使用可能範囲を VSAN とも共有します。サポートされる VLAN および VSAN の数の詳細については、「設定の制限値」セクション（51-1 ページ）を参照してください。

表 6-1 は、VLAN 範囲の詳細について説明しています。

表 6-1　VLAN 範囲

VLAN 番号	範囲	使用法
1	標準	シスコのデフォルトです。この VLAN は使用できますが、変更や削除はできません。
2 ～ 1005	標準	これらの VLAN は、作成、使用、変更、削除できます。
1006 ～ 4094	拡張	これらの VLAN は、作成、命名、使用できます。次のパラメータは変更できません。 • ステートは常にアクティブになります。 • VLAN は常にイネーブルになります。これらの VLAN はシャットダウンできません。
3968 ～ 4047 および 4094	内部割り当て	これらの 80 個の VLAN および VLAN 4094 は、内部で使用するために割り当てられています。内部使用に予約されたブロック内の VLAN の作成、削除、変更はできません。

（注） VLAN 3968 ～ 4047 および 4094 は内部使用に予約されています。これらの VLAN の変更または使用はできません。

Cisco NX-OS では、動作のために内部 VLAN を使用する必要がある、マルチキャストや診断などの機能用に、80 個の VLAN 番号のグループを割り当てています。デフォルトでは、番号 3968 ～ 4047 の VLAN が内部使用に割り当てられます。VLAN 4094 もスイッチの内部使用のために予約されています。

予約グループの VLAN の使用、変更、削除はできません。内部的に割り当てられている VLAN、およびそれに関連した用途は表示できます。

VLAN の作成、削除、変更

VLAN には 1 ～ 4094 の番号が付けられます。スイッチを初めて起動したとき、すべての設定済みポートはデフォルト VLAN に属します。デフォルト VLAN（VLAN1）はデフォルト値だけを使用し、デフォルト VLAN でアクティビティの作成、削除、一時停止を行うことはできません。

VLAN は番号を割り当てて作成します。VLAN は削除でき、アクティブ動作ステートから一時停止動作ステートに移行することもできます。既存の VLAN ID で VLAN を作成しようとすると、スイッチは VLAN サブモードになりますが、同一の VLAN は再作成しません。

新しく作成した VLAN は、その VLAN にポートが割り当てられるまで使用されません。すべてのポートはデフォルトで VLAN1 に割り当てられます。

VLAN の範囲により、次のパラメータを VLAN 用に設定できます（デフォルト VLAN を除く）。

- VLAN 名
- シャットダウンまたは非シャットダウン

特定の VLAN を削除すると、その VLAN に関連するポートはシャットダウンされ、トラフィックは流れなくなります。しかしシステムはその VLAN の VLAN/ポート マッピングをすべて維持するため、その VLAN の再イネーブル化や再作成を行うと、その VLAN の元のすべてのポートは自動的に回復します。

（注）　VLAN コンフィギュレーション サブモードで入力したコマンドはすぐに実行されます。Cisco Nexus 5000 シリーズのシスコ リリース 5.1 以降のデバイスでは、設定の変更を有効にするために、VLAN コンフィギュレーション サブモードを終了する必要があります。

（注）　VLAN 3968 ～ 4047 および 4094 は内部使用に予約されています。これらの VLAN の変更または使用はできません。

VLAN の設定

この項では、次のトピックについて取り上げます。

- VLAN の作成と削除（6-4 ページ）
- VLAN サブモードの開始と VLAN の設定（6-5 ページ）
- VLAN へのポートの追加（6-6 ページ）

VLAN の作成と削除

デフォルト VLAN およびスイッチによる使用のために内部的に割り当てられている VLAN を除き、すべての VLAN は、作成または削除が可能です。

VLAN を作成すると、その VLAN は自動的にアクティブ ステートになります。

（注）　VLAN を削除すると、その VLAN にアソシエートされたポートはシャットダウンします。トラフィックは流れなくなり、パケットはドロップされます。

VLAN を作成する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# vlan {vlan-id | vlan-range}`	VLAN または VLAN の範囲を作成します。 VLAN にすでに割り当てられている番号を入力すると、その VLAN の VLAN コンフィギュレーション サブモードがスイッチによって開始されます。内部的に割り当てられている VLAN に割り当てられている番号を入力すると、エラー メッセージが返されます。VLAN の範囲を入力し、指定 VLAN の 1 つ以上が、内部的に割り当てられた VLAN の範囲外である場合、コマンドは範囲外の VLAN *だけ*で有効になります。指定できる範囲は 2 ～ 4094 です。VLAN1 はデフォルト VLAN であり、作成や削除はできません。内部使用のために予約されている VLAN の作成や削除はできません。

次の例は、15 ～ 20 の範囲で VLAN を作成する方法を示しています。

```
switch# configure terminal
switch(config)# vlan 15-20
```

（注）　VLAN コンフィギュレーション サブモードで VLAN の作成と削除を行うこともできます。

VLAN を削除する手順は、次のとおりです。

コマンド	目的
`switch(config-vlan)# no vlan {vlan-id | vlan-range}`	指定した VLAN または VLAN の範囲を削除し、VLAN コンフィギュレーション サブモードを終了します。VLAN1 または内部的に割り当てられている VLAN は削除できません。

VLAN サブモードの開始と VLAN の設定

VLAN の次のパラメータの設定または変更を行うには、VLAN コンフィギュレーション サブモードを開始する必要があります。

- 名前
- Shut down

（注）　デフォルト VLAN または内部的に割り当てられた VLAN の作成、削除、変更はできません。一部の VLAN ではパラメータの一部を変更できません。詳細については、「VLAN 範囲の概要」セクション（6-2 ページ）を参照してください。

サブモードを開始して VLAN を設定する手順は次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# vlan {vlan-id | vlan-range}`	VLAN コンフィギュレーション サブモードを開始します。VLAN が存在しない場合は、先に指定 VLAN が作成されます。
ステップ 3	`switch(config-vlan)# name vlan-name`	VLAN に名前を付けます。32 文字までの英数字を入力して VLAN に名前を付けることができます。VLAN1 または内部的に割り当てられている VLAN の名前は変更できません。デフォルト値は VLANxxxx であり、xxxx は、VLAN ID 番号と等しい 4 桁の数字（先行ゼロも含む）を表します。
ステップ 4	`switch(config-vlan)# no shutdown`	VLAN をイネーブルにします。デフォルト値は **no shutdown**（イネーブル）です。デフォルト VLAN の VLAN1、または VLAN 1006 ～ 4094 はシャットダウンできません。

次の例は、VLAN 5 のオプション パラメータを設定する方法を示しています。

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# name accounting
switch(config-vlan)# state active
switch(config-vlan)# no shutdown
```

VLAN へのポートの追加

VLAN の設定が完了したら、ポートを割り当てます。ポートを追加する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** {*type slot/port* | **port-channel** *number*}	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスには、物理イーサネット ポートまたはポート チャネルを指定できます。
ステップ 3	switch(config-if)# **switchport access vlan** *vlan-id*	インターフェイスのアクセス モードを指定 VLAN に設定します。

次の例は、VLAN 5 に参加するようにイーサネット インターフェイスを設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/13
switch(config-if)# switchport access vlan 5
```

VLAN 設定の確認

VLAN の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
switch# **show running-config vlan** [*vlan_id* | *vlan_range*]	VLAN 情報を表示します。
switch# **show vlan** [**brief** | **id** [*vlan_id* | *vlan_range*] | **name** *name* | **summary**]	定義済み VLAN の選択した設定情報を表示します。

次の例は、1 ～ 21 の範囲で定義されているすべての VLAN を表示しています。

```
switch# show running-config vlan 1-21
version 4.0(0)
vlan 1
vlan 5
```

次の例は、スイッチで作成されている VLAN およびそのステータスを表示しています。

```
switch# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Eth1/1, Eth1/2, Eth1/3, Eth1/4
                                                Eth1/5, Eth1/6, Eth1/7, Eth1/8
                                                Eth1/9, Eth1/10, Eth1/11
                                                Eth1/12, Eth1/15, Eth1/16
                                                Eth1/17, Eth1/18, Eth1/19
                                                Eth1/20, Eth1/21, Eth1/22
                                                Eth1/23, Eth1/24, Eth1/25
                                                Eth1/26, Eth1/27, Eth1/28
                                                Eth1/29, Eth1/30, Eth1/31
                                                Eth1/32, Eth1/33, Eth1/34
                                                Eth1/35, Eth1/36, Eth1/37
                                                Eth1/38, Eth1/39, Eth1/40
                                                Eth3/1, Eth3/2, Eth3/3, Eth3/4
                                                veth1/1
13   VLAN0005                         active    Eth1/13, Eth1/14
```

次の例は、メンバ ポートも含めた、VLAN 13 の詳細を表示しています。

```
switch# show vlan id 13

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
13   VLAN0005                         active    Eth1/13, Eth1/14


VLAN Type   MTU
---- ----- -----
13   enet  576

Remote SPAN VLAN
----------------
ディセーブル

Primary  Secondary  Type             Ports
-------  ---------  ---------------  ------------------------------------------
```

次の例は、VLAN 設定の概要を表示しています。

```
switch# show vlan summary

Number of existing VLANs           : 2
 Number of existing VTP VLANs      : 2
 Number of existing extended VLANs : 0
```

CHAPTER 7

プライベート VLAN の設定

この章では、プライベート VLAN の設定方法について説明します。

（注） この章で説明している設定を行う前に、プライベート VLAN をイネーブルにする必要があります。

この章は、次の項で構成されています。

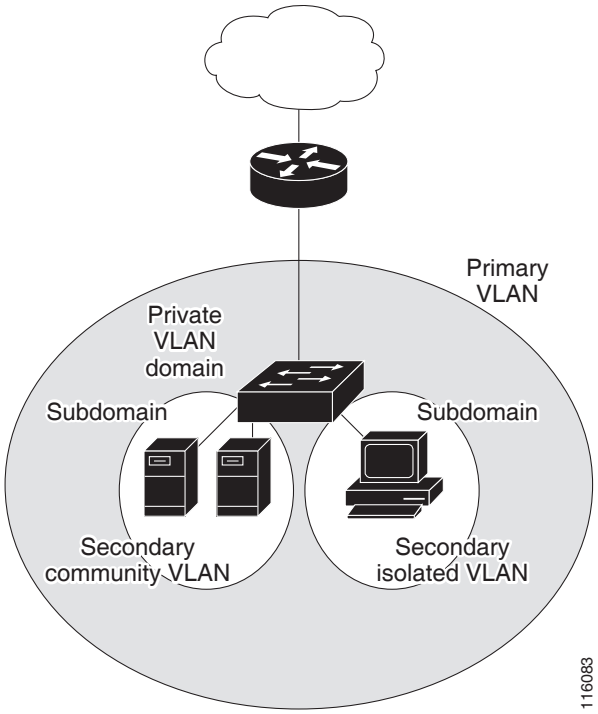
- プライベート VLAN の概要（7-1 ページ）
- プライベート VLAN の設定（7-6 ページ）
- プライベート VLAN 設定の確認（7-11 ページ）

プライベート VLAN の概要

プライベート VLAN では VLAN のレイヤ 2 ブロードキャスト ドメインがサブドメインに分割されるので、スイッチで相互にポートを分離できます。サブドメインは、1 つのプライマリ VLAN と 1 つまたは複数のセカンダリ VLAN で構成されます（図 7-1 を参照）。プライベート VLAN にあるすべての VLAN は、同じプライマリ VLAN を共有します。セカンダリ VLAN ID は、各サブドメインの区別に使用されます。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかの場合があります。独立 VLAN 上のホストは、そのプライマリ VLAN 上でアソシエートされている無差別ポートのみと通信できます。コミュニティ VLAN 上のホストは、それぞれのホスト間およびアソシエートされている無差別ポートと通信できますが、他のコミュニティ VLAN にあるポートとは通信できません。

（注） 現行リリースの Cisco NX-OS を実行している Cisco Nexus 5000 シリーズ スイッチの PVLAN 独立ポートは、IEEE 802.1q のカプセル化をサポートせず、トランク ポートとして使用できません。

図 7-1　　プライベート VLAN ドメイン



（注）　VLAN は、プライマリまたはセカンダリのプライベート VLAN に変換する前に、まず、作成する必要があります。VLAN 作成の詳細については、第 6 章「VLAN の設定」を参照してください。

この項では、次のトピックについて取り上げます。

- プライベート VLAN のプライマリ VLAN とセカンダリ VLAN（7-2 ページ）
- プライベート VLAN ポートの概要（7-3 ページ）
- プライベート VLAN におけるブロードキャスト トラフィックの概要（7-5 ページ）
- プライベート VLAN ポート隔離の概要（7-5 ページ）

プライベート VLAN のプライマリ VLAN とセカンダリ VLAN

プライベート VLAN ドメインには、プライマリ VLAN が 1 つのみ含まれています。プライベート VLAN ドメインの各ポートは、プライマリ VLAN のメンバです。プライマリ VLAN は、プライベート VLAN ドメイン全体です。

セカンダリ VLAN は、同じプライベート VLAN ドメイン内のポート間を分離します。プライマリ VLAN 内のセカンダリ VLAN には、次の 2 つのタイプがあります。

- 独立 VLAN：独立 VLAN 内のポートは、レイヤ 2 レベルで直接かつ相互には通信できません。
- コミュニティ VLAN：コミュニティ VLAN 内のポートは相互通信できますが、他のコミュニティ VLAN またはレイヤ 2 レベルの独立 VLAN にあるポートとは通信できません。

プライベート VLAN ポートの概要

プライベート VLAN ポートのタイプは、次のとおりです。

- 無差別：無差別ポートはプライマリ VLAN に属します。無差別ポートは、無差別ポートとアソシエートされているセカンダリ VLAN に属し、プライマリ VLAN とアソシエートされている、すべてのインターフェイスと通信でき、この通信可能なインターフェイスには、コミュニティ ポートと独立ホスト ポートも含まれます。プライマリ VLAN には、複数の無差別ポートを含めることができます。各無差別ポートには、ポートにアソシエートされている、複数のセカンダリ VLAN を含めることができ、また、セカンダリ VLAN を含めないこともできます。無差別ポートとセカンダリ VLAN が同じプライマリ VLAN にある限り、セカンダリ VLAN は、複数の無差別ポートとアソシエートすることができます。ロード バランシングまたは冗長性を持たせる目的で、これを行う必要が生じる場合があります。無差別ポートと関連付けられていないセカンダリ VLAN も、含めることができます。
- 独立：独立ポートは、独立セカンダリ VLAN に属しているホスト ポートです。このポートは、アソシエートされている無差別ポートと通信できることを除き、同じプライベート VLAN ドメイン内の他のポートから、完全に隔離されています。プライベート VLAN は、無差別ポートからのトラフィックを除き、独立ポート宛のトラフィックをすべてブロックします。独立ポートから受信されたトラフィックは、無差別ポートにだけ転送されます。指定した独立 VLAN には、複数の独立ポートを含めることができます。各ポートは、独立 VLAN にある他のすべてのポートから、完全に隔離されています。
- コミュニティ：コミュニティ ポートは、1 つのコミュニティ セカンダリ VLAN に属しているホスト ポートです。コミュニティ ポートは、同じコミュニティ VLAN にある他のポートおよびアソシエートされている無差別ポートと通信します。これらのインターフェイスは、他のコミュニティにある他のすべてのインターフェイスからも、プライベート VLAN ドメイン内のすべての独立ポートからも、隔離されています。

（注） トランクでは、無差別ポート、独立ポート、コミュニティ ポート間で VLAN がトラフィックを伝送するのをサポートできるので、独立ポート トラフィックおよびコミュニティ ポート トラフィックは、トランク インターフェイスを通じてスイッチでの着信/発信を行う可能性があります。

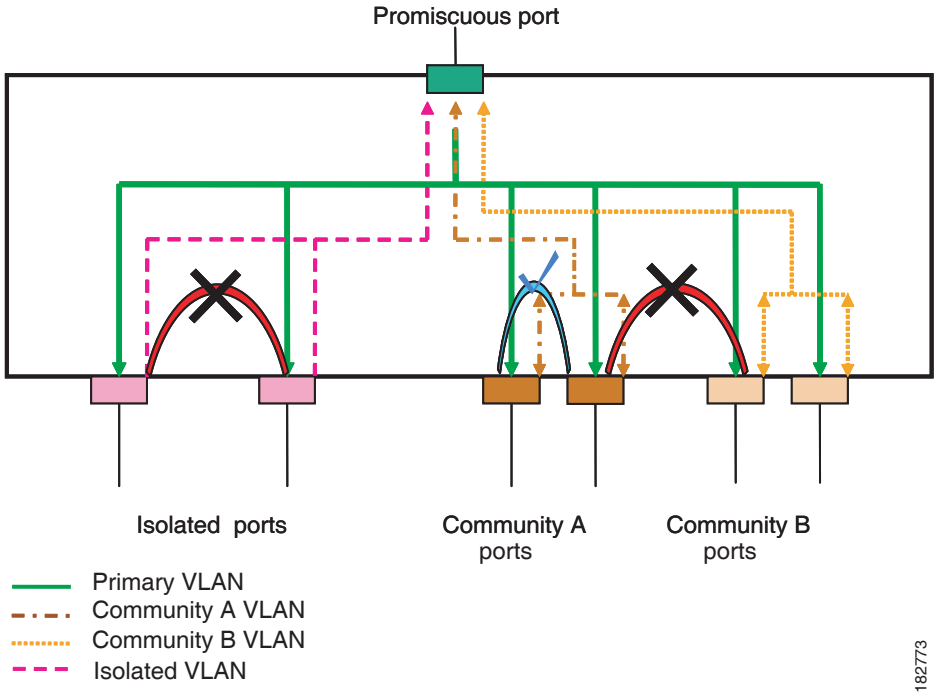
プライマリ VLAN、独立 VLAN、コミュニティ プライベート VLAN の概要

プライマリ VLAN および 2 つのタイプのセカンダリ VLAN（独立 VLAN とコミュニティ VLAN）には、次のような特徴があります。

- プライマリ VLAN：独立ポートおよびコミュニティ ポートであるホスト ポート、および他の無差別ポートに、無差別ポートからトラフィックを伝送します。
- 独立 VLAN：ホストから無差別ポートにアップストリームに単方向トラフィックを伝送するセカンダリ VLAN です。プライベート VLAN ドメインには、複数の独立 VLAN を設定できます。すべてのトラフィックは、それぞれの内部に隔離されて残ります。各独立 VLAN には、複数の独立ポートを含めることができ、各独立ポートからのトラフィックも、完全に別に残ります。
- コミュニティ VLAN：コミュニティ VLAN は、コミュニティ ポートから、無差別ポートおよび同じコミュニティにある他のホスト ポートへ、アップストリーム トラフィックを送信するセカンダリ VLAN です。プライベート VLAN には、複数のコミュニティ VLAN を設定できます。1 つのコミュニティ内のポートは相互に通信できますが、これらのポートは、他のコミュニティにあるポートとも、プライベート VLAN にある独立 VLAN とも、通信できません。

図 7-2 に、プライベート VLAN 内のトラフィック フローと、VLAN のタイプ、ポートのタイプを示します。

図 7-2　　プライベート VLAN のトラフィック フロー



（注）　プライベート VLAN のトラフィック フローは、ホスト ポートから無差別ポートへの単方向です。プライマリ VLAN で受信するトラフィックによって隔離は行われず、転送は通常 VLAN として実行されます。

無差別ポートでは、1 つのみのプライマリ VLAN と複数のセカンダリ VLAN（コミュニティ VLAN および独立 VLAN）を処理できます。無差別ポートでは、広範囲なデバイスをプライベート VLAN のアクセス ポイントとして接続できます。たとえば、すべてのプライベート VLAN サーバを管理ワークステーションから監視したりバックアップしたりするのに、無差別ポートを使用できます。

スイッチング環境では、個々のエンド ステーションに、または共通グループのエンド ステーションに、個別のプライベート VLAN や、関連する IP サブネットを割り当てることができます。エンド ステーションはデフォルト ゲートウェイとの通信を行うだけで、プライベート VLAN の外部と通信することができます。

プライマリ VLAN とセカンダリ VLAN の関連付け

セカンダリ VLAN にあるホスト ポートで、プライベート VLAN の外部と通信するには、セカンダリ VLAN をプライマリ VLAN にアソシエートします。アソシエーションの操作が可能ではない場合、セカンダリ VLAN のホスト ポート（コミュニティ ポートと独立ポート）は、ダウンされます。

（注）　セカンダリ VLAN は、1 つのプライマリ VLAN のみにアソシエートすることができます。

アソシエーションの操作を可能にするには、次の条件を満たす必要があります。

- プライマリ VLAN を終了し、プライマリ VLAN として設定する必要があります。
- セカンダリ VLAN を終了し、独立 VLAN またはコミュニティ VLAN として設定する必要があります。

（注）　関連付けが動作していることを確認するには、**show** コマンドを使用します。関連付けが動作していないとき、スイッチはエラー メッセージを表示しません。（設定確認の詳細については、「プライベート VLAN 設定の確認」セクション（7-11 ページ）を参照してください）。

プライマリ VLAN またはセカンダリ VLAN を削除すると、その VLAN に関連付けされたポートは非アクティブになります。VLAN を通常モードに戻すには、**no private-vlan** コマンドを使用します。その VLAN におけるすべてのプライマリとセカンダリの関連付けは一時停止しますが、インターフェイスはプライベート VLAN モードのままです。VLAN をプライベート VLAN モードに戻すときには、元のアソシエーションが戻されます。

プライマリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN に関連付けされたすべてのプライベート VLAN は失われます。ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力した場合、その VLAN とプライベート VLAN の関連付けは一時停止します。この VLAN を再作成して以前のセカンダリ VLAN として設定すると元に戻ります。

セカンダリ VLAN とプライマリ VLAN の関連付けを変更するには、現在の関連付けを削除してから目的の関連付けを追加します。

プライベート VLAN におけるブロードキャスト トラフィックの概要

プライベート VLAN にあるポートからのブロードキャスト トラフィックは、次のように流れます。

- ブロードキャスト トラフィックは、プライマリ VLAN で、無差別ポートからすべてのポート（コミュニティ VLAN と独立 VLAN にあるすべてのポートも含む）に流れます。このブロードキャスト トラフィックは、プライベート VLAN パラメータで設定されていないポートを含め、プライマリ VLAN 内のすべてのポートに配信されます。
- 独立ポートからのブロードキャスト トラフィックは、独立ポートにアソシエートされているプライマリ VLAN にある無差別ポートにのみ配信されます。
- コミュニティ ポートからのブロードキャスト トラフィックは、そのポートのコミュニティ内のすべてのポート、およびそのコミュニティ ポートに関連付けられているすべての無差別ポートに配信されます。ブロードキャスト パケットは、プライマリ VLAN 内の他のコミュニティにも、いずれの独立ポートにも、配信されません。

プライベート VLAN ポート隔離の概要

プライベート VLAN を使用すると、次のように、エンド ステーションへのアクセスを制御できます。

- 通信を防止するには、エンド ステーションに接続されているインターフェイスのうち、選択したインターフェイスを、独立ポートとして設定します。たとえば、エンド ステーションがサーバの場合、この設定により、サーバ間の通信が防止されます。
- デフォルト ゲートウェイおよび選択したエンド ステーション（バックアップ サーバなど）に接続されているインターフェイスを無差別ポートとして設定し、すべてのエンド ステーションがデフォルト ゲートウェイにアクセスできるようにします。

プライベート VLAN の設定

（注）　指定 VLAN をプライベート VLAN として割り当てるには、VLAN をすでに作成している必要があります。

この項では、次のトピックについて取り上げます。

- プライベート VLAN の設定についての注意事項（7-6 ページ）
- プライベート VLAN のイネーブル化（7-6 ページ）
- プライベート VLAN としての VLAN の設定（7-7 ページ）
- セカンダリ VLAN とプライマリ プライベート VLAN の関連付け（7-8 ページ）
- プライベート VLAN ホスト ポートとしてのインターフェイスの設定（7-9 ページ）
- プライベート VLAN の無差別ポートとしてのインターフェイスの設定（7-10 ページ）

プライベート VLAN の設定についての注意事項

プライベート VLAN を設定する場合は、次の注意事項に従ってください。

- スイッチがプライベート VLAN 機能を適用するには、プライベート VLAN をイネーブルにする必要があります。
- プライベート VLAN モードで動作しているポートがスイッチに含まれる場合、プライベート VLAN をディセーブルにできません。
- セカンダリ VLAN を、同じ Multiple Spanning Tree（MST）インスタンスにプライマリ VLAN としてマッピングするには、**private-vlan synchronize** コマンドを入力します。詳細については、「プライベート VLAN でセカンダリ VLAN をプライマリ VLAN として同じ MSTI にマッピングするには」セクション（9-16 ページ）を参照してください。

プライベート VLAN のイネーブル化

プライベート VLAN 機能を使用するには、プライベート VLAN をスイッチでイネーブルにする必要があります。

（注）　プライベート VLAN コマンドは、プライベート VLAN 機能をイネーブルにするまで表示されません。

プライベート VLAN 機能をスイッチでイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# feature private-vlan`	プライベート VLAN 機能をスイッチでイネーブルにします。

次の例は、プライベート VLAN 機能をスイッチでイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# feature private-vlan
```

プライベート VLAN の機能をディセーブルにする手順は、次のとおりです。

コマンド	目的
`switch(config)# no feature private-vlan`	プライベート VLAN 機能をスイッチでディセーブルにします。 **（注）** プライベート VLAN モードで動作しているポートがスイッチに含まれる場合、プライベート VLAN をディセーブルにできません。

プライベート VLAN としての VLAN の設定

プライベート VLAN を作成するには、まず VLAN を作成し、次に、VLAN をプライベート VLAN に設定します。プライベート VLAN 機能がイネーブルであることを確認してください。

プライベート VLAN を作成する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# vlan {vlan-id | vlan-range}`	VLAN 設定サブモードにします。
ステップ 3	`switch(config-vlan)# private-vlan {community | isolated | primary}`	VLAN を、コミュニティ VLAN、独立 VLAN、またはプライマリ プライベート VLAN として設定します。プライベート VLAN には、1 つのプライマリ VLAN を設定する必要があります。複数のコミュニティ VLAN と独立 VLAN を設定することができます。

次の例は、VLAN 5 をプライマリ VLAN としてプライベート VLAN に割り当てる方法を示しています。

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# private-vlan primary
```

次の例は、VLAN 100 をコミュニティ VLAN としてプライベート VLAN に割り当てる方法を示しています。

```
switch(config-vlan)# exit
switch(config)# vlan 100
switch(config-vlan)# private-vlan community
```

次の例は、VLAN 109 を独立 VLAN としてプライベート VLAN に割り当てる方法を示しています。

```
switch(config-vlan)# exit
switch(config)# vlan 109
switch(config-vlan)# private-vlan isolated
```

プライベート VLAN をディセーブルにする手順は、次のとおりです。

コマンド	目的
switch(config-vlan)# **no private-vlan** {**community** | **isolated** | **primary**}	指定した VLAN からプライベート VLAN の設定を削除し、通常の VLAN モードに戻します。プライマリ VLAN またはセカンダリ VLAN を削除すると、その VLAN に関連付けされたポートは非アクティブになります。

セカンダリ VLAN とプライマリ プライベート VLAN の関連付け

セカンダリ VLAN をプライマリ VLAN とアソシエートするときには、次の事項に注意してください。

- *secondary-vlan-list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目は、単一のセカンダリ VLAN ID、またはセカンダリ VLAN ID をハイフンでつないだ範囲にできます。
- *secondary-vlan-list* パラメータには、複数のコミュニティ VLAN ID と独立 VLAN ID を含めることができます。
- セカンダリ VLAN をプライマリ VLAN にアソシエートするには、*secondary-vlan-list* と入力するか、*secondary-vlan-list* に **add** キーワードを使用します。
- セカンダリ VLAN とプライマリ VLAN とのアソシエーションをクリアするには、*secondary-vlan-list* に **remove** キーワードを使用します。
- セカンダリ VLAN とプライマリ VLAN とのアソシエーションを変更するには、既存のアソシエーションを削除し、次に必要なアソシエーションを追加します。

プライマリ VLAN またはセカンダリ VLAN を削除すると、その VLAN に関連付けされたポートは非アクティブになります。**no private-vlan** コマンドを入力すると、VLAN は通常の VLAN モードに戻ります。その VLAN におけるすべてのプライマリとセカンダリの関連付けは一時停止しますが、インターフェイスはプライベート VLAN モードのままです。指定した VLAN をプライベート VLAN モードに再変換すると、元のアソシエーションが戻されます。

プライマリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN に関連付けされたすべてのプライベート VLAN は失われます。ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力した場合、その VLAN とプライベート VLAN の関連付けは一時停止します。この VLAN を再作成して以前のセカンダリ VLAN として設定すると元に戻ります。

プライベート VLAN 機能がイネーブルであることを確認してください。

セカンダリ VLAN をプライマリ VLAN に関連付けるには、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **vlan** *primary-vlan-id*	プライベート VLAN 設定の操作対象のプライマリ VLAN の番号を入力します。
ステップ 3	switch(config-vlan)# **private-vlan association** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}	セカンダリ VLAN をプライマリ VLAN に関連付けます。

次の例は、コミュニティ VLAN 100 ～ 103 および独立 VLAN 109 をプライマリ VLAN 5 と関連付ける方法を示しています。

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# private-vlan association 100-103, 109
```

プライベート VLAN からすべてのアソシエーションを削除する手順は、次のとおりです。

コマンド	目的
`switch(config-vlan)# no private-vlan association`	プライマリ VLAN からすべてのアソシエーションを削除し、通常の VLAN モードに戻します。

プライベート VLAN ホスト ポートとしてのインターフェイスの設定

インターフェイスは、プライベート VLAN ホスト ポートとして設定できます。プライベート VLAN では、ホスト ポートがセカンダリ VLAN の一部です。セカンダリ VLAN は、コミュニティ VLAN または独立 VLAN のいずれかです。次に、ホスト ポートを、プライマリ VLAN とセカンダリ VLAN の両方にアソシエートします。

（注） ホスト ポートとして設定したすべてのインターフェイスで BPDU ガードをイネーブルにすることを推奨します。BPDU ガードの設定の詳細については、第 10 章「STP 拡張機能の設定」を参照してください。

プライベート VLAN 機能がイネーブルであることを確認してください。

インターフェイスをプライベート VLAN ホスト ポートとして設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface type slot/port`	プライベート VLAN ホスト ポートとして設定するポートを選択します。インターフェイスには、物理イーサネット ポートを指定できます。
ステップ 3	`switch(config-if)# switchport mode private-vlan host`	プライベート VLAN のホスト ポートとしてポートを設定します。
ステップ 4	`switch(config-if)# switchport private-vlan host-association {primary-vlan-id} {secondary-vlan-id}`	ポートを、プライベート VLAN のプライマリ VLAN とセカンダリ VLAN にアソシエートします。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかとして設定できます。

次の例は、プライベート VLAN のホスト ポートとしてイーサネット ポート 1/12 を設定し、プライマリ VLAN 5 とセカンダリ VLAN 101 にそのポートを関連付ける方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/12
switch(config-if)# switchport mode private-vlan host
switch(config-if)# switchport private-vlan host-association 5 101
```

プライベート VLAN のアソシエーションをインターフェイスから削除する手順は、次のとおりです。

コマンド	目的
switch(config-if)# **no switchport private-vlan host-association**	プライベート VLAN のアソシエーションをポートから削除します。

プライベート VLAN の無差別ポートとしてのインターフェイスの設定

インターフェイスは、プライベート VLAN 無差別ポートとして設定できます。次に、無差別ポートをプライマリ VLAN とセカンダリ VLAN とアソシエーションできます。

プライベート VLAN 機能がイネーブルであることを確認してください。

インターフェイスをプライベート VLAN 無差別ポートとして設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** *type slot/port*	プライベート VLAN 無差別ポートとして設定するポートを選択します。物理インターフェイスが必要です。
ステップ 3	switch(config-if)# **switchport mode private-vlan promiscuous**	プライベート VLAN の無差別ポートとしてポートを設定します。物理イーサネット ポートのみを、無差別ポートとしてイネーブルにできます。
ステップ 4	switch(config-if)# **switchport private-vlan mapping** {*primary-vlan-id*} {*secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list*}	ポートを無差別ポートとして設定し、プライマリ VLAN と、セカンダリ VLAN の選択リストに、指定したポートをアソシエートします。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかとして設定できます。

次の例は、無差別ポートとしてポート 1/2 を設定し、プライマリ VLAN 5 およびセカンダリ独立 VLAN 109 にそのポートを関連付ける方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# switchport mode private-vlan promiscuous
switch(config-if)# switchport private-vlan mapping 5 109
```

このコマンドは、物理インターフェイスにのみ使用できます。

プライベート VLAN のマッピングをクリアにする手順は、次のとおりです。

コマンド	目的
switch(config-if)# **no switchport private-vlan mapping**	プライベート VLAN から、マッピングをクリアします。

プライベート VLAN 設定の確認

プライベート VLAN 設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
switch# **show system internal clis feature**	スイッチでイネーブルになっている機能を表示します。
switch# **show vlan private-vlan** [**type**]	プライベート VLAN のステータスを表示します。
switch# **show interface switchport**	スイッチ ポートとして設定されているすべてのインターフェイスの情報を表示します。

次に、プライベート VLAN の設定を表示する例を示します。

```
switch# show vlan private-vlan
Primary  Secondary  Type             Ports
-------  ---------  ---------------  ------------------------------------------
5        100        community
5        101        community        Eth1/12, veth1/1
5        102        community
5        103        community
5        109        isolated         Eth1/2
switch# show vlan private-vlan type
Vlan Type
---- -----------------
5    primary
100  community
101  community
102  community
103  community
109  isolated
```

次に、イネーブルの機能を表示する例を示します。

```
switch# show system internal clis feature
 7 pvlan                          enabled
```

CHAPTER 8

Rapid PVST+ の設定

スパニングツリー プロトコル（STP）は、ループのないネットワークを提供するために実装しました。Rapid per VLAN Spanning Tree（Rapid PVST+）は STP を更新した実装であり、VLAN ごとに 1 つのスパニングツリー トポロジを作成できます。Rapid PVST+ は、スイッチのデフォルト STP モードです。

この章は、次の項で構成されています。

- Rapid PVST+ について（8-1 ページ）
- Rapid PVST+ の設定（8-18 ページ）
- Rapid PVST+ の設定の確認（8-27 ページ）

（注） このマニュアルでは、IEEE 802.1w および IEEE 802.1s を指す用語として、「スパニングツリー」を使用します。IEEE 802.1D STP について説明している箇所では、802.1D と明記します。Multiple Spanning Tree（MST）の詳細については、第 9 章「MST の設定」を参照してください。STP 拡張機能の詳細については、第 10 章「STP 拡張機能の設定」を参照してください。

Rapid PVST+ について

ここでは、VLAN ごとに実装されている Rapid PVST+ プロトコルである IEEE 802.1w 標準の高速スパニングツリー プロトコル（RSTP）について説明します。Rapid PVST+ は、IEEE 802.1D 規格との相互運用が可能で、VLAN ごとではなく、すべての VLAN で、単一の STP インスタンスの役割を委任されます（「Rapid PVST+ と IEEE 802.1Q トランク」セクション（8-16 ページ）を参照してください）。

Rapid PVST+ は、デフォルト VLAN（VLAN1）と、ソフトウェアで新たに作成された新しい VLAN でデフォルトでイネーブルになります。Rapid PVST+ は、レガシー IEEE 802.1D STP が実行されているスイッチと、相互運用されます（「Rapid PVST+ のレガシー 802.1D STP との相互運用」セクション（8-17 ページ）を参照）。

RSTP は、元の STP 規格 802.1D の拡張版で、より高速な収束が可能です。

ここでは、Rapid PVST+ の概要について説明します。この章の内容は次のとおりです。

- STP の概要（8-2 ページ）
- Rapid PVST+ の概要（8-6 ページ）
- Rapid PVST+ のレガシー 802.1D STP との相互運用（8-17 ページ）
- Rapid PVST+ の 802.1s MST との相互運用（8-17 ページ）

STP の概要

RSTP、Rapid PVST+、MST はすべて、元の IEEE 802.1D STP の拡張版です（MST の詳細は、第 9 章「MST の設定」を参照してください）。STP はレイヤ 2 のループ防止プロトコルで、パスの冗長性を実現しながら、ネットワークにおける不必要なループを防止します。

ここでは、STP の概要に関する次の内容について説明します。

- 概要（8-2 ページ）
- トポロジ形成の概要（8-2 ページ）
- ブリッジ ID の概要（8-3 ページ）
- BPDU の概要（8-5 ページ）
- ルート ブリッジの選定（8-5 ページ）
- スパニングツリー トポロジーの作成（8-6 ページ）

概要

イーサネット ネットワークが適切に動作するには、任意の 2 つのステーション間のアクティブ パスは 1 つだけでなければなりません。STP の動作はエンド ステーションに対してトランスペアレントなので、単一の LAN セグメントに接続されているのか、それとも複数セグメントからなるスイッチド LAN に接続されているのかを、エンド ステーションが検知することはできません。

フォールトトレラントなインターネットワークを作成する場合、ネットワーク上のすべてのノード間にループフリー パスを構築する必要があります。STP アルゴリズムでは、スイッチド ネットワーク中で、ループのない最適のパスが計算されます。LAN ポートでは、定期的な間隔で、ブリッジ プロトコル データ ユニット（BPDU）と呼ばれる STP フレームの送受信が実行されます。スイッチはこのフレームを転送しませんが、このフレームを使って、ループの発生しないパスを実現します。

エンド ステーション間に複数のアクティブ パスがあると、ネットワーク内でループが発生する原因になります。ネットワークにループがあると、エンド ステーションがメッセージを重複して受信したり、複数の LAN ポートでエンド ステーションの MAC アドレスをスイッチが認識してしまうことがあります。このような状態になるとブロードキャスト ストームが発生し、ネットワークが不安定になります。

STP では、ルート ブリッジでツリーを定義し、ルートからネットワーク内のすべてのスイッチへ、ループのないパスを定義します。STP は冗長データパスを強制的にブロック状態にします。スパニングツリーのネットワーク セグメントに障害が発生した場合、冗長パスがあると、STP アルゴリズムにより、スパニングツリー トポロジが再計算され、ブロックされたパスがアクティブになります。

スイッチの 2 つの LAN ポートで同じ MAC アドレスを認識することでループが発生している場合は、STP ポートのプライオリティとポート パス コストの設定により、フォワーディング ステートになるポートと、ブロッキング ステートになるポートが決定されます。

トポロジ形成の概要

スパニングツリーを構成している、拡張 LAN のスイッチはすべて、BPDU を交換することによって、ネットワーク内の他のスイッチについての情報を収集します。この BPDU の交換により、次のアクションが発生します。

- そのスパニングツリー ネットワーク トポロジでルート スイッチが 1 台選択されます。
- LAN セグメントごとに指定スイッチが 1 台選定されます。

- 冗長なインターフェイスをバックアップ ステートにする（スイッチド ネットワークの任意の箇所からルート スイッチに到達するために必要としないパスをすべて STP ブロック ステートにする）ことにより、スイッチド ネットワークのループをすべて解除します。

アクティブなスイッチド ネットワーク上のトポロジは、次の情報によって決定されます。

- 各スイッチにアソシエートされている、スイッチの一意なスイッチ識別情報である MAC アドレス
- 各インターフェイスにアソシエートされているルートのパス コスト
- 各インターフェイスにアソシエートされているポートの識別情報

スイッチド ネットワークでは、ルート スイッチが論理的にスパニングツリー トポロジの中心になります。STP では、BPDU を使用して、スイッチド ネットワークのルート スイッチやルート ポート、および、各スイッチド セグメントのルート ポートや指定ポートが選定されます。

ブリッジ ID の概要

それぞれのスイッチの各 VLAN には固有の 64 ビット ブリッジ ID があります。この ID は、ブリッジ プライオリティ値、拡張システム ID（IEEE 802.1t）、STP MAC アドレス割り当てから構成されます。

ここでは、次の内容について説明します。

- ブリッジ プライオリティ値（8-3 ページ）
- 拡張システム ID（8-3 ページ）
- STP MAC アドレスの割り当て（8-4 ページ）

ブリッジ プライオリティ値

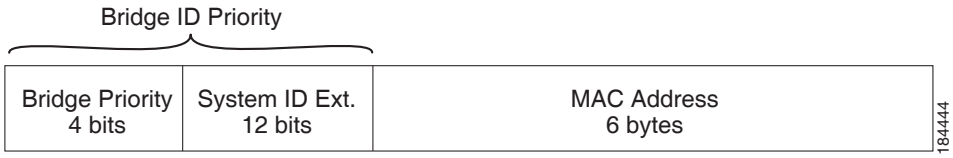
ブリッジのプライオリティは、拡張システム ID がイネーブルにされているときの 4 ビットの値です（「VLAN の Rapid PVST+ のブリッジ プライオリティの設定」セクション（8-24 ページ）を参照）。

（注） Cisco NX-OS では、拡張システム ID が常にイネーブルであり、拡張システム ID をディセーブルにできません。

拡張システム ID

12 ビットの拡張システム ID フィールドは、ブリッジ IDの一部です（図 8-1 を参照）。

図 8-1　拡張システム ID 付きのブリッジ ID



スイッチは 12 ビットの拡張システム ID を常に使用します。

システム ID の拡張は、ブリッジ ID と組み合わされ、VLAN の一意の識別情報として機能します（表 8-1 を参照）。

表 8-1　拡張システム ID がイネーブルの場合のブリッジ プライオリティ値および拡張システム ID

ブリッジ プライオリティ値				拡張システム ID（VLAN ID と同設定）											
ビット 16	ビット 15	ビット 14	ビット 13	ビット 12	ビット 11	ビット 10	ビット 9	ビット 8	ビット 7	ビット 6	ビット 5	ビット 4	ビット 3	ビット 2	ビット 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

STP MAC アドレスの割り当て

（注）　拡張システム ID と MAC アドレス削減は、ソフトウェア上で常にイネーブルです。

任意のスイッチの MAC アドレス削減がイネーブルの場合、不要なルート ブリッジの選定とスパニングツリー トポロジの問題を避けるため、他のすべての接続スイッチでも、MAC アドレス削減をイネーブルにする必要があります。

MAC アドレス リダクションをイネーブルにすると、ルート ブリッジ プライオリティは、4096 + VLAN ID の倍数となります。スイッチのブリッジ ID（最小の優先ルート ブリッジを特定するために、スパニングツリー アルゴリズムによって使用される）は、4096 の倍数を指定します。指定できるのは次の値だけです。

- 0
- 4096
- 8192
- 12288
- 16384
- 20480
- 24576
- 28672
- 32768
- 36864
- 40960
- 45056
- 49152
- 53248
- 57344
- 61440

STP は、拡張システム ID および MAC アドレスを使用して、VLAN ごとにブリッジ ID を一意にします。

（注）　同じスパニングツリー ドメインにある別のブリッジで MAC アドレス削減機能が実行されていない場合、そのブリッジのブリッジ ID と、MAC アドレス削減機能で指定されている値のいずれかが一致する可能性があり、その場合はそのブリッジがルート ブリッジとして機能することになります。

BPDU の概要

スイッチは STP インスタンス全体にブリッジ プロトコル データ ユニット（BPDU）を送信します。各スイッチにより、コンフィギュレーション BPDU が送信され、スパニングツリー トポロジの通信が行われ、計算されます。各コンフィギュレーション BPDU に含まれる最小限の情報は、次のとおりです。

- 送信するスイッチによりルート ブリッジが特定される、スイッチの一意なブリッジ ID
- ルートまでの STP パス コスト
- 送信側ブリッジのブリッジ ID
- メッセージ エージ
- 送信側ポートの ID
- Hello タイマー、転送遅延タイマー、最大エージング タイム プロトコル タイマー
- STP 拡張プロトコルの追加情報

スイッチにより Rapid PVST+ BPDU フレームが送信されるときには、フレームの送信先の VLAN に接続されているすべてのスイッチで、BPDU を受信します。スイッチで BPDU を受信するときに、スイッチによりフレームは送信されませんが、フレームにある情報を使用して BPDU が計算されます。トポロジが変更される場合は、BPDU の送信が開始されます。

BPDU 交換によって次の処理が行われます。

- 1 つのスイッチがルート ブリッジとして選択されます。
- ルート ブリッジへの最短距離は、パス コストに基づいてスイッチごとに計算されます。
- LAN セグメントごとに指定ブリッジが選択されます。これは、ルート ブリッジに最も近いスイッチで、そのスイッチを介してフレームがルートに転送されます。
- ルート ポートが選択されます。これはブリッジからルート ブリッジまでの最適パスを提供するポートです。
- スパニングツリーに含まれるポートが選択されます。

Rapid PVST+ によって BPDU に追加されるフィールドの詳細については、「Rapid PVST+ BPDU」セクション（8-8 ページ）を参照してください。

ルート ブリッジの選定

各 VLAN では、最も大きいブリッジ ID（つまり、最小の ID の数値）のスイッチが、ルート ブリッジとして選択されます。すべてのスイッチがデフォルトのプライオリティ（32768）で設定されている場合、その VLAN で最小の MAC アドレスを持つスイッチが、ルート ブリッジになります。ブリッジ プライオリティ値はブリッジ ID の最上位ビットを占めます。

ブリッジのプライオリティの値を変更すると、スイッチがルート ブリッジとして選定される可能性を変更することになります。小さい値を設定するほどその可能性が大きくなり、大きい値を設定するほどその可能性は小さくなります。

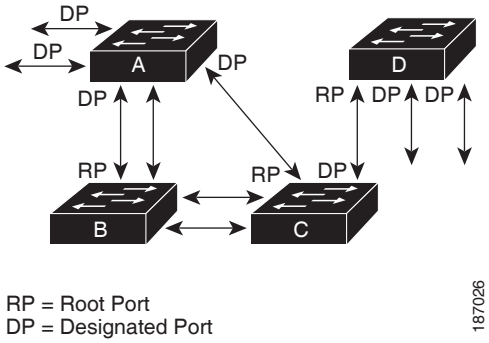
STP ルート ブリッジは論理的に、ネットワークで各スパニングツリー トポロジの中心です。ネットワークの任意の箇所からルート ブリッジに到達するために必要ではないすべてのパスは、STP ブロッキング モードになります。

BPDU には、送信側ブリッジおよびそのポートについて、ブリッジおよび MAC アドレス、ブリッジ プライオリティ、ポート プライオリティ、パス コストなどの情報が含まれます。STP では、この情報を使用して、STP インスタンス用のルート ブリッジを選定し、ルート ブリッジに導くルート ポートを選択し、各セグメントの指定ポートを特定します。

スパニングツリー トポロジーの作成

図 8-2 では、すべてのスイッチのブリッジのプライオリティがデフォルト（32768）に設定されているため、また、スイッチ A に最小 MAC アドレスがあるため、ルート ブリッジとしてスイッチ A が選択されています。ただし、トラフィック パターン、転送ポートの数、またはリンク タイプによっては、スイッチ A が最適なルート ブリッジであるとは限りません。任意のスイッチのプライオリティを高くする（数値を小さくする）ことでそのスイッチがルート ブリッジになるようにします。これにより STP が強制的に再計算され、そのスイッチをルートとする新しいスパニングツリー トポロジが形成されます。

図 8-2　　スパニングツリー トポロジー



スパニングツリー トポロジがデフォルトのパラメータに基づいて算出された場合、スイッチドネットワークの送信元エンド ステーションから宛先エンド ステーションまでのパスが最適にならない場合があります。たとえば、現在のルート ポートよりも数値の大きいポートに高速リンクを接続すると、ルート ポートが変更される場合があります。最高速のリンクをルート ポートにすることが重要です。

たとえば、スイッチ B の 1 つのポートが光ファイバ リンクであり、同じスイッチの別のポート（シールドなしツイストペア（UTP）リンク）がルート ポートになっていると仮定します。ネットワーク トラフィックを高速の光ファイバ リンクに流した方が効率的です。光ファイバ ポートの STP ポート プライオリティをルート ポートよりも高いプライオリティに変更すると（数値を下げる）、光ファイバ ポートが新しいルート ポートになります。

Rapid PVST+ の概要

ここでは、Rapid PVST+ tの内容について説明します。

- 概要（8-7 ページ）
- Rapid PVST+ BPDU（8-8 ページ）
- 提案と合意のハンドシェイク（8-9 ページ）
- プロトコル タイマー（8-10 ページ）
- ポートのロール（8-10 ページ）
- ポート ステート（8-11 ページ）
- ポートの役割の同期（8-13 ページ）
- 単一方向リンク障害の検出（8-15 ページ）
- ポート コスト（8-15 ページ）
- ポートのプライオリティ（8-16 ページ）

概要

Rapid PVST+ は、VLAN ごとに実装されている IEEE 802.1w（RSTP）規格です。（手作業で STP をディセーブルにしていない場合、）STP の 1 つのインスタンスは、設定されている各 VLAN で実行されます。VLAN 上の各 Rapid PVST+ インスタンスには、1 つのルート スイッチがあります。Rapid PVST+ の実行中には、VLAN ベースで STP をイネーブルまたはディセーブルにできます。

（注）　Rapid PVST+ は、スイッチでのデフォルト STP モードです。

Rapid PVST+ では、ポイントツーポイントの配線を使用して、スパニングツリーの高速収束が行われます。Rapid PVST+ によりスパニングツリーの再設定を 1 秒未満に発生させることができます（802.1D STP のデフォルト設定では 50 秒）。

（注）　Rapid PVST+ では、VLAN ごとに 1 つの STP インスタンスがサポートされます。

Rapid PVST+ を使用すると、STP コンバージェンスが急速に発生します。STP にある各指定ポートまたは各ルート ポートにより、デフォルトで、2 秒ごとに BPDU が送信されます。トポロジの指定ポートまたはルート ポートで、hello メッセージが 3 回連続失われた場合、または、最大経過時間の期限が切れた場合、ポートでは、すべてのプロトコル情報がテーブルにただちにフラッシュされます。ポートでは、3 つの BPDU が失われるか、最大経過時間の期限が切れた場合、直接のネイバー ルートまたは指定ポートへの接続が失われたと見なされます。プロトコル情報の急速な経過により、障害検出を迅速に行うことができます。スイッチは PVID を自動的に確認します。

Rapid PVST+ により、ネットワーク デバイス、スイッチ ポート、または LAN の障害の直後に、接続が迅速に回復されます。RSTP は、エッジ ポート、新しいルート ポート、およびポイントツーポイント リンクで接続されているポートに次のような高速コンバージェンスを提供します。

- エッジ ポート：RSTP スイッチにあるエッジ ポートとしてポートを設定する場合、エッジ ポートでは、フォワーディング ステートにただちに移行します（この急速な移行は、PortFast と呼ばれていたシスコ特有の機能でした）。エッジ ポートとして 1 つのエンド ステーションに接続されているポートにのみ、設定する必要があります。エッジ ポートでは、リンクの変更時にはトポロジの変更は生成されません。

  STP エッジ ポートとしてポートを設定するには、**spanning-tree port type** インターフェイス コンフィギュレーション コマンドを入力します。

  （注）　ホストに接続されているすべてのポートを、エッジ ポートとして設定することを推奨します。STP ポート タイプについての詳細は、第 10 章「STP 拡張機能の設定」を参照してください。

- ルート ポート：Rapid PVST+ により新しいルート ポートが選択された場合、古いポートがブロックされ、新しいルート ポートがただちにフォワーディング ステートに移行します。
- ポイントツーポイント リンク：ポイントツーポイント リンクによってあるポートと別のポートを接続することでローカル ポートが指定ポートになると、提案合意ハンドシェイクを使用して他のポートと急速な移行がネゴシエートされ、トポロジにループがなくなります。

Rapid PVST+ では、エッジ ポートとポイントツーポイント リンクでのみ、フォワーディング ステートへの急速な移行が達成されます。リンク タイプは設定が可能ですが、システムでは、ポートのデュプレックス設定からリンク タイプ情報が自動的に引き継がれます。全二重ポートはポイントツーポイント ポートであると見なされ、半二重ポートは共有ポートであると見なされます。

エッジ ポートでは、トポロジの変更は生成されませんが、直接接続されているネイバーから 3 回連続 BPDU の受信に失敗するか、最大経過時間のタイム アウトが発生すると、他のすべての指定ポートとルート ポートにより、トポロジ変更（TC）BPDU が生成されます。この時点で、指定ポートまたはルート ポートにより、TC フラグがオンに設定された状態で BPDU が送信されます。BPDU では、ポート上で TC While タイマーが実行されている限り、TC フラグが設定され続けます。TC While タイマーの値は、hello タイムに 1 秒を加えて設定された値です。トポロジ変更の初期ディテクタにより、トポロジ全体で、この情報がフラッディングされます。

Rapid PVST+ により、トポロジの変更が検出される場合、プロトコルでは次の処理が発生します。

- すべての非エッジ ルート ポートと指定ポートで、必要に応じ、hello タイムの 2 倍の値で TC While タイマーが開始されます。
- これらのすべてのポートにアソシエートされている MAC アドレスがフラッシュされます。

トポロジ変更通知は、トポロジ全体で迅速にフラッディングされます。システムでトポロジの変更が受信されると、システムにより、ポート ベースでダイナミック エントリがただちにフラッシュされます。

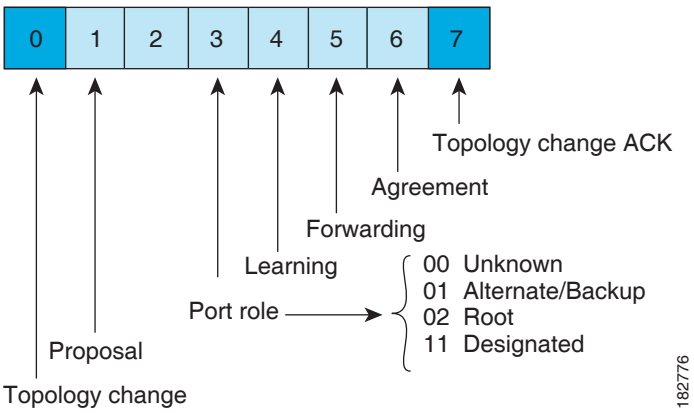
（注）　スイッチが、レガシー 802.1D STP を実行しているスイッチと相互に動作しているときにのみ、TCA フラグが使用されます。Rapid PVST+ の 802.1D STP との相互動作についての詳細は、「Rapid PVST+ のレガシー 802.1D STP との相互運用」セクション（8-17 ページ）を参照してください。

次に、提案と合意のシーケンスがネットワークのエッジに迅速に伝搬され、トポロジ変更後の接続が迅速に戻されます（「ポートの役割の同期」セクション（8-13 ページ）を参照）。

Rapid PVST+ BPDU

Rapid PVST+ と 802.1w では、フラグ バイトの 6 ビットすべてを使用して、BPDU の送信元のポートのロールおよびステートと、提案や合意のハンドシェイクが追加されます。図 8-3 に、Rapid PVST+ の BPDU フラグの用途について示します。

図 8-3　BPDU の Rapid PVST+ フラグ バイト

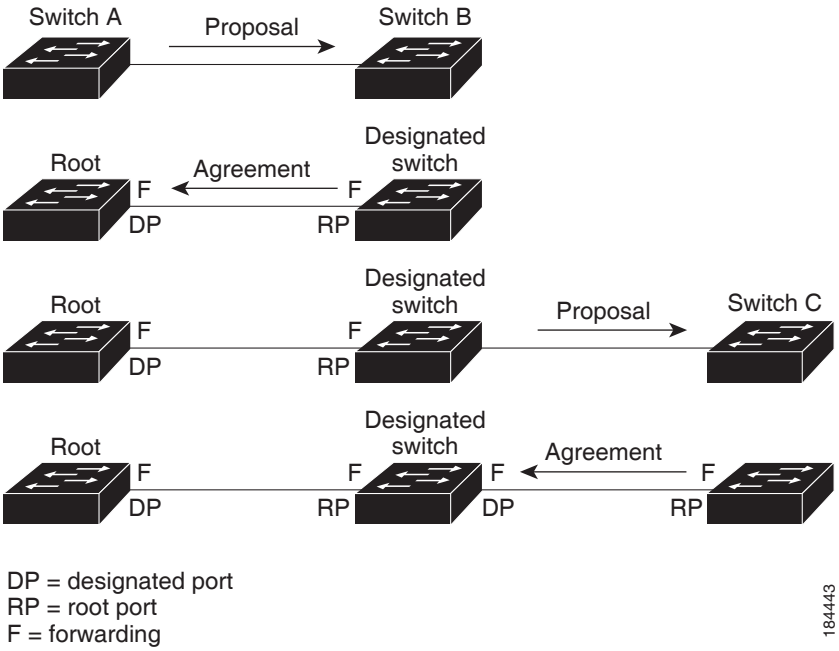


もう一つの重要な変更点は、Rapid PVST+ BPDU がタイプ 2、バージョン 2 であることで、これにより、スイッチでは、接続されているレガシー（802.1D）ブリッジを検出できるようになります。802.1D の BPDU は、バージョン 0 です。

提案と合意のハンドシェイク

図 8-4 で示したように、スイッチ A は、ポイントツーポイント リンクを介してスイッチ B に接続され、すべてのポートがブロッキング ステートになります。このとき、スイッチ A のプライオリティが、スイッチ B のプライオリティよりも小さい数値であるとします。

図 8-4　高速コンバージェンスの提案と合意のハンドシェーク



スイッチ A がスイッチ B に提案メッセージ（プロポーザル フラグがオンに設定されたコンフィギュレーション BPDU）を送信します。これにより、スイッチ A が指定スイッチとして提案されます（図 8-4 を参照）。

提案メッセージの受信後、スイッチ B は、その新しいルート ポートとして、提案メッセージが受信されたポートからポートを選択し、すべての非エッジ ポートをブロッキング ステートにし、新しいルート ポートを使って合意メッセージ（合意フラグがオンに設定された BPDU）を送信します。

スイッチ B から合意 メッセージの受信後、スイッチ A でも、その指定ポートがただちにフォワーディング ステートに移行されます。スイッチ B ですべての非エッジ ポートがブロックされ、スイッチ A とスイッチ B の間にポイントツーポイント リンクがあるため、ネットワークではループは形成できません（ポート ステートの詳細については、「ポート ステート」セクション（8-11 ページ）を参照してください）。

スイッチ C がスイッチ B に接続されると、類似したハンドシェイク メッセージのセットがやり取りされます。スイッチ C は、そのルート ポートとしてスイッチ B に接続されたポートを選択し、リンクの両端がただちにフォワーディング ステートになります。このハンドシェイク処理の繰り返しごとに、さらに 1 つのネットワーク デバイスがアクティブなトポロジに参加します。ネットワークの収束時には、この提案と合意のハンドシェーク処理がスパニング ツリーのルートからリーフに進みます。

スイッチは、ポート デュプレックス モードからリンク タイプを認識します。全二重ポートはポイントツーポイント接続であると見なされ、半二重ポートは共有接続であると見なされます。デュプレックス設定によって制御されるデフォルト設定は、**spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを入力することで上書きできます。

この提案合意ハンドシェイクが開始されるのは、非エッジ ポートがブロッキング ステートからフォワーディング ステートに移行するときだけです。次に、ハンドシェイク処理は、トポロジ全体に段階的に広がります。

プロトコル タイマー

表 8-2 では、Rapid PVST+ のパフォーマンスに影響を及ぼすプロトコル タイマーについて説明しています。

表 8-2　Rapid PVST+ のプロトコル タイマー

変数	説明
ハロー タイマー	各スイッチから他のスイッチに BPDU をブロードキャストする頻度を決定します。デフォルトは 2 秒で、範囲は 1 ～ 10 です。
転送遅延タイマー	ポートが転送を開始するまでの、リスニング ステートおよびラーニング ステートが継続する時間を決定します。このタイマーは通常、プロトコルによっては使用されませんが、バックアップとして使用されます。デフォルトは 15 秒で、範囲は 4 ～ 30 秒です。
最大エージング タイマー	ポートで受信したプロトコル情報がスイッチで保存される時間を決めます。このタイマーは通常、プロトコルによっては使用されませんが、802.1D スパニングツリーと相互に動作するときに使用されます。デフォルトは 20 秒で、範囲は 6 ～ 40 秒です

ポートのロール

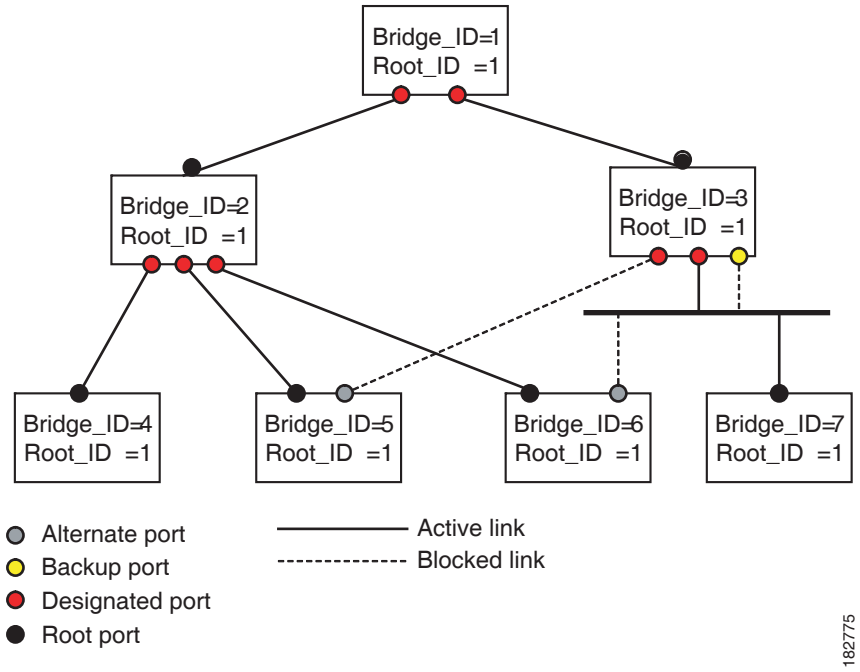
Rapid PVST+ では、ポート ロールを割り当て、アクティビティ トポロジを認識することによって、高速収束が行われます。「ルート ブリッジの選定」セクション（8-5 ページ）で説明しているように、Rapid PVST+ は、802.1D STP に構築され、最高のプライオリティ（最小数値のプライオリティの値）のスイッチがルート ブリッジとして選択されます。Rapid PVST+ により、次のポートのロールの 1 つが個々のポートに割り当てられます。

- ルート ポート：スイッチによりパケットがルート ブリッジに転送されるときに、最適のパス（最小コスト）を用意します。
- 指定ポート：指定スイッチに接続します。指定スイッチでは、LAN からルート ブリッジにパケットが転送されるときに、発生するパス コストが最小になります。指定スイッチが LAN に接続するポートのことを指定ポートと呼びます。
- 代替ポート：現在のルート ポートによって用意されているパスに、ルート ブリッジへの代替パスを用意します。代替ポートにより、トポロジにある別のスイッチへのパスが確保されます。
- バックアップ ポート：指定ポートが提供した、スパニング ツリーのリーフに向かうパスのバックアップとして機能します。バックアップ ポートが存在できるのは、2 つのポートがポイントツーポイント リンクよってループバックで接続されている場合、または 1 つのスイッチに共有 LAN セグメントへの接続が 2 つ以上ある場合です。バックアップ ポートにより、スイッチに対する別のパスがトポロジ内で確保されます。
- ディセーブル ポート：スパニング ツリーの動作において何もロールが与えられていません。

ネットワーク全体でポートのロールに一貫性のある安定したトポロジでは、Rapid PVST+ により、ルート ポートと指定ポートがすべてただちにフォワーディング ステートになり、代替ポートとバックアップ ポートはすべて、必ずブロッキング ステートになります。指定ポートはブロッキング ステートで開始されます。ポートのステートにより、転送処理および学習処理の動作が制御されます。

ルート ポートまたは指定ポートのロールを持つポートは、アクティブなトポロジに含まれます。代替ポートまたはバックアップ ポートのロールを持つポートは、アクティブなトポロジから除外されます（図 8-5を参照）。

図 8-5　　ポートのロールをデモンストレーションするトポロジのサンプル



ポート ステート

ここでは、Rapid PVST+ および MST のポート ステートについて説明します。

- Rapid PVST+ ポート ステートの概要（8-11 ページ）
- ブロッキング ステート（8-12 ページ）
- ラーニング ステート（8-12 ページ）
- フォワーディング ステート（8-13 ページ）
- ディセーブル ステート（8-13 ページ）
- ポート ステートの概要（8-13 ページ）

Rapid PVST+ ポート ステートの概要

プロトコル情報がスイッチド LAN を通過するとき、伝播遅延が生じることがあります。その結果、スイッチド ネットワークのさまざまな時点および場所でトポロジーの変化が発生します。スパニングツリー トポロジで LAN ポートが非伝搬ステートからフォワーディング ステートに直接移行する際、一時的にデータがループすることがあります。ポートは新しいトポロジー情報がスイッチド LAN 経由で伝播されるまで待機し、それからフレーム転送を開始する必要があります。

Rapid PVST+ または MST を使用しているソフトウェア上の各 LAN ポートは、次の 4 つのステートの 1 つで終了します。

- ブロッキング：LAN ポートはフレーム転送に参加しません。
- ラーニング：LAN ポートは、フレーム転送への参加を準備します。

- フォワーディング:LAN ポートはフレームを転送します。
- ディセーブル:LAN ポートは STP に参加せず、フレームを転送しません。

Rapid PVST+ をイネーブルにすると、ソフトウェアのすべてのポート、VLAN、ネットワークは、電源投入時にブロッキング ステートからラーニングの移行ステートに進みます。各 LAN ポートは、適切に設定されていれば、フォワーディング ステートまたはブロッキング ステートで安定します。

STP アルゴリズムにより LAN ポートがフォワーディング ステートになると、次の処理が発生します。

1. ラーニング ステートに進む必要があることを示すプロトコル情報を待つ間、LAN ポートはブロッキング ステートになります。
2. LAN ポートは転送遅延タイマーの期限が切れるのを待ち、ラーニング ステートに移行し、転送遅延タイマーを再開します。
3. ラーニング ステートでは、LAN ポートはフォワーディング データベースのエンド ステーション位置情報をラーニングする間、フレームの転送をブロックし続けます。
4. LAN ポートは転送遅延タイマーの期限が切れるのを待って、フォワーディング ステートに移行します。このフォワーディング ステートでは、ラーニングとフレーム転送がイネーブルになります。

ブロッキング ステート

ブロッキング ステートにある LAN ポートはフレームを転送しません。

ブロッキング ステートの LAN ポートでは、次の処理が実行されます。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- エンド ステーションの場所は、そのアドレス データベースには取り入れません(ブロッキング LAN ポートではラーニングがないため、アドレス データベースは更新されません)。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから送られた BPDU を受信し、処理して送信します。
- ネットワーク管理メッセージを受信して応答します。

ラーニング ステート

ラーニング ステートにある LAN ポートは、フレームの MAC アドレスをラーニングすることによって、フレーム転送の準備をします。LAN ポートは、ブロッキング ステートからラーニング ステートになります。

ラーニング ステートの LAN ポートでは、次の処理が実行されます。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- エンド ステーションの場所を、そのアドレス データベースに取り入れます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから送られた BPDU を受信し、処理して送信します。
- ネットワーク管理メッセージを受信して応答します。

フォワーディング ステート

フォワーディング ステートにある LAN ポートでは、フレームを転送します。LAN ポートは、ラーニング ステートからフォワーディング ステートになります。

フォワーディング ステートの LAN ポートでは、次の処理が実行されます。

- 接続セグメントから受信したフレームを転送します。
- 転送用に他のポートからスイッチングされたフレームを転送します。
- エンド ステーションの場所情報を、そのアドレス データベースに取り入れます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから受信した BPDU を処理します。
- ネットワーク管理メッセージを受信して応答します。

ディセーブル ステート

ディセーブル ステートにある LAN ポートは、フレーム転送または STP は行いません。ディセーブル ステートの LAN ポートは、実質的に動作が停止しています。

ディセーブルの LAN ポートでは、次の処理が実行されます。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- エンド ステーションの場所は、そのアドレス データベースには取り入れません（ラーニングは行われないため、アドレス データベースは更新されません）。
- ネイバーから BPDU を受信しません。
- システム モジュールから送信用の BPDU を受信しません。

ポート ステートの概要

表 8-3 に、ポートおよびそれに対応してアクティブ トポロジに含められる、可能性のある動作と Rapid PVST+ のステートのリストを示します。

表 8-3　アクティブなトポロジのポート ステート

動作ステータス	ポート ステート	ポートがアクティブ トポロジに含まれているか
Enabled	Blocking	No
Enabled	Learning	Yes
Enabled	Forwarding	Yes
Disabled	Disabled	No

ポートの役割の同期

スイッチがいずれかのポートで提案メッセージを受信し、そのポートが新しいルート ポートとして選択されると、Rapid PVST+ は、強制的に、すべての他のポートと新しいルート情報との同期をとります。

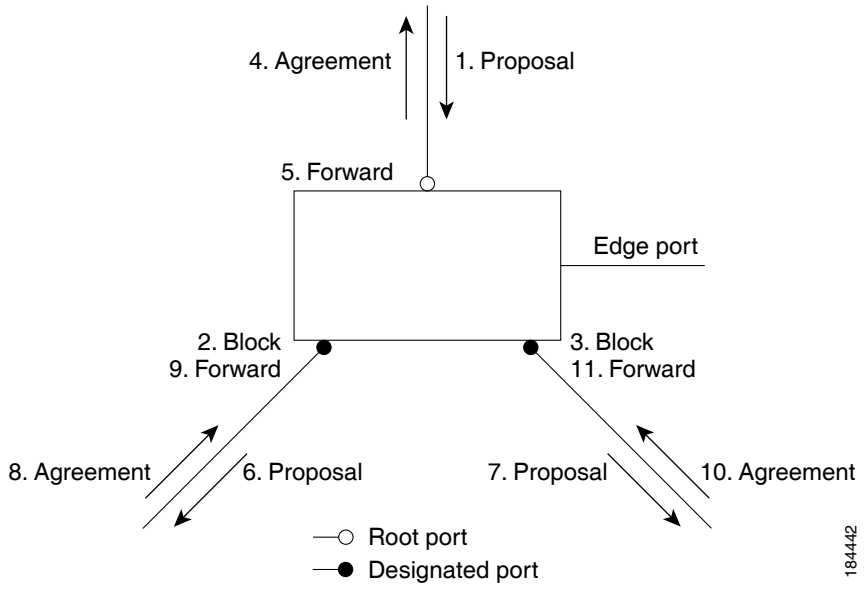
他のすべてのポートが同期化されると、スイッチはルート ポートで受信した優位のルート情報に同期化されます。次のいずれかが当てはまる場合、スイッチ上の個々のポートで同期がとられます。

- ポートがブロッキング ステートである。
- エッジ ポートである（ネットワークのエッジに存在するように設定されたポート）。

指定ポートがフォワーディング ステートの場合で、エッジ ポートとして設定されていない場合、Rapid PVST+ により強制的に新しいルート情報との同期がとられるときに、ブロッキング ステートに移行します。一般的に、Rapid PVST+ により、強制的にルート情報との同期がとられる場合で、ポートで前述の条件のいずれかが満たされない場合、ポート ステートはブロッキングに設定されます。

すべてのポートで同期がとられた後で、スイッチから、ルート ポートに対応する指定スイッチへ、合意メッセージが送信されます。ポイントツーポイント リンクで接続されているスイッチが、そのポートのロールについての合意に存在する場合、Rapid PVST+ により、ポート ステートがただちにフォワーディング ステートに移行します。イベントのシーケンスについては、図 8-6 を参照してください。

図 8-6　　高速コンバージェンス中のイベントのシーケンス



上位 BPDU 情報の処理

上位 BPDU とは、自身のために現在保存されているものより上位であるルート情報（より小さいスイッチ ID、より小さいパス コストなど）を持つ BPDU のことです。

上位 BPDU がポートで受信されると、Rapid PVST+ は再設定を起動します。そのポートが新しいルート ポートとして提案、選択されている場合、Rapid PVST+ は残りすべてのポートを同期させます。

受信した BPDU が提案フラグの設定された Rapid PVST+ BPDU の場合、スイッチは残りすべてのポートを同期させたあと、合意メッセージを送信します。前のポートがブロッキング ステートになるとすぐに、新しいルート ポートがフォワーディング ステートに移行します。

ポートで受信した上位情報によりポートがバックアップ ポートまたは代替ポートになる場合、Rapid PVST+ はポートをブロッキング ステートに設定し、合意メッセージを送信します。指定ポートは、転送遅延タイマーが期限切れになるまで、提案フラグが設定された BPDU を送信し続けます。期限切れになると、ポートはフォワーディング ステートに移行します。

下位 BPDU 情報の処理

下位 BPDU とは、自身のために現在保存されているものより下位であるルート情報（より大きいスイッチ ID、より大きいパス コストなど）を持つ BPDU のことです。

DP は、下位 BPDU を受信すると、独自の情報ですぐに応答します。

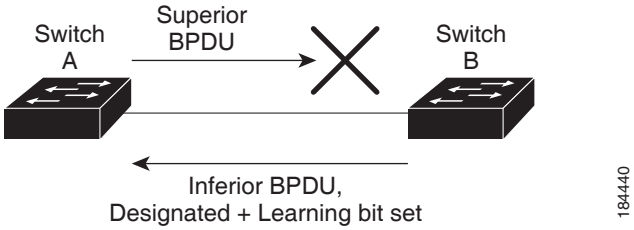
単一方向リンク障害の検出

ソフトウェアは、受信した BPDU でポートのロールおよびステートの一貫性をチェックし、ブリッジング ループの原因となることがある単方向リンク障害を検出します。

指定ポートは、矛盾を検出すると、そのロールを維持しますが、廃棄ステートに戻ります。一貫性がない場合は、接続を中断した方がブリッジング ループを解決できるからです。

図 8-7 に、一般的にブリッジング ループになる単一方向リンク障害を示します。スイッチ A はルート ブリッジであり、スイッチ B へのリンクで BPDU は失われます。802.1w-standard BPDU には、送信側ポートの役割と状態が含まれます。この情報により、送信する上位 BPDU に対してスイッチ B が反応しないこと、スイッチ B はルート ポートではなく指定ポートであることが、スイッチ A によって検出できます。結果として、スイッチ A は自身のポートをブロックし（またはブロックを維持して）、ブリッジ処理のループを回避します。ブロックは、STP の矛盾として示されます。

図 8-7　　単一方向リンク障害の検出



ポート コスト

（注）　Rapid PVST+ では、デフォルトで、ショート型（16 ビット）のパスコスト方式を使用して、コストが計算されます。ショート型のパスコスト方式では、1 ～ 65535 の範囲で値を割り当てることができます。ただし、ロング型（32 ビット）のパスコスト方式を使用するようにスイッチを設定することもできます。この場合、1 ～ 200,000,000 の範囲の値を割り当てることができます。パスコスト計算方式は、グローバルに設定します。

STP ポートのパスコストのデフォルト値は、メディア速度と LAN インターフェイスのパスコストの計算方式によって決まります（表 8-4 を参照）。ループが発生した場合、STP では、LAN インターフェイスの選択時に、フォワーディング ステートにするためのポート コストを考慮します。

表 8-4　デフォルトのポート コスト

帯域幅	ポート コストのショート パスコスト方式	ポート コストのロング パスコスト方式
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 ギガビット イーサネット	4	20,000
10 ギガビット イーサネット	2	2,000

STP に最初に選択させたい LAN インターフェイスには低いコスト値を、最後に選択させたい LAN インターフェイスには高いコスト値を割り当てることができます。すべての LAN インターフェイスが同じコスト値を使用している場合には、STP は LAN インターフェイス番号が最も小さい LAN インターフェイスをフォワーディング ステートにして、残りの LAN インターフェイスをブロックします。

アクセス ポートでは、ポートごとにポート コストを割り当てます。トランク ポートでは VLAN ごとにポート コストを割り当てるため、トランク ポート上のすべての VLAN に同じポート コストを設定できます。

ポートのプライオリティ

ループが発生し、複数のポートに同じパス コストが割り当てられている場合、Rapid PVST+ では、フォワーディング ステートにする LAN ポートの選択時に、ポートのプライオリティを考慮します。Rapid PVST+ に最初に選択させる LAN ポートには小さいプライオリティ値を割り当て、Rapid PVST+ に最後に選択させる LAN ポートには大きいプライオリティ値を割り当てます。

すべての LAN ポートに同じプライオリティ値が割り当てられている場合、Rapid PVST+ は、LAN ポート番号が最小の LAN ポートをフォワーディング ステートにし、他の LAN ポートをブロックします。有効なプライオリティの範囲は 0 ～ 224（デフォルトは 128）で、32 ずつ増やして設定できます。LAN ポートがアクセス ポートとして設定されているときはポートのプライオリティ値が使用され、LAN ポートがトランク ポートとして設定されているときは VLAN ポートのプライオリティ値が使用されます。

Rapid PVST+ と IEEE 802.1Q トランク

802.1Q トランクによって、ネットワークの STP の構築方法に、いくつかの制約が課されます。Cisco スイッチを 802.1Q トランクで接続しているネットワークでは、スイッチは、トランクの VLAN ごとに STP のインスタンスを 1 つ維持します。ただし、非 Cisco 802.1Q スイッチでは、トランクのすべての VLAN に対して維持する STP のインスタンスは 1 つだけです。

802.1Q トランクで Cisco スイッチを非 Cisco スイッチに接続している場合は、Cisco スイッチにより、トランクの 802.1Q VLAN の STP インスタンスが、非 Cisco 802.1Q スイッチの STP インスタンスと組み合わされます。ただし、Cisco スイッチで維持されている VLAN ごとの STP 情報はすべて、非シスコ 802.1Q スイッチのクラウドによって分けられます。Cisco スイッチを分ける非 Cisco 802.1Q クラウドは、スイッチ間の単一のトランク リンクとして扱われます。

Rapid PVST+ のレガシー 802.1D STP との相互運用

Rapid PVST+ は、レガシー 802.1D プロトコルを実行中のスイッチと相互に動作させることができます。スイッチが BPDU バージョン 0 を受信すると、802.1D を実行中の機器と相互に動作していることを認識します。Rapid PVST+ の BPDU はバージョン 2 です。受信した BPDU が、提案フラグがオンに設定された 802.1w BPDU バージョン 2 の場合、スイッチは残りすべてのポートを同期させたあと、合意メッセージを送信します。受信した BPDU が 802.1D BPDU バージョン 0 の場合は、スイッチは提案フラグを設定せずに、ポートの転送遅延タイマーを開始します。新しいルート ポートでは、フォワーディング ステートに移行するために、2 倍の転送遅延時間が必要となります。

スイッチは、次のように、レガシー 802.1D スイッチと相互動作します。

- 通知：802.1D BPDU とは異なり 802.1w は、TCN BPDU を使用しません。ただし、802.1D スイッチとの相互運用のため、Cisco NX-OS では、TCN BPDU を処理し、生成します。
- 受信応答：802.1w スイッチでは、802.1D スイッチから指定ポート上に TCN メッセージを受信すると、TCA ビットを設定し、802.1D コンフィギュレーション BPDU で応答します。ただし、802.1D スイッチに接続されているルート ポートで TC While タイマー（802.1D の TC タイマーと同じ）がアクティブの場合、TCA がセットされたコンフィギュレーション BPDU を受信すると、TC While タイマーはリセットされます。

  動作のこの方式は、802.1D スイッチでのみ必要です。802.1w BPDU では、TCA ビットは設定されません。
- プロトコル移行：802.1D スイッチとの下位互換性のために、802.1w は、802.1D コンフィギュレーション BPDU と TCN BPDU をポートごとに選択的に送信します。

  ポートが初期化されると、移行遅延タイマー（802.1w BPDU が送信される最小時間を指定）が開始され、802.1w BPDU が送信されます。このタイマーがアクティブな間、スイッチはそのポートで受信したすべての BPDU を処理し、プロトコル タイプを無視します。

  ポート移行遅延タイマーの期限切れ後にスイッチで 802.1D BPDU を受信した場合は、802.1D スイッチに接続していると見なして、802.1D BPDU のみを使用して開始します。ただし、802.1w スイッチが、ポート上で 802.1D BPDU を使用中で、タイマーの期限切れ後に 802.1w BPDU を受信すると、タイマーが再起動され、ポート上の 802.1w BPDU を使用して開始されます。

（注）　すべてのスイッチでプロトコルを再ネゴシエーションするには、Rapid PVST+ を再起動する必要があります。詳細については、「プロトコルの再開」セクション（8-26 ページ）を参照してください。

Rapid PVST+ の 802.1s MST との相互運用

Rapid PVST+ は、IEEE 802.1s マルチ スパニングツリー（MST）規格とシームレスに相互運用されます。ユーザによる設定は不要です。

Rapid PVST+ の設定

Rapid PVST+ プロトコルには 802.1w 規格が適用されていますが、Rapid PVST+ は、ソフトウェアのデフォルト STP 設定です。

Rapid PVST+ は VLAN ごとにイネーブルにします。STP のインスタンスが VLAN ごとに維持されます（STP をディセーブルにした VLAN を除く）。デフォルトで Rapid PVST+ は、デフォルト VLAN と、作成した各 VLAN でイネーブルになります。

この項では、次のトピックについて取り上げます。

- Rapid PVST+ のイネーブル化（8-18 ページ）
- Rapid PVST+ の VLAN ベースの イネーブル化（8-19 ページ）
- ルート ブリッジ ID の設定（8-20 ページ）
- セカンダリ ルート ブリッジの設定（8-21 ページ）
- Rapid PVST+ のポート プライオリティの設定（8-22 ページ）
- Rapid PVST+ のパス コスト方式とポート コストの設定（8-23 ページ）
- VLAN の Rapid PVST+ のブリッジ プライオリティの設定（8-24 ページ）
- VLAN の Rapid PVST+ の hello タイムの設定（8-24 ページ）
- VLAN の Rapid PVST+ の転送遅延時間の設定（8-25 ページ）
- VLAN の Rapid PVST+ の最大経過時間の設定（8-25 ページ）
- リンク タイプの設定（8-25 ページ）
- プロトコルの再開（8-26 ページ）

Rapid PVST+ のイネーブル化

スイッチ上で Rapid PVST+ をイネーブルにすると、指定されている VLAN で Rapid PVST+ をイネーブルにする必要があります（「Rapid PVST+ の VLAN ベースの イネーブル化」セクション（8-19 ページ）を参照）。

Rapid PVST+ はデフォルトの STP モードです。MST と Rapid PVST+ は同時には実行できません。

（注）　スパニングツリー モードを変更すると、変更前のモードのスパニングツリー インスタンスがすべて停止されて新しいモードで起動されるため、トラフィックが中断する場合があります。

スイッチで Rapid PVST+ をイネーブルにする手順は次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree mode rapid-pvst`	スイッチで Rapid PVST+ をイネーブルにします。Rapid PVST+ はデフォルトのスパニングツリー モードです。 **（注）** スパニングツリー モードを変更すると、変更前のモードのスパニングツリー インスタンスがすべて停止されて新しいモードで起動されるため、トラフィックが中断する場合があります。

次の例は、スイッチで Rapid PVST+ をイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mode rapid-pvst
```

（注） STP はデフォルトでイネーブルのため、設定結果を参照するために **show running** コマンドを入力しても、Rapid PVST+ をイネーブルするために入力したコマンドは表示されません。

Rapid PVST+ の VLAN ベースの イネーブル化

Rapid PVST+ は、VLAN ごとにイネーブルまたはディセーブルにできます。

（注） Rapid PVST+ は、デフォルト VLAN と、作成したすべての VLAN でデフォルトでイネーブルになります。

VLAN ごとに Rapid PVST+ をイネーブルにする手順は次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree vlan-range`	VLAN ごとに Rapid PVST+（デフォルト STP）をイネーブルにします。*vlan-range* の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。第 6 章「VLAN の設定」を参照してください。

次の例は、VLAN 5 で STP をイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5
```

VLAN ごとに Rapid PVST+ をディセーブルにする手順は次のとおりです。

コマンド	目的
`switch(config)# no spanning-tree vlan-range`	指定した VLAN で Rapid PVST+ をディセーブルにします。このコマンドについては次の注意を参照してください。

注意 VLAN のすべてのスイッチおよびブリッジでスパニングツリーがディセーブルになっていない場合は、VLAN でスパニングツリーをディセーブルにしないでください。スパニングツリーは、VLAN の一部のスイッチおよびブリッジでディセーブルにしておきながら、VLAN のその他のスイッチおよびブリッジでイネーブルにしておくことはできません。スパニングツリーをイネーブルにしたスイッチとブリッジに、ネットワークの物理トポロジに関する不完全な情報が含まれることになるので、この処理によって予想外の結果となることがあります。

VLAN に物理ループが存在しないことを確認せずに、VLAN でスパニング ツリーをディセーブルにしないでください。スパニングツリーは、設定の誤りおよび配線の誤りに対する保護手段として動作します。

ルート ブリッジ ID の設定

Rapid PVST+ では、STP のインスタンスはアクティブな VLAN ごとに管理されます。各 VLAN では、最も小さいブリッジ ID を持つスイッチが VLAN のルート ブリッジになります。

特定の VLAN インスタンスがルート ブリッジになるように設定するには、そのブリッジのプライオリティをデフォルト値（32768）よりかなり小さい値に変更します。

spanning-tree vlan *vlan_ID* **root** コマンドを入力すると、各 VLAN で現在ルートになっているブリッジのブリッジ プライオリティがスイッチによって確認されます。スイッチは指定した VLAN のブリッジ プライオリティを 24576 に設定します（このスイッチがその VLAN のルートになる値）。指定した VLAN のいずれかのルート ブリッジに 24576 より小さいブリッジ プライオリティが設定されている場合は、スイッチはその VLAN のブリッジ プライオリティを、最小のブリッジ プライオリティより 4096 だけ小さい値に設定します。

（注） ルート ブリッジになるために必要な値が 1 より小さい場合は、**spanning-tree vlan** *vlan_ID* **root** コマンドはエラーになります。

注意 STP の各インスタンスのルート ブリッジは、バックボーン スイッチまたはディストリビューション スイッチでなければなりません。アクセス スイッチは、STP のプライマリ ルートとして設定しないでください。

キーワード **diameter** を入力し、ネットワーク直径（ネットワーク内の任意の 2 つのエンド ステーション間での最大ブリッジ ホップ数）を指定します。ネットワーク直径を指定すると、その直径のネットワークに最適な hello タイム、転送遅延時間、最大エージング タイムが自動的に選択されます。これにより、STP コンバージェンスの時間が大幅に削減されます。キーワード **hello-time** を入力すると、自動的に計算された hello タイムを上書きできます。

（注）　ルート ブリッジとして設定されているスイッチでは、hello タイム、転送遅延時間、最大エージング タイムは手動で設定（**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、**spanning-tree mst max-age** の各グローバル コンフィギュレーション コマンドを使用）しないでください。

Rapid PVST+ で VLAN のプライマリ ルート ブリッジになるようにスイッチを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree vlan vlan-range root primary [diameter dia [hello-time hello-time]]`	ソフトウェア スイッチをプライマリ ルート ブリッジとして設定します。*vlan-range* の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。*dia* のデフォルトは 7 です。*hello-time* の範囲は 1 ～ 10 秒で、デフォルト値は 2 秒です。

次の例は、ネットワーク直径を 4 にして、スイッチを VLAN 5 のルート ブリッジとして設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 root primary diameter 4
```

セカンダリ ルート ブリッジの設定

ソフトウェア スイッチをセカンダリ ルートとして設定しているときに、STP ブリッジのプライオリティをデフォルト値（32768）から変更しておくと、プライマリ ルート ブリッジに障害が発生した場合に、そのスイッチが、指定した VLAN のルート ブリッジになります（ネットワークの他のスイッチで、デフォルトのブリッジ プライオリティ 32768 が使用されているとします）。STP により、ブリッジ プライオリティが 28672 に設定されます。

キーワード **diameter** を入力し、ネットワーク直径（ネットワーク内の任意の 2 つのエンド ステーション間での最大ブリッジ ホップ数）を指定します。ネットワーク直径を指定すると、その直径のネットワークに最適な hello タイム、転送遅延時間、最大エージング タイムが自動的に選択されます。これにより、STP コンバージェンスの時間が大幅に削減されます。キーワード **hello-time** を入力すると、自動的に計算された hello タイムを上書きできます。

複数のスイッチに対して同様に設定すれば、複数のバックアップ ルート ブリッジを設定できます。プライマリ ルート ブリッジの設定時に使用した値と同じネットワーク直径と hello タイムの値を入力します。

（注）　ルート ブリッジとして設定されているスイッチでは、hello タイム、転送遅延時間、最大エージング タイムは手動で設定（**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、**spanning-tree mst max-age** の各グローバル コンフィギュレーション コマンドを使用）しないでください。

Rapid PVST+ で VLAN のセカンダリ ルート ブリッジになるようにスイッチを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree vlan vlan-range root secondary [diameter dia [hello-time hello-time]]`	ソフトウェア スイッチをセカンダリ ルート ブリッジとして設定します。*vlan-range* の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。*dia* のデフォルトは 7 です。*hello-time* の範囲は 1 ～ 10 秒で、デフォルト値は 2 秒です。

次の例は、ネットワーク直径を 4 にして、スイッチを VLAN 5 のセカンダリ ルート ブリッジとして設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 root secondary diameter 4
```

Rapid PVST+ のポート プライオリティの設定

Rapid PVST+ に最初に選択させる LAN ポートには小さいプライオリティ値を割り当て、Rapid PVST+ に最後に選択させる LAN ポートには大きいプライオリティ値を割り当てます。すべての LAN ポートに同じプライオリティ値が割り当てられている場合、Rapid PVST+ は、LAN ポート番号が最小の LAN ポートをフォワーディング ステートにし、他の LAN ポートをブロックします。

LAN ポートがアクセス ポートとして設定されているときはポートのプライオリティ値が使用され、LAN ポートがトランク ポートとして設定されているときは VLAN ポートのプライオリティ値が使用されます。

Rapid PVST+ のポート プライオリティを個々のポートに割り当てる手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface type slot/port`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# spanning-tree [vlan vlan-list] port-priority priority`	LAN インターフェイスのポート プライオリティを設定します。*priority* の値は 0 ～ 224 の範囲です。値が小さいほどプライオリティが高くなります。プライオリティ値は、0、32、64、96、128、160、192、224 です。その他の値はすべて拒否されます。デフォルト値は 128 です。

次の例は、イーサネット アクセス ポート 1/4 のポート プライオリティを 160 に設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree port-priority 160
```

このコマンドを使用できるのは、物理イーサネット インターフェイスに対してだけです。

Rapid PVST+ のパス コスト方式とポート コストの設定

アクセス ポートでは、ポートごとにポート コストを割り当てます。トランク ポートでは VLAN ごとにポート コストを割り当てるため、トランク上のすべての VLAN に同じポート コストを設定できます。

（注） Rapid PVST+ モードでは、ショート型またはロング型のいずれかのパス コスト方式を使用できます。この方式は、インターフェイスまたはコンフィギュレーション サブモードのいずれかで設定できます。デフォルトのパス コスト方式は、ショート型です。

Rapid PVST+ パスコスト方式およびポートのコストを設定する手順は次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree pathcost method {long | short}`	Rapid PVST+ パス コストの計算に使用される方式を選択します。デフォルト方式は short 型です。
ステップ 3	`switch(config)# interface type slot/port`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	`switch(config-if)# spanning-tree [vlan vlan-id] cost [value | auto]`	LAN インターフェイスのポート コストを設定します。コストの値は、パス コスト計算の方式により、次の値になります。 • ショート型:1 ～ 65535 • ロング型:1 ～ 200000000 （注） このパラメータは、アクセス ポートのポート別、およびトランク ポートの VLAN 別に設定します。 デフォルトは **auto** で、パス コスト計算方式とメディア速度の両方に基づいてポート コストが設定されます。

次の例は、イーサネット アクセス ポート 1/4 のポート コストを 1000 に設定する方法を示しています。

```
switch# configure terminal
switch (config)# spanning-tree pathcost method long
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree cost 1000
```

このコマンドを使用できるのは、物理イーサネット インターフェイスに対してだけです。

VLAN の Rapid PVST+ のブリッジ プライオリティの設定

VLAN の Rapid PVST+ のブリッジ プライオリティを設定できます。

（注）　この設定を使用するときは注意が必要です。ほとんどの場合、プライマリ ルートとセカンダリ ルートを設定して、ブリッジ プライオリティを変更することを推奨します。

特定の VLAN のブリッジ プライオリティを選択する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree vlan vlan-range priority value`	VLAN のブリッジ プライオリティを設定します。有効な値は 0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。その他の値はすべて拒否されます。デフォルト値は 32768 です。

次の例は、ギガビット イーサネット ポート 1/4 で VLAN 5 のプライオリティを 8192 に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 priority 8192
```

VLAN の Rapid PVST+ の hello タイムの設定

VLAN では、Rapid PVST+ の hello タイムを設定できます。

（注）　この設定を使用するときは注意が必要です。ほとんどの場合、プライマリ ルートとセカンダリ ルートを設定して、hello タイムを変更することを推奨します。

Rapid PVST+ の VLAN で hello タイムを設定にする手順は次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree vlan vlan-range hello-time value`	VLAN の hello タイムを設定します。hello タイムの値の範囲は 1 ～ 10 秒で、デフォルトは 2 秒です。

次の例は、VLAN 5 の hello タイムを 7 秒に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 hello-time 7
```

VLAN の Rapid PVST+ の転送遅延時間の設定

Rapid PVST+ の使用時は、VLAN ごとに転送遅延時間を設定できます。VLAN ごとに転送遅延時間を設定する手順は次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree vlan vlan-range forward-time value`	VLAN の転送遅延時間を設定します。転送遅延時間の値の範囲は 4 ～ 30 秒で、デフォルトは 15 秒です。

次の例は、VLAN 5 の転送遅延時間を 21 秒に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 forward-time 21
```

VLAN の Rapid PVST+ の最大経過時間の設定

Rapid PVST+ の使用時は、VLAN ごとに最大経過時間を設定できます。Rapid PVST+ の VLAN で最大経過時間を設定にする手順は次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree vlan vlan-range max-age value`	VLAN の最大エージング タイムを設定します。最大経過時間の値の範囲は 6 ～ 40 秒で、デフォルトは 20 秒です。

次の例は、VLAN 5 の最大エージング タイムを 36 秒に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 max-age 36
```

リンク タイプの設定

Rapid の接続性（802.1w 規格）は、ポイントツーポイントのリンク上でのみ確立されます。リンク タイプは、デフォルトでは、インターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続であると見なされ、半二重ポートは共有接続であると見なされます。

リモート スイッチの 1 つのポートに、ポイントツーポイントで物理的に接続されている半二重リンクがある場合、リンク タイプのデフォルト設定を上書きし、高速移行をイネーブルにできます。

リンクを共有に設定すると、STP は 802.1D に戻ります。

リンク タイプを指定する手順は次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** *type slot/port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **spanning-tree link-type** {**auto** | **point-to-point** | **shared**}	リンク タイプを、ポイントツーポイント インクまたは共有リンクに設定します。デフォルト値はスイッチ接続から読み取られ、半二重リンクは共有、全二重リンクはポイントツーポイントです。リンク タイプが共有の場合、STP は 802.1D に戻ります。デフォルトは auto で、インターフェイスのデュプレックス設定に基づいてリンク タイプが設定されます。

次の例は、リンク タイプをポイントツーポイント リンクとして設定する方法を示しています。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree link-type point-to-point
```

このコマンドを使用できるのは、物理イーサネット インターフェイスに対してだけです。

プロトコルの再開

レガシー ブリッジに接続されている場合、Rapid PVST+ を実行しているブリッジは、そのポートの 1 つに 802.1D BPDU を送信できます。ただし、STP プロトコルの移行では、レガシー スイッチが指定スイッチではない場合、レガシー スイッチがリンクから削除されたかどうかを認識できません。スイッチ全体または指定したインターフェイスでプロトコル ネゴシエーションを再開する（強制的に隣接スイッチと再ネゴシエーションさせる）ことができます。

プロトコル ネゴシエーションを再開する手順は次のとおりです。

コマンド	目的
switch# **clear spanning-tree detected-protocol** [**interface** *interface* [*interface-num* | *port-channel*]]	スイッチのすべてのインターフェイスまたは指定インターフェイスで Rapid PVST+ を再起動します。

次の例は、スロット 2、ポート 8 のイーサネット インターフェイスで Rapid PVST+ を再起動する方法を示しています。

```
switch# clear spanning-tree detected-protocol interface ethernet 2/8
```

Rapid PVST+ の設定の確認

Rapid PVST+ の設定情報を表示するには、次のいずれかの処理を実行します。

コマンド	目的
switch# **show running-config spanning-tree** [**all**]	現在のスパニングツリー設定を表示します。
switch# **show spanning-tree** [*options*]	最新のスパニングツリー設定について、指定した詳細情報を表示します。

次の例は、スパニングツリーのステータスの表示方法を示しています。

```
switch# show spanning-tree brief

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32768
             Address     001c.b05a.5447
             Cost        2
             Port        131 (Ethernet1/3)
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000d.ec6d.7841
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- -------------------------------
Eth1/3           Root FWD 2         128.131  P2p Peer(STP)
veth1/1          Desg FWD 2         128.129  Edge P2p
```

CHAPTER 9

MST の設定

IEEE 802.1s 標準である Multiple Spanning Tree（MST）では、複数の VLAN を 1 つのスパニングツリー インスタンスに割り当てることができます。MST は、デフォルトのスパニングツリー モードではありません。Rapid per VLAN Spanning Tree（Rapid PVST+）がデフォルト モードです。MST インスタンスは、同じ名前、リビジョン番号、VLAN からインスタンスへのマッピングと組み合わされて、MST 領域が形成されます。MST 領域は、領域外のスパニングツリー設定への単一のブリッジとして表示されます。MST は、近接スイッチから 802.1D メッセージを受信すると、IEEE 802.1D スパニングツリー プロトコル（STP）にフェールオーバーします。

（注） このマニュアルでは、IEEE 802.1w および IEEE 802.1s を指す用語として、「スパニングツリー」を使用します。IEEE 802.1D STP について説明している箇所では、802.1D と明記します。

この章は、次の項で構成されています。

- MST について（9-1 ページ）
- MST の設定（9-10 ページ）

（注） STP および Rapid PVST+ の詳細については第 8 章「Rapid PVST+ の設定」を、STP 拡張機能の詳細については第 10 章「STP 拡張機能の設定」を参照してください。

MST について

この項では、次のトピックについて取り上げます。

- MST の概要（9-2 ページ）
- MST リージョン（9-2 ページ）
- MST BPDU（9-3 ページ）
- MST 設定情報（9-3 ページ）
- IST、CIST、CST（9-4 ページ）
- ホップ カウント（9-7 ページ）
- 境界ポート（9-7 ページ）
- 単一方向リンク障害の検出（9-8 ページ）
- ポート コストとポート プライオリティ（9-8 ページ）

- IEEE 802.1D との相互運用性（9-9 ページ）
- Rapid PVST+ の相互運用性と PVST シミュレーションについて（9-9 ページ）

MST の概要

（注）MST をイネーブルにする必要があります。Rapid PVST+ は、デフォルトのスパニングツリー モードです。

MST は、複数の VLAN をスパニングツリー インスタンスにマッピングします。各インスタンスには、他のスパニングツリー インスタンスとは別のスパニングツリー トポロジがあります。このアーキテクチャでは、データ トラフィックに対して複数のフォワーディング パスがあり、ロード バランシングが可能です。これによって、非常に多数の VLAN をサポートする際に必要な STP インスタンスの数を削減できます。MST では、1 つのインスタンス（転送パス）で障害が発生しても他のインスタンス（転送パス）に影響しないため、ネットワークのフォールトトレランスが向上します。

MST では、各 MST インスタンスで IEEE 802.1w 規格を採用することによって、明示的なハンドシェイクによる高速コンバージェンスが可能なため、802.1D 転送遅延がなくなり、ルート ブリッジ ポートと指定ポートが迅速にフォワーディング ステートに変わります。（明示的なハンドシェイクの取り決めについての詳細は、第 8 章「Rapid PVST+ の設定」を参照してください）。

MST の使用中は、MAC アドレスの削減が常にイネーブルに設定されます（MAC アドレスの削減についての詳細は、第 8 章「Rapid PVST+ の設定」を参照してください）。この機能はディセーブルにはできません。

MST ではスパニング ツリーの動作が改善され、次の STP バージョンとの下位互換性を維持しています。

- 元の 802.1D スパニング ツリー
- Rapid per-VLAN スパニングツリー（Rapid PVST+）

（注）
- IEEE 802.1w では RSTP が定義されて、IEEE 802.1D に組み込まれました。
- IEEE 802.1s では MST が定義されて、IEEE 802.1Q に組み込まれました。

MST リージョン

スイッチが MSTI に参加できるようにするには、同一の MST 設定情報でスイッチの設定に整合性を持たせる必要があります（「MST 設定情報」セクション（9-3 ページ）を参照）。

同じ MST 設定の相互接続スイッチの集まりが MST リージョンです。MST リージョンは、同じ MST 設定で MST ブリッジのグループとリンクされます。

MST 設定により、各スイッチが属する MST リージョンが制御されます。この設定には、領域の名前、バージョン番号、MST VLAN とインスタンスの割り当てマップが含まれます。

リージョンには、同一の MST コンフィギュレーションを持った 1 つまたは複数のメンバが必要です。各メンバには、802.1w Bridge Protocol Data Unit（BPDU：ブリッジ プロトコル データ ユニット）を処理する機能が必要です。ネットワーク内の MST リージョンには、数の制限はありません。

各リージョンは、最大 65 の MST インスタンス（MSTI）までサポートします。インスタンスは、1 ～ 4094 の範囲の任意の番号によって識別されます。インスタンス 0 は、特別なインスタンスである IST 用に予約されています。VLAN は、一度に 1 つの MST インスタンスに対してのみ割り当てることができます。IST の詳細については、「IST、CIST、CST」セクション（9-4 ページ）を参照してください。

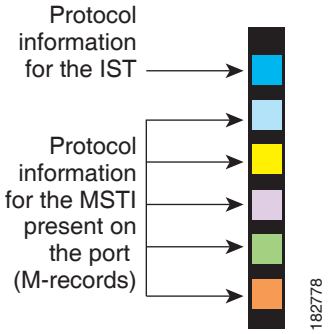
MST 領域は、隣接の MST 領域、他の Rapid PVST+ 領域、802.1D スパニングツリー プロトコルへの単一のブリッジとして表示されます。

（注）　ネットワークを、非常に多数の領域に分けることは推奨しません。

MST BPDU

1 つの領域に含まれる MST BPDU は 1 つだけで、その BPDU により、領域内の各 MSTI について M レコードが保持されます（図 9-1 を参照）。IST だけが MST 領域の BPDU を送信します。すべての M レコードは、IST が送信する 1 つの BPDU でカプセル化されています（IST の詳細については、「IST、CIST、CST の概要」セクション（9-4 ページ）を参照してください）。MST BPDU にはすべてのインスタンスに関する情報が保持されるため、MSTI をサポートするために処理する必要がある BPDU の数は、非常に少なくなります。

図 9-1　　MSTI の M レコードが含まれる MST BPDU



MST 設定情報

MST の設定は 1 つの MST リージョン内のすべてのスイッチで同一である必要があり、ユーザが設定します。

MST 設定の次の 3 つのパラメータを設定できます。

- 名前：32 文字の文字列。MST リージョンを指定します。ヌルで埋められ、ヌルで終了します。
- リビジョン番号：現在の MST 設定のリビジョンを指定する 16 ビットの符号なし数字。

（注）　MST 設定の一部として必要な場合、リビジョン番号を設定する必要があります。リビジョン番号は、MST 設定がコミットされるごとに自動的には増やされ*ません*。

- MST 設定テーブル：要素が 4096 あるテーブルで、サポート対象の、存在する可能性のある 4094 の各 VLAN を該当のインスタンスにアソシエートします。最初（0）と最後（4095）の要素は 0 に設定されています。要素番号 X の値は、VLAN X がマッピングされるインスタンスを表します。

注意　VLAN/MSTI マッピングを変更すると、MST は再起動されます。

MST BPDU には、これらの 3 つの設定パラメータが含まれています。MST ブリッジは、これら 3 つの設定パラメータが厳密に一致する場合、MST BPDU をそのリージョンに受け入れます。設定属性が 1 つでも異なっていると、MST ブリッジでは、BPDU が別の MST リージョンのものであると見なされます。

IST、CIST、CST

ここでは、Internal Spanning Tree（IST）、Common and Internal Spanning Tree（CIST）、Common Spanning Tree（CST）について説明します。

- IST、CIST、CST の概要（9-4 ページ）
- MST リージョン内でのスパニングツリーの動作（9-5 ページ）
- MST リージョン間のスパニングツリーの動作（9-5 ページ）
- MST 用語（9-6 ページ）

IST、CIST、CST の概要

すべての STP インスタンスが依存関係にない Rapid PVST+（第 8 章「Rapid PVST+ の設定」を参照）とは異なり、MST では、IST、CIST、CST の各スパニングツリーが次のように確立され、維持されます。

- IST は、MST 領域で実行されるスパニングツリーです。

  MST では、各 MST 領域内に追加のスパニングツリーが確立され、維持されます。これらのスパニングツリーを MSTI（複数スパニングツリー インスタンス）といいます。

  インスタンス 0 は、IST という、領域の特殊インスタンスです。IST は、すべてのポートに必ず存在します。IST（インスタンス 0）は削除できません。デフォルトでは、すべての VLAN が IST に割り当てられます。その他すべての MSTI には、1 ～ 4094 の番号が付きます。

  IST は、BPDU の送受信を行う唯一の STP インスタンスです。他の MSTI 情報はすべて MST レコード（M レコード）に含まれ、MST BPDU 内でカプセル化されます。

  同じリージョン内のすべての MSTI は同じプロトコル タイマーを共有しますが、各 MSTI には、ルート ブリッジ ID やルート パス コストなど、それぞれ独自のトポロジ パラメータがあります。

  MSTI は、リージョンに対してローカルです。たとえば、リージョン A とリージョン B が相互接続されている場合でも、リージョン A にある MSTI 9 は、リージョン B にある MSTI 9 には依存しません。

- CST は、MST リージョンと、ネットワーク上で実行されている可能性がある 802.1D および 802.1w STP のインスタンスを相互接続します。CST は、ブリッジ型ネットワーク全体で 1 つ存在する STP インスタンスで、すべての MST リージョン、802.1w インスタンスおよび 802.1D インスタンスを含みます。

- CIST は、各 MST リージョンにある IST の集まりです。CIST は、MST リージョン内部の IST や、MST リージョン外部の CST と同じです。

MST 領域で計算されるスパニングツリーは、スイッチ ドメイン全体を含んだ CST 内のサブツリーとして認識されます。CIST は、802.1w、802.1s、802.1D の各規格をサポートするスイッチで実行されているスパニングツリー アルゴリズムによって形成されています。MST リージョン内の CIST は、リージョン外の CST と同じです。

詳細については、「MST リージョン内でのスパニングツリーの動作」セクション（9-5 ページ）および「MST リージョン間のスパニングツリーの動作」セクション（9-5 ページ）を参照してください。

MST リージョン内でのスパニングツリーの動作

IST は、リージョンにあるすべての MST スイッチを接続します。IST が収束すると、IST のルートは CIST リージョナルのルートになります（図 9-2（9-6 ページ））。ネットワークに領域が 1 つしかない場合、CIST リージョナル ルートは CIST ルートにもなります。CIST ルートがリージョン外にある場合、リージョンの境界にある MST スイッチの 1 つが、CIST リージョナル ルートとしてプロトコルにより選択されます。

MST スイッチが初期化されると、スイッチ自体を識別する BPDU が、CIST のルートおよび CIST リージョナル ルートとして送信されます。このとき、CIST ルートと CIST リージョナル ルートへのパス コストは両方ゼロに設定されます。また、スイッチはすべての MSTI を初期化し、これらすべての MSTI のルートであることを示します。現在ポートに格納されている情報よりも上位の MST ルート情報（より小さいスイッチ ID、より小さいパス コストなど）をスイッチが受信すると、CIST リージョナル ルートとしての主張を撤回します。

初期化中に、MST リージョン内に独自の CIST リージョナル ルートを持つ多くのサブ リージョンが形成される場合があります。スイッチは、同じリージョンのネイバーから上位の IST 情報を受信すると、元のサブ リージョンを脱退して、真の CIST リージョナル ルートが含まれる新しいサブ リージョンに加入します。このようにして、真の CIST リージョナル ルートが含まれているサブ リージョン以外のサブ領域はすべて縮小します。

MST リージョン内のすべてのスイッチが同じ CIST リージョナル ルートを承認する必要があります。リージョン内にある任意の 2 つのスイッチは、共通 CIST リージョナル ルートに収束する場合、MSTI に対するポート ロールのみを同期します。

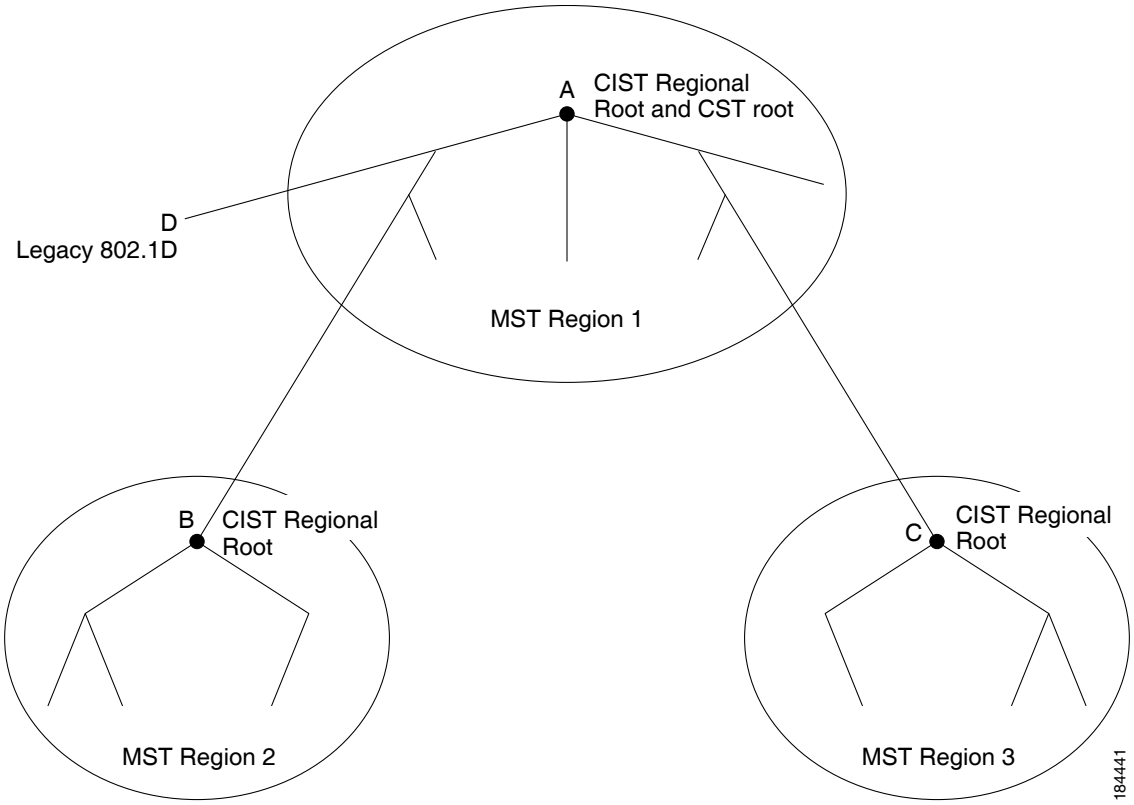
MST リージョン間のスパニングツリーの動作

ネットワーク内に複数の領域、または 802.1 w や 802.1D STP インスタンスがある場合、MST はネットワーク内のすべての MST 領域、すべての 802.1w と 802.1D STP スイッチを含む CST を確立して、維持します。MSTI は、リージョンの境界で IST と結合して CST になります。

IST は、リージョン内のすべての MST スイッチを接続し、スイッチ ドメイン全体を含んだ CIST 内のサブツリーとして認識されます。サブツリーのルートは CIST リージョナル ルートです。MST リージョンは、隣接する STP スイッチや MST リージョンからは仮想スイッチとして認識されます。

図 9-2 に、3 つの MST 領域と 802.1D（D）があるネットワークを示します。リージョン 1 の CIST リージョナル ルート（A）は、CIST ルートでもあります。リージョン 2 の CIST リージョナル ルート（B）、およびリージョン 3 の CIST リージョナル ルート（C）は、CIST 内のそれぞれのサブツリーのルートです。

図 9-2　MST リージョン、CIST リージョナル ルート、CST ルート



BPDU を送受信するのは CST インスタンスのみです。MSTI は、そのスパニングツリー情報を BPDU に（M レコードとして）追加し、隣接スイッチと相互作用して、最終的なスパニングツリー トポロジを計算します。このため、BPDU の送信に関連するスパニングツリー パラメータ（hello タイム、転送時間、最大エージング タイム、最大ホップ カウントなど）は、CST インスタンスにのみ設定されますが、すべての MSTI に影響します。スパニングツリー トポロジに関連するパラメータ（スイッチ プライオリティ、ポート VLAN コスト、ポート VLAN プライオリティなど）は、CST インスタンスと MSTI の両方に設定できます。

MST スイッチは、802.1D 専用スイッチと通信する場合、バージョン 3 BPDU または 802.1D STP BPDU を使用します。MST スイッチは、MST スイッチと通信する場合、MST BPDU を使用します。

MST 用語

MST の命名規則には、内部パラメータまたはリージョナル パラメータの識別情報が含まれます。これらのパラメータは MST 領域内だけで使用され、ネットワーク全体で使用される外部パラメータと比較されます。CIST だけがネットワーク全体に広がるスパニングツリー インスタンスなので、CIST パラメータだけに外部修飾子が必要になり、修飾子またはリージョン修飾子は不要です。MST 用語を次に示します。

- CIST ルートは CIST のルート ブリッジで、ネットワーク全体にまたがる一意のインスタンスです。
- CIST 外部ルート パス コストは、CIST ルートまでのコストです。このコストは MST 領域内で変化しません。MST リージョンは、CIST に対する唯一のスイッチのように見えます。CIST 外部ルート パス コストは、これらの仮想スイッチとリージョンに属していないスイッチ間を計算して出したルート パス コストです。

- CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。または、CIST リージョナル ルートがそのリージョンで CIST ルートに最も近いスイッチになります。CIST リージョナル ルートは、IST のルート ブリッジとして動作します。
- CIST 内部ルート パス コストは、領域内の CIST リージョナル ルートまでのコストです。このコストは IST（インスタンス 0）のみに関係します。

ホップ カウント

MST リージョン内の STP トポロジを計算する場合、MST はコンフィギュレーション BPDU のメッセージ有効期間と最大エージング タイムの情報は使用しません。代わりに、ルートへのパスコストと、IP の存続可能時間（TTL）メカニズムに類似したホップ カウント メカニズムを使用します。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用すると、領域内の最大ホップ数を設定し、IST およびその領域のすべての MSTI に適用できます。

ホップ カウントは、メッセージ エージ情報と同じ結果になります（再設定を開始）。インスタンスのルート ブリッジは、コストが 0 でホップ カウントが最大値に設定された BPDU（M レコード）を常に送信します。スイッチがこの BPDU を受信すると、受信 BPDU の残存ホップ カウントから 1 だけ差し引いた値を残存ホップ カウントとする BPDU を生成し、これを伝播します。このホップ カウントが 0 になると、スイッチはその BPDU を廃棄し、ポート用に維持されていた情報を期限切れにします。

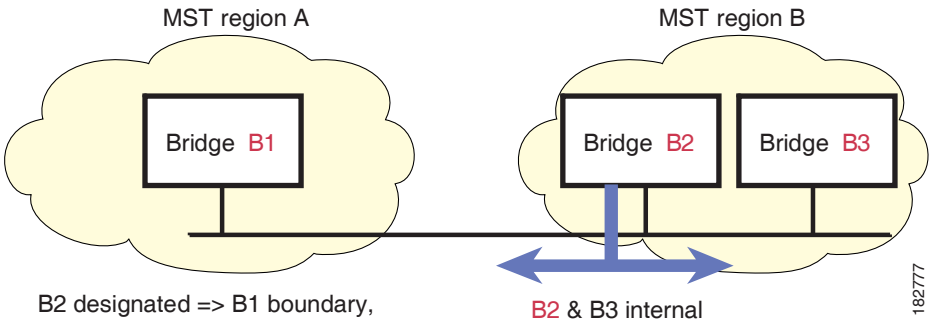
BPDU の 802.1w 部分に格納されているメッセージ有効期間および最大エージング タイムの情報は、領域全体で同じです（IST の場合のみ）。同じ値が、境界にある領域の指定ポートによって伝播されます。

スイッチがスパニングツリー設定メッセージを受信せずに再設定を試行するまで待機する秒数として最大エージング タイムを設定します。

境界ポート

境界ポートは、LAN に接続されたポートで、その代表ブリッジは、MST 設定が異なるブリッジ（つまり、別の MST 領域）、または Rapid PVST+ や 802.1D STP スイッチのいずれかです。指定ポートは、STP ブリッジを検出するか、設定が異なる MST ブリッジまたは Rapid PVST+ ブリッジから合意提案を受信すると、境界にあることを認識します。この定義により、領域の内部にある 2 つのポートが、異なる領域に属すポートとセグメントを共有できるため、ポートで内部メッセージと外部メッセージの両方を受信できる可能性があります（図 9-3 を参照）。

図 9-3　MST 境界ポート



境界では、MST ポートのロールは問題ではなく、そのステートは強制的に IST ポート ステートと同じに設定されます。境界フラグがポートに対してオンに設定されている場合、MST ポートのロールの選択処理では、ポートのロールが境界に割り当てられ、同じステートが IST ポートのステートとして割り当てられます。境界にある IST ポートでは、バックアップ ポート ロール以外のすべてのポート ロールを引き継ぐことができます。

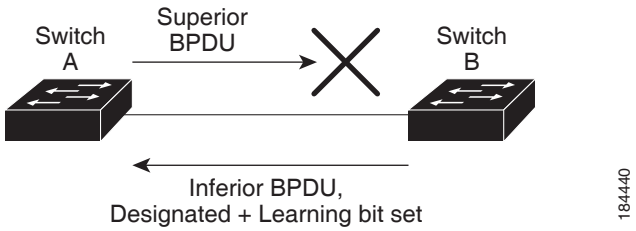
単一方向リンク障害の検出

現在、この機能は、IEEE MST 規格にはありませんが、規格準拠の実装に含まれています。ソフトウェアは、受信した BPDU でポートのロールおよびステートの一貫性をチェックし、ブリッジング ループの原因となることがある単方向リンク障害を検出します。

指定ポートは、矛盾を検出すると、そのロールを維持しますが、廃棄ステートに戻ります。一貫性がない場合は、接続を中断した方がブリッジング ループを解決できるからです。

図 9-4 に、ブリッジング ループの一般的な原因となる単一方向リンク障害を示します。スイッチ A はルート ブリッジであり、スイッチ B へのリンクで BPDU は失われます。Rapid PVST+ (802.1w) および MST BPDU には、送信側ポートの役割と状態が含まれます。この情報により、スイッチ B は送信される上位 BPDU に対して反応せず、スイッチ B はルート ポートではなく指定ポートであることが、スイッチ A によって検出できます。この結果、スイッチ A は、そのポートをブロックし（またはブロックし続け）、ブリッジング ループが防止されます。ブロックは、STP の矛盾として示されます。

図 9-4　　単一方向リンク障害の検出



ポート コストとポート プライオリティ

スパニングツリーはポート コストを使用して、指定ポートを決定します。値が低いほど、ポート コストは小さくなります。スパニングツリーでは、最小のコスト パスが選択されます。デフォルト ポート コストは、次のように、インターフェイス帯域幅から取得されます。

- 10 Mbps：2,000,000
- 100 Mbps：200,000
- 1 ギガビット イーサネット：20,000
- 10 ギガビット イーサネット：2,000

ポート コストを設定すると、選択されるポートが影響を受けます。

（注） MST では、ロング パス コスト計算方式が常に使用されるため、有効値の範囲は、1 ～ 200,000,000 です。

コストが同じポートを差別化するために、ポート プライオリティが使用されます。値が小さいほど、プライオリティが高いことを示します。デフォルトのポートのプライオリティは 128 です。プライオリティは、0 ～ 224 の間の値に、32 ずつ増やして設定できます。

IEEE 802.1D との相互運用性

MST が実行されるスイッチでは、802.1D STP スイッチとの相互運用を可能にする、内蔵プロトコル移行機能がサポートされます。このスイッチで、802.1D コンフィギュレーション BPDU（プロトコル バージョンが 0 に設定されている BPDU）を受信する場合、そのポート上の 802.1D BPDU のみが送信されます。さらに、MST スイッチでは、802.1D BPDU、異なるリージョンに関連付けられている MST BPDU（バージョン 3）、または 802.1w BPDU（バージョン 2）を受信するときに、ポートがリージョンの境界にあることを検出できます。

ただし、スイッチは、802.1D BPDU を受信しなくなった場合でも、自動的には MSTP モードには戻りません。これは、802.1D スイッチが指定スイッチではない場合、802.1D スイッチがリンクから削除されたかどうかを検出できないためです。さらにスイッチは、接続先スイッチがリージョンに加入した場合であっても、引き続きポートに境界の役割を指定する可能性があります。

プロトコル移行プロセスを再開する（強制的に隣接スイッチと再ネゴシエーションさせる）には、**clear spanning-tree detected-protocols** コマンドを入力します。

リンク上にあるすべての Rapid PVST+ スイッチ（およびすべての 8021.D STP スイッチ）では、MST BPDU を 802.1w BPDU の場合と同様に処理できます。MST スイッチでは、境界ポート上にある、バージョン 0 コンフィギュレーションおよびトポロジ変更通知（TCN）BPDU、またはバージョン 3 MST BPDU のいずれかを送信できます。境界ポートは LAN に接続され、その指定スイッチは、単一スパニングツリー スイッチか、MST 設定が異なるスイッチのいずれかです。

（注） MST は、MST ポート上で先行標準 MSTP を受信するたびに、シスコの先行標準 MSTP と相互に動作します。明示的な設定は必要ありません。

Rapid PVST+ の相互運用性と PVST シミュレーションについて

MST は、ユーザが設定しなくても、Rapid PVST+ と相互運用できます。PVST シミュレーション機能により、このシームレスな相互運用が可能になっています。

（注） PVST シミュレーションは、デフォルトでイネーブルになっています。つまり、スイッチ上のすべてのインターフェイスは、デフォルトで、MST と Rapid PVST+ との間で相互動作します。

ただし、MST と Rapid PVST+ との接続を制御し、MST 対応ポートを Rapid PVST+ 対応ポートに誤って接続するのを防止することが必要な場合もあります。Rapid PVST+ はデフォルト STP モードのため、Rapid PVST+ がイネーブルな多数の接続が検出されることがあります。

ポートごと、またはスイッチ全体にグローバルに、Rapid PVST+ シミュレーションをディセーブルにできますが、これを実行することにより、MST がイネーブルなポートが Rapid PVST+ がイネーブルなポートに接続されていることが検出されると、MST がイネーブルなポートはブロッキング ステートになります。このポートは、Rapid PVST+/SSTP BPDU の受信が停止されるまで不整合のステートのままになります。そしてポートは、通常の STP 送信プロセスに戻ります。

MST の設定

この項では、次のトピックについて取り上げます。

- MST 設定時の注意事項(9-10 ページ)
- MST のイネーブル化(9-11 ページ)
- MST コンフィギュレーション モードの開始(9-11 ページ)
- MST の名前の指定(9-13 ページ)
- MST 設定のリビジョン番号の指定(9-13 ページ)
- VLAN から MST インスタンスへのマッピングとマッピング解除(9-15 ページ)
- プライベート VLAN でセカンダリ VLAN をプライマリ VLAN として同じ MSTI にマッピングするには(9-16 ページ)
- ルート ブリッジの設定(9-17 ページ)
- セカンダリ ルート ブリッジの設定(9-18 ページ)
- ポートのプライオリティの設定(9-19 ページ)
- ポート コストの設定(9-19 ページ)
- スイッチのプライオリティの設定(9-20 ページ)
- hello タイムの設定(9-21 ページ)
- 転送遅延時間の設定(9-22 ページ)
- 最大経過時間の設定(9-22 ページ)
- 最大ホップ カウントの設定(9-22 ページ)
- PVST シミュレーションのグローバル設定(9-23 ページ)
- ポートごとの PVST シミュレーションの設定(9-23 ページ)
- リンク タイプの設定(9-24 ページ)
- プロトコルの再開(9-25 ページ)

MST 設定時の注意事項

MST を設定する場合は、次の注意事項に従ってください。

- プライベート VLAN を操作するときには、**private-vlan synchronize** コマンドを使用して、プライマリ VLAN として、セカンダリ VLAN を同じ MST インスタンスにマッピングします。
- MST 設定サブモードの場合、次の注意事項が適用されます。
  - 各コマンド参照行により、保留中のリージョン設定が作成されます。
  - 保留中のリージョン設定により、現在のリージョン設定が開始されます。
  - 変更をコミットすることなく MST 設定サブモードを終了するには、**abort** コマンドを入力します。
  - 行った変更内容をすべてコミットして MST 設定サブモードを終了するには、**exit** コマンドを入力します。

MST のイネーブル化

MST はイネーブルにする必要があります。デフォルトは Rapid PVST+ です。

（注）スパニングツリー モードを変更すると、変更前のモードのスパニングツリー インスタンスがすべて停止されて新しいモードで起動されるため、トラフィックが中断する場合があります。

スイッチ上で MST をイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree mode mst`	スイッチ上で MST をイネーブルにします。

次の例は、スイッチで MST をイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mode mst
```

スイッチ上で MST をディセーブルにする手順は、次のとおりです。

コマンド	目的
`switch(config)# no spanning-tree mode mst`	スイッチ上の MST がディセーブルにされ、Rapid PVST+ に戻ります。

注意　スパニングツリー モードを変更すると、トラフィックが混乱することがあります。すべてのスパニングツリー インスタンスが以前のモードで停止し、新しいモードで再起動されるからです。

（注）STP はデフォルトでイネーブルのため、設定結果を参照するために **show running** コマンドを入力しても、STP をイネーブルするために入力したコマンドは表示されません。

MST コンフィギュレーション モードの開始

スイッチ上で、MST の名前、VLAN からインスタンスへのマッピング、MST リビジョン番号を設定するには、MST コンフィギュレーション モードを開始します。

同じ MST リージョンにある複数のスイッチには、同じ MST の名前、VLAN からインスタンスへのマッピング、MST リビジョン番号を設定しておく必要があります。

（注）各コマンド参照行により、MST コンフィギュレーション モードで保留中の領域設定が作成されます。さらに、保留中の領域設定により、現在の領域設定が開始されます。

MST コンフィギュレーション モードを開始する手順は、次のとおりです（**exit** と **abort** との違いに注意してください）。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree mst configuration`	システム上で、MST 設定サブモードを開始します。次の MST 設定パラメータを割り当てるには、MST 設定サブモードを開始しておく必要があります。 • MST 名 • インスタンスから VLAN へのマッピング • MST リビジョン番号 • プライベート VLAN でのプライマリ VLAN とセカンダリ VLAN との同期
ステップ 3	`switch(config-mst)# exit`	すべての変更をコミットし、MST 設定サブモードを終了します。
	`switch(config-mst)# abort`	いずれの変更もコミットすることなく、MST 設定サブモードを終了します。

次の例は、スイッチで MST コンフィギュレーション サブモードを開始する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst configuration
```

次の例は、スイッチで変更をコミットして MST コンフィギュレーション サブモードを終了する方法を示しています。

```
sswitch(config-mst)# exit
```

次の例は、スイッチで変更をコミットせずに MST コンフィギュレーション サブモードを終了する方法を示しています。

```
sswitch(config-mst)# abort
```

MST コンフィギュレーション モードをディセーブルにする手順は、次のとおりです。

コマンド	目的
`switch(config-mst)# no spanning-tree mst configuration`	MST リージョン設定を次のデフォルト値に戻します。 • 領域名は空の文字列になります。 • VLAN は MSTI にマッピングされません（すべての VLAN は CIST インスタンスにマッピングされます）。 • リビジョン番号は 0 です。

MST の名前の指定

リージョン名は、ブリッジ上に設定します。同じ MST リージョンにある複数のブリッジには、同じ MST の名前、VLAN からインスタンスへのマッピング、MST リビジョン番号を設定しておく必要があります。

MST の名前を指定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree mst configuration`	MST コンフィギュレーション サブモードを開始します。
ステップ 3	`switch(config-mst)# name name`	MST リージョンの名前を指定します。*name* ストリングには最大 32 文字まで使用でき、大文字と小文字が区別されます。デフォルトは空の文字列です。

次の例は、MST リージョンの名前の設定方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst configuration
switch(config-mst)# name accounting
```

MST 設定のリビジョン番号の指定

リビジョン番号は、ブリッジ上に設定します。同じ MST リージョンにある複数のブリッジには、同じ MST の名前、VLAN からインスタンスへのマッピング、MST リビジョン番号を設定しておく必要があります。

MST のリビジョン番号を指定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree mst configuration`	MST コンフィギュレーション サブモードを開始します。
ステップ 3	`switch(config-mst)# revision version`	MST リージョンのリビジョン番号を指定します。範囲は 0 ～ 65535 で、デフォルト値は 0 です。

次の例は、MSTI リージョンのリビジョン番号を 5 に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst configuration
switch(config-mst)# revision 5
```

MST 領域での設定の指定

2 台以上のスイッチを同一 MST リージョン内に存在させるには、同じ VLAN からインスタンスへのマッピング、同じ構成リビジョン番号、および同じ MST の名前が設定されている必要があります。

領域には、同じ MST 設定の 1 つのメンバまたは複数のメンバを存在させることができます。各メンバでは、IEEE 802.1w RSTP BPDU を処理できる必要があります。ネットワーク内の MST リージョンには、数の制限はありませんが、各リージョンでは、最大 65 までのインスタンスをサポートできます。VLAN は、一度に 1 つの MST インスタンスに対してのみ割り当てることができます。

MST 領域で設定を指定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configure terminal`**	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`spanning-tree mst configuration`**	MST コンフィギュレーション サブモードを開始します。
ステップ 3	`switch(config-mst)#` **`instance`** *`instance-id`* **`vlan`** *`vlan-range`*	VLAN を MST インスタンスにマッピングする手順は、次のとおりです。 • *instance-id* の範囲は 1 ～ 4094 です。 • **vlan** *vlan-range* の範囲は 1 ～ 4094 です。 VLAN を MSTI にマップする場合、マッピングは増加され、コマンドに指定した VLAN は、以前マッピングした VLAN に追加されるか、そこから削除されます。 VLAN 範囲を指定する場合は、ハイフンを使用します。たとえば、**instance 1 vlan 1-63** とコマンドを入力すると、MST インスタンス 1 に VLAN 1 ～ 63 がマッピングされます。 複数の VLAN を指定する場合はカンマで区切ります。たとえば、**instance 1 vlan 10, 20, 30** と指定すると、MST インスタンス 1 に VLAN 10、20、および 30 がマッピングされます。
ステップ 4	`switch(config-mst)#` **`name`** *`name`*	インスタンス名を指定します。*name* 文字列の最大の長さは 32 文字であり、大文字と小文字が区別されます。
ステップ 5	`switch(config-mst)#` **`revision`** *`version`*	設定リビジョン番号を指定します。範囲は 0 ～ 65535 です。

デフォルトに戻すには、次のように操作します。

- デフォルト MST 領域設定に戻すには、**no spanning-tree mst configuration** グローバル コンフィギュレーション コマンドを入力します。
- デフォルトの VLAN からインスタンスへのマッピングに戻すには、**no instance** *instance_id* **vlan** *vlan-range* MST コンフィギュレーション コマンドを入力します。
- デフォルトの名前に戻すには、**no name** MST コンフィギュレーション コマンドを入力します。

- デフォルトのリビジョン番号に戻すには、**no revision** MST コンフィギュレーション コマンドを入力します。
- Rapid PVST+ を再度イネーブルにするには、**no spanning-tree mode** または **spanning-tree mode rapid-pvst** のグローバル コンフィギュレーション コマンドを入力します。

次の例は、MST コンフィギュレーション モードを開始し、VLAN 10 ～ 20 を MSTI 1 にマッピングし、リージョンに *region1* という名前を付けて、設定リビジョンを 1 に設定し、保留中の設定を表示し、変更を適用してグローバル コンフィギュレーション モードに戻る方法を示しています。

```
switch(config)# spanning-tree mst configuration
switch(config-mst)# instance 1 vlan 10-20
switch(config-mst)# name region1
switch(config-mst)# revision 1
switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instances configured 2
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------
```

VLAN から MST インスタンスへのマッピングとマッピング解除

注意　VLAN/MSTI マッピングを変更すると、MST は再起動されます。

（注）　MSTI はディセーブルにできません。

同じ MST リージョンにある複数のブリッジには、同じ MST の名前、VLAN からインスタンスへのマッピング、MST リビジョン番号を設定しておく必要があります。

VLAN を MST インスタンスにマッピングする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree mst configuration`	MST コンフィギュレーション サブモードを開始します。

	コマンド	目的
ステップ 3	switch(config-mst)# **instance** *instance-id* **vlan** *vlan-range*	VLAN を MST インスタンスにマッピングする手順は、次のとおりです。 • *instance_id* の範囲は 1 ～ 4094 です。 インスタンス 0 は、各 MST リージョンでの IST 用に予約されています。 • *vlan-range* の範囲は 1 ～ 4094 です。 VLAN を MSTI にマッピングすると、マッピングは差分で実行され、コマンドで指定された VLAN が、以前マッピングされた VLAN に追加または VLAN から削除されます。

次の例は、VLAN 200 を MSTI 3 にマッピングする方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst configuration
switch(config-mst)# instance 3 vlan 200
```

VLAN を MST インスタンスからマッピング解除する手順は、次のとおりです。

コマンド	目的
switch(config-mst)# **no instance** *instance-id* **vlan** *vlan-range*	指定したインスタンスを削除し、VLAN を、デフォルト MSTI である CIST に戻します。

プライベート VLAN でセカンダリ VLAN をプライマリ VLAN として同じ MSTI にマッピングするには

システム上のプライベート VLAN を操作するときに、すべてのセカンダリ VLAN は、同じ MSTI とそれがアソシエートされているプライマリ VLAN に存在させておく必要があります。

この同期を自動的に実現する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **spanning-tree mst configuration**	MST コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-mst)# **private-vlan synchronize**	すべてのセカンダリ VLAN を、同じ MSTI と、すべてのプライベート VLAN にアソシエートされているプライマリ VLAN に、自動的にマッピングします。

次の例は、すべてのプライベート VLAN のすべてのセカンダリ VLAN を、それぞれ関連するプライマリ VLAN と同じ MSTI に自動的にマッピングする方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst configuration
switch(config-mst)# private-vlan synchronize
```

ルート ブリッジの設定

スイッチは、ルート ブリッジになるよう設定できます。

（注） 各 MSTI のルート ブリッジは、バックボーン スイッチまたはディストリビューション スイッチである必要があります。アクセス スイッチは、スパニングツリーのプライマリ ルート ブリッジとして設定しないでください。

MSTI 0（または IST）でのみ使用可能な **diameter** キーワードを入力し、ネットワーク直径（ネットワーク内の任意の 2 つのエンド ステーション間での最大ホップ数）を指定します。ネットワークの直径を指定すると、その直径のネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムをスイッチが自動的に設定するので、コンバージェンスの所要時間を大幅に短縮できます。**hello** キーワードを入力すると、自動的に計算された hello タイムを上書きできます。

（注） ルート ブリッジとして設定されているスイッチでは、hello タイム、転送遅延時間、最大エージング タイムは手動で設定（**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、**spanning-tree mst max-age** の各グローバル コンフィギュレーション コマンドを使用）しないでください。

ルート ブリッジをイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree mst` *`instance-id`* `root {primary | secondary} [diameter` *`dia`* `[hello-time` *`hello-time`*`]]`	次のように、ルート ブリッジとしてスイッチを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 1 ～ 4094 です。 • **diameter** *net-diameter* には、2 つのエンド ステーション間にホップの最大数を設定します。デフォルト値は 7 です。このキーワードは、MSTI インスタンス 0 の場合にのみ使用できます。 • **hello-time** *seconds* には、ルート ブリッジによって生成された設定メッセージの間隔を秒単位で指定します。有効範囲は 1 ～ 10 秒で、デフォルトは 2 秒です。

次の例は、MSTI 5 のルート スイッチとしてスイッチを設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst 5 root primary
```

ルート ブリッジをディセーブルにする手順は、次のとおりです。

コマンド	目的
switch(config)# **no spanning-tree mst** *instance-id* **root**	スイッチのプライオリティ、範囲、hello タイムをデフォルト値に戻します。

セカンダリ ルート ブリッジの設定

このコマンドは、複数のスイッチに対して実行し、複数のバックアップ ルート ブリッジを設定できます。**spanning-tree mst root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート ブリッジを設定したときに使用したのと同じネットワーク直径と hello タイムの値を入力します。

セカンダリ ルート ブリッジをイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]]	次のように、セカンダリ ルート ブリッジとしてスイッチを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 1 ～ 4094 です。 • **diameter** *net-diameter* には、2 つのエンド ステーション間にホップの最大数を設定します。デフォルト値は 7 です。このキーワードは、MSTI インスタンス 0 の場合にのみ使用できます。 • **hello-time** *seconds* には、ルート ブリッジによって生成された設定メッセージの間隔を秒単位で指定します。有効範囲は 1 ～ 10 秒で、デフォルトは 2 秒です。

次の例は、MSTI 5 のセカンダリ ルート スイッチとしてスイッチを設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst 5 root secondary
```

セカンダリ ルート ブリッジをディセーブルにする手順は、次のとおりです。

コマンド	目的
switch(config)# **no spanning-tree mst** *instance-id* **root**	スイッチのプライオリティ、範囲、hello タイムをデフォルト値に戻します。

ポートのプライオリティの設定

ループが発生する場合、MST は、フォワーディング ステートにするインターフェイスを選択するとき、ポート プライオリティを使用します。最初に選択させるインターフェイスには低いプライオリティの値を割り当て、最後に選択させるインターフェイスには高いプライオリティの値を割り当てることができます。すべてのインターフェイスのプライオリティ値が同一である場合、MST はインターフェイス番号が最も低いインターフェイスをフォワーディング ステートにして、その他のインターフェイスをブロックします。

ポートのプライオリティを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface {{type slot/port} | {port-channel number}}`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# spanning-tree mst instance-id port-priority priority`	次のように、ポートのプライオリティを設定します。 • *instance-id* には、1 つの MSTI、それぞれをハイフンで区切った MSTI の範囲、またはカンマで区切った一連の MSTI を指定できます。指定できる範囲は 1 ～ 4094 です。 • *priority* の範囲は 0 ～ 224 で、32 ずつ増加します。デフォルト値は 128 です。値が小さいほど、プライオリティが高いことを示します。 プライオリティ値は、0、32、64、96、128、160、192、224 です。システムでは、他のすべての値が拒否されます。

次の例は、イーサネット ポート 3/1 で MSTI 3 の MST インターフェイス ポート プライオリティを 64 に設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# spanning-tree mst 3 port-priority 64
```

このコマンドを使用できるのは、物理イーサネット インターフェイスに対してだけです。

ポート コストの設定

MST パス コストのデフォルト値は、インターフェイスのメディア速度から取得されます。ループが発生した場合、MST は、コストを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択させるインターフェイスには小さいコストの値を割り当て、最後に選択させるインターフェイスの値には大きいコストを割り当てることができます。すべてのインターフェイスのコスト値が同一である場合、MST はインターフェイス番号が最も低いインターフェイスをフォワーディング ステートにして、その他のインターフェイスをブロックします。

（注） MST では、ロング パス コスト計算方式が使用されます。

ポート コストを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface {{type slot/port} | {port-channel number}}`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# spanning-tree mst instance-id cost [cost | auto]`	コストを設定します。 ループが発生した場合、MST はパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。パス コストが小さいほど、送信速度が速いことを示します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 1 ～ 4094 です。 • *cost* の範囲は 1 ～ 200000000 です。デフォルト値は **auto** で、インターフェイスのメディア速度から取得されるものです。

次の例は、イーサネット ポート 3/1 で MSTI 4 の MST インターフェイス ポート コストを設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# spanning-tree mst 4 cost 17031970
```

スイッチのプライオリティの設定

MST インスタンスのスイッチのプライオリティは、指定されたポートがルート ブリッジとして選択されるように設定できます。

（注） このコマンドの使用には注意してください。ほとんどの場合、スイッチのプライオリティを変更するには、**spanning-tree mst root primary** および **spanning-tree mst root secondary** のグローバル コンフィギュレーション コマンドの使用を推奨します。

MST インスタンスのスイッチのプライオリティを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree mst` *instance-id* **priority** *priority-value*	次のように、スイッチのプライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 1 ～ 4094 です。 • **priority** には、4096 単位で 0 ～ 61440 の値を指定します。デフォルトは 32768 です。小さい値を設定すると、スイッチがルート スイッチとして選択される可能性が高くなります。 使用可能な値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。システムでは、他のすべての値が拒否されます。

次の例は、MSTI 5 のブリッジのプライオリティを 4096 に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst 5 priority 4096
```

hello タイムの設定

hello タイムを変更することによって、スイッチ上のすべてのインスタンスについて、ルート ブリッジにより設定メッセージを生成する間隔を設定できます。

（注）　このコマンドの使用には注意してください。ほとんどの場合、hello タイムを変更するには、**spanning-tree mst** *instance-id* **root primary** および **spanning-tree mst** *instance-id* **root secondary** のグローバル コンフィギュレーション コマンドの使用を推奨します。

hello タイムを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree mst` **hello-time** *seconds*	すべての MST インスタンスについて、hello タイムを設定します。hello タイムは、ルート ブリッジが設定メッセージを生成する時間です。これらのメッセージは、スイッチがアクティブであることを意味します。*seconds* の範囲は 1 ～ 10 で、デフォルトは 2 秒です。

次の例は、スイッチの hello タイムを 1 秒に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst hello-time 1
```

転送遅延時間の設定

スイッチ上のすべての MST インスタンスには、1 つのコマンドで転送遅延タイマーを設定できます。

転送遅延タイマーを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree mst forward-time` *seconds*	すべての MST インスタンスについて、転送時間を設定します。転送遅延は、スパニングツリー ブロッキング ステートとラーニング ステートからフォワーディング ステートに変更する前に、ポートが待つ秒数です。*seconds* の範囲は 4 ～ 30 で、デフォルトは 15 秒です。

次の例は、スイッチの転送遅延時間を 10 秒に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst forward-time 10
```

最大経過時間の設定

最大経過時間タイマーは、スイッチが、再設定を試行する前に、スパニングツリー設定メッセージの受信を待つ秒数です。

スイッチ上のすべての MST インスタンスには、1 つのコマンドで最大経過時間タイマーを設定できます（最大経過時間は IST にのみ適用されます）。

最大経過時間タイマーを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree mst max-age` *seconds*	すべての MST インスタンスについて、最大経過時間を設定します。最大経過時間は、スイッチが、再設定を試行する前に、スパニングツリー設定メッセージの受信を待つ秒数です。*seconds* の範囲は 6 ～ 40 で、デフォルトは 20 秒です。

次の例は、スイッチの最大エージング タイマーを 40 秒に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst max-age 40
```

最大ホップ カウントの設定

MST では、IST リージョナル ルートへのパス コストと、IP の存続可能時間（TTL）メカニズムに類似したホップ カウント メカニズムが、使用されます。リージョン内の最大ホップを設定し、それを、そのリージョンにある IST とすべての MST インスタンスに適用できます。ホップ カウントは、メッセージ エージ情報と同じ結果になります（再設定を開始）。

最大ホップ カウントを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree mst max-hops hop-count`	BPDU を廃棄してポート用に保持していた情報を期限切れにするまでの、リージョンでのホップ数を設定します。*hop-count* の範囲は 1 ～ 255 で、デフォルト値は 20 ホップです。

次の例は、最大ホップ カウントを 40 に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst max-hops 40
```

PVST シミュレーションのグローバル設定

この自動機能は、グローバルまたはポートごとにブロックできます。グローバル コマンドを入力すると、インターフェイス コマンド モードの実行中に、スイッチ全体の PVST シミュレーション設定を変更できます。

PVST シミュレーションを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# no spanning-tree mst simulate pvst global`	Rapid PVST+ モードで実行中の接続スイッチと自動的に相互動作する状態から、スイッチ上のすべてのインターフェイスをディセーブルにできます。これはデフォルトでイネーブルです。つまり、デフォルトでは、スイッチ上のすべてのインターフェイスは、Rapid PVST+ と MST との間でシームレスに動作します。

次の例は、Rapid PVST+ を実行している接続スイッチと自動的に相互運用することを防止するようにスイッチを設定する方法を示しています。

```
switch# configure terminal
switch(config)# no spanning-tree mst simulate pvst global
```

ポートごとの PVST シミュレーションの設定

（注） PVST シミュレーションは、デフォルトでイネーブルになっています。スイッチ上のすべてのインターフェイスは、MST と Rapid PVST+ との間で相互動作します。

MST は、Rapid PVST+ とシームレスに相互動作します。ただし、デフォルト STP モードとして MST が実行されていないスイッチへの誤った接続を防ぐため、この自動機能をディセーブルにする必要が生じる場合があります。Rapid PVST+ シミュレーションをディセーブルにした場合、MST がイネーブルなポートが Rapid PVST+ がイネーブルなポートに接続されていることが検出

されると、MST がイネーブルなポートは、ブロッキング ステートに移行します。このポートは、BPDU の受信が停止されるまで、一貫性のないステートのままになり、それから、ポートは、通常の STP 送信プロセスに戻ります。

この自動機能は、グローバルまたはポートごとにブロックできます。

PVST シミュレーションをディセーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface {{type slot/port} | {port-channel number}}`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# spanning-tree mst simulate pvst disable`	Rapid PVST+ モードで実行中の接続スイッチと自動的に相互動作する状態から、指定したインターフェイスをディセーブルにします。 スイッチ上のすべてのインターフェイスは、デフォルトで、Rapid PVST+ と MST との間でシームレスに動作します。
	`switch(config-if)# spanning-tree mst simulate pvst`	指定したインターフェイスで、MST と Rapid PVST+ との間のシームレスな動作を再度イネーブルにします。
	`switch(config-if)# no spanning-tree mst simulate pvst`	インターフェイスを、**spanning-tree mst simulate pvst global** コマンドを使用して、設定したスイッチ全体で MST と Rapid PVST+ との間で相互動作するよう設定します。

次の例は、MST を実行していない接続スイッチと自動的に相互運用することを防止するように指定インターフェイスを設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree mst simulate pvst disable
```

リンク タイプの設定

Rapid の接続性（802.1w 規格）は、ポイントツーポイントのリンク上でのみ確立されます。リンク タイプは、デフォルトでは、インターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続であると見なされ、半二重ポートは共有接続であると見なされます。

リモート スイッチの 1 つのポートに、ポイントツーポイントで物理的に接続されている半二重リンクがある場合、リンク タイプのデフォルト設定を上書きし、高速移行をイネーブルにできます。

リンクを共有に設定すると、STP は 802.1D に戻されます。

リンク タイプを指定する手順は次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** *type slot/port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **spanning-tree link-type** {**auto** | **point-to-point** | **shared**}	リンク タイプを、ポイントツーポイントまたは共有に設定します。システムでは、スイッチ接続からデフォルト値を読み込みます。半二重リンクは共有で、全二重リンクはポイントツーポイントです。リンク タイプが共有の場合、STP は 802.1D に戻ります。デフォルトは auto で、インターフェイスのデュプレックス設定に基づいてリンク タイプが設定されます。

次の例は、リンク タイプをポイントツーポイントとして設定する方法を示しています。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree link-type point-to-point
```

プロトコルの再開

MST ブリッジでは、レガシー BPDU または異なるリージョンに関連付けられている MST BPDU を受信するときに、ポートがリージョンの境界にあることを検出できます。ただし、STP プロトコルの移行では、レガシー スイッチが指定スイッチではない場合、IEEE 802.1D のみが実行されているレガシー スイッチが、リンクから削除されたかどうかを認識できません。スイッチ全体または指定したインターフェイスでプロトコル ネゴシエーションを再開する（強制的に隣接スイッチと再ネゴシエーションさせる）には、このコマンドを入力します。

プロトコルを再開する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **clear spanning-tree detected-protocol** [**interface** *interface* [*interface-num* | *port-channel*]]	スイッチ全体または指定したインターフェイスで、MST を再開します。

次の例は、スロット 2、ポート 8 のイーサネット インターフェイスで MST を再起動する方法を示しています。

```
switch# clear spanning-tree detected-protocol interface ethernet 2/8
```

MST の設定の確認

MST の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
switch# **show running-config spanning-tree** [**all**]	現在のスパニングツリー設定を表示します。
switch# **show spanning-tree mst** [*options*]	現在の MST 設定の詳細情報を表示します。

次に、現在の MST 設定を表示する例を示します。

```
switch# show spanning-tree mst configuration
% Switch is not in mst mode
Name      [mist-attempt]
Revision  1     Instances configured 2
Instance  Vlans mapped
--------  -------------------------------------------------------------------
0         1-12,14-41,43-4094
1         13,42
-------------------------------------------------------------------------------
```

CHAPTER 10

STP 拡張機能の設定

シスコでは、スパニングツリー プロトコル（STP）に、収束をより効率的に行うための拡張機能を追加しました。場合によっては、同様の機能が IEEE 802.1w 高速スパニングツリー プロトコル（RSTP）標準にも組み込まれている可能性がありますが、シスコの拡張機能を使用することを推奨します。これらの拡張機能はすべて、Rapid per VLAN Spanning Tree（RPVST+）および Multiple Spanning Tree（MST）と組み合わせて使用できます。

使用可能な拡張機能には、スパニングツリー ポート タイプ、Bridge Assurance、ブリッジ プロトコル データ ユニット（BPDU）ガード、BPDU フィルタリング、ループ ガード、ルート ガードがあります。これらの機能の大部分は、グローバルに、または指定インターフェイスに適用できます。

（注） このマニュアルでは、IEEE 802.1w および IEEE 802.1s を指す用語として、「スパニングツリー」を使用します。IEEE 802.1D STP について説明している箇所では、802.1D と明記します。

この章は、次の項で構成されています。

- STP 拡張機能について（10-1 ページ）
- STP 拡張機能の設定（10-5 ページ）
- STP 拡張機能の設定の確認（10-15 ページ）

（注） STP および Rapid PVST+ の詳細については第 8 章「Rapid PVST+ の設定」を、MST の詳細については第 9 章「MST の設定」を参照してください。

STP 拡張機能について

ここでは、次の内容について説明します。

- STP ポート タイプの概要（10-2 ページ）
- Bridge Assurance の概要（10-2 ページ）
- BPDU ガードの概要（10-3 ページ）
- BPDU フィルタリングの概要（10-3 ページ）
- ループ ガードの概要（10-4 ページ）
- ルート ガードの概要（10-5 ページ）

STP ポート タイプの概要

スパニングツリー ポートは、エッジ ポート、ネットワーク ポート、または標準ポートとして構成できます。ポートは、ある一時点において、これらのうちいずれか 1 つの状態をとります。デフォルトのスパニング ツリー ポート タイプは「標準」です。インターフェイスが接続されているデバイスのタイプによって、スパニングツリー ポートを上記いずれかのポート タイプに設定できます。

この項では、次のトピックについて取り上げます。

- スパニングツリー エッジ ポート（10-2 ページ）
- スパニングツリー ネットワーク ポート（10-2 ページ）
- スパニングツリー標準ポート（10-2 ページ）

スパニングツリー エッジ ポート

エッジ ポートは、ホストに接続されるポートであり、アクセス ポートとトランク ポートのどちらにもなります。エッジ ポート インターフェイスは、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します（この直接移行動作は、以前は、シスコ独自の機能 PortFast として設定していました）。

ホストに接続されているインターフェイスは、STP ブリッジ プロトコル データ ユニット（BPDU）を受信してはなりません。

（注）　別のスイッチに接続されているポートをエッジ ポートとして設定すると、ブリッジング ループが発生する可能性があります。

スパニングツリー ネットワーク ポート

ネットワーク ポートは、スイッチまたはブリッジだけに接続されます。Bridge Assurance はネットワーク ポート上でだけイネーブルになります。

（注）　ホストまたは他のエッジ デバイスに接続されているポートを誤ってスパニングツリー ネットワーク ポートとして設定すると、それらのポートは自動的にブロッキング ステートに移行します。

スパニングツリー標準ポート

標準ポートは、ホスト、スイッチ、またはブリッジに接続できます。これらのポートは、標準スパニングツリー ポートとして機能します。

デフォルトのスパニングツリー インターフェイスは標準ポートです。

Bridge Assurance の概要

Bridge Assurance を使用すると、ネットワーク内でブリッジング ループの原因となる問題の発生を防ぐことができます。具体的には、単方向リンク障害や、スパニングツリー アルゴリズムを実行しなくなってもデータ トラフィックの転送を続けているデバイスなどからネットワークを保護できます。

（注）　Bridge Assurance は、Rapid PVST+ および MST だけでサポートされています。従来の 802.1D スパニングツリーではサポートされていません。

Bridge Assurance はデフォルトでイネーブルになっており、グローバル単位でだけディセーブルにできます。また、Bridge Assurance をイネーブルにできるのは、ポイントツーポイント リンクに接続されたスパニングツリー ネットワーク ポートだけです。Bridge Assurance は必ず、リンクの両端でイネーブルにする必要があります。

Bridge Assurance をイネーブルにすると、BPDU が hello タイムごとに、動作中のすべてのネットワーク ポート（代替ポートとバックアップ ポートを含む）に送出されます。所定の期間 BPDU を受信しないポートは、ブロッキング ステートに移行し、ルート ポートの決定に使用されなくなります。BPDU を再度受信するようになると、そのポートで通常のスパニングツリー状態遷移が再開されます。

BPDU ガードの概要

BPDU ガードをイネーブルにすると、BPDU を受信したときにそのインターフェイスがシャットダウンされます。

BPDU ガードはインターフェイス レベルで設定できます。BPDU ガードをインターフェイス レベルで設定すると、そのポートはポート タイプ設定にかかわらず BPDU を受信するとすぐにシャットダウンされます。

BPDU ガードをグローバル単位で設定すると、動作中のスパニングツリー エッジ ポート上だけで有効となります。正しい設定では、LAN エッジ インターフェイスは BPDU を受信しません。エッジ インターフェイスが BPDU を受信すると、無効な設定（未認証のホストまたはスイッチへの接続など）を知らせるシグナルが送信されます。BPDU ガードをグローバル単位でイネーブルにすると、BPDU を受信したすべてのスパニングツリー エッジ ポートがシャットダウンされます。

BPDU ガードは、無効な設定があると確実に応答を返します。無効な設定をした場合は、当該 LAN インターフェイスを手動でサービス状態に戻す必要があるからです。

（注）　BPDU ガードをグローバル単位でイネーブルにすると、動作中のすべてのスパニングツリー エッジ インターフェイスに適用されます。

BPDU フィルタリングの概要

BPDU フィルタリングを使用すると、スイッチが特定のポートで BPDU を送信または受信するのを禁止できます。

グローバルに設定された BPDU フィルタリングは、動作中のすべてのスパニングツリー エッジ ポートに適用されます。エッジ ポートはホストだけに接続してください。ホストでは通常、BPDU は破棄されます。動作中のスパニングツリー エッジ ポートが BPDU を受信すると、ただちに標準のスパニングツリー ポート タイプに戻り、通常のポート状態遷移が行われます。その場合、当該ポートで BPDU フィルタリングはディセーブルとなり、スパニングツリーによって、同ポートでの BPDU の送信が再開されます。

BPDU フィルタリングは、インターフェイスごとに設定することもできます。BPDU フィルタリングを特定のポートに明示的に設定すると、そのポートは BPDU を送出しなくなり、受信した BPDU をすべてドロップします。特定のインターフェイスを設定することによって、個々のポート上のグローバルな BPDU フィルタリングの設定を実質的に上書きできます。このようにインターフェイスに対して実行された BPDU フィルタリングは、そのインターフェイスがトランキングであるか否かに関係なく、インターフェイス全体に適用されます。

注意　BPDU フィルタリングをインターフェイスごとに設定するときは注意が必要です。ホストに接続されていないポートに BPDU フィルタリングを明示的に設定すると、ブリッジング ループに陥る可能性があります。というのは、そうしたポートは受信した BPDU をすべて無視して、フォワーディング ステートに移行するからです。

ポートがデフォルトで BPDU フィルタリングに設定されていなければ、エッジ設定によって BPDU フィルタリングが影響を受けることはありません。表 10-1 に、すべての BPDU フィルタリングの組み合わせを示します。

表 10-1　BPDU フィルタリングの設定

ポート単位の BPDU フィルタリングの設定	グローバルな BPDU フィルタリングの設定	STP エッジ ポート設定	BPDU フィルタリングの状態
デフォルト	Enable	Enable	Enable[1]
デフォルト	Enable	Disable	Disable
デフォルト	Disable	N/A	Disable
Disable	N/A	N/A	Disable
Enable	N/A	N/A	Enable

1. ポートは 10 以上の BPDU を送信します。このポートは、BPDU を受信すると、スパニングツリー標準ポート状態に戻り、BPDU フィルタリングはディセーブルになります。

ループ ガードの概要

ループ ガードは、次のような原因によってネットワークでループが発生するのを防ぎます。

- ネットワーク インターフェイスの誤動作
- CPU の過負荷
- BPDU の通常転送を妨害する要因

STP ループは、冗長なトポロジにおいてブロッキング ポートが誤ってフォワーディング ステートに移行すると発生します。こうした移行は通常、物理的に冗長なトポロジ内のポートの 1 つ（ブロッキング ポートとは限らない）が BPDU の受信を停止すると起こります。

ループ ガードは、デバイスがポイントツーポイント リンクによって接続されているスイッチドネットワークだけで役立ちます。ポイントツーポイント リンクでは、下位 BPDU を送信するか、リンクをダウンしない限り、代表ブリッジは消えることはありません。

（注）　ループ ガードは、ネットワークおよび標準のスパニングツリー ポート タイプ上だけでイネーブルにできます。

ループ ガードを使用して、ルート ポートまたは代替/バックアップ ループ ポートが BPDU を受信するかどうかを確認できます。BPDU を受信しないポートを検出すると、ループ ガードは、そのポートを不整合状態（ブロッキング ステート）に移行します。このポートは、再度 BPDU の受信を開始するまで、ブロッキング ステートのままです。不整合状態のポートは BPDU を送信しません。このようなポートが BPDU を再度受信すると、ループ ガードはそのループ不整合状態を解除し、STP によってそのポート状態が確定されます。こうしたリカバリは自動的に行われます。

ループ ガードは障害を分離し、STP は障害のあるリンクやブリッジを含まない安定したトポロジに収束できます。ループ ガードをディセーブルにすると、すべてのループ不整合ポートはリスニング ステートに移行します（STP ポート状態については、第 8 章「Rapid PVST+ の設定」を参照してください）。

ループ ガードはポート単位でイネーブルにできます。ループ ガードを特定のポートでイネーブルにすると、そのポートが属するすべてのアクティブ インスタンスまたは VLAN にループ ガードが自動的に適用されます。ループ ガードをディセーブルにすると、指定ポートでディセーブルになります。

ルート ガードの概要

特定のポートでルート ガードをイネーブルにすると、そのポートはルート ポートになることが禁じられます。受信した BPDU によって STP コンバージェンスが実行され、指定ポートがルート ポートになると、そのポートはルート不整合（ブロッキング）状態になります。このポートは、上位 BPDU の送信を停止すると、再度ブロッキングを解除されます。次に、STP によって、フォワーディング ステートに移行します。このようにポートのリカバリは自動的に行われます。

特定のインターフェイスでルート ガードをイネーブルにすると、そのインターフェイスが属するすべての VLAN にルート ガード機能が適用されます。

ルート ガードを使用すると、ネットワーク内にルート ブリッジを強制的に配置できます。ルート ガードは、ルート ガードがイネーブルにされたポートを指定ポートに選出します。通常、ルート ブリッジのポートはすべて指定ポートとなります（ただし、ルート ブリッジの 2 つ以上のポートが接続されている場合はその限りではありません）。ルート ブリッジは、ルート ガードがイネーブルにされたポートで上位 BPDU を受信すると、そのポートをルート不整合 STP 状態に移行します。このようにして、ルート ガードはルート ブリッジを強制的に配置します。

ルート ガードをグローバルには設定できません。

（注）　ルート ガードはすべてのスパニングツリー ポート タイプ（標準、エッジ、ネットワーク）でイネーブルにできます。

STP 拡張機能の設定

この項では、次のトピックについて取り上げます。

- STP 拡張機能の設定における注意事項（10-6 ページ）
- スパニングツリー ポート タイプのグローバルな設定（10-6 ページ）
- 指定インターフェイスでのスパニングツリー エッジ ポートの設定（10-7 ページ）
- 指定インターフェイスでのスパニングツリー ネットワーク ポートの設定（10-8 ページ）
- BPDU ガードのグローバルなイネーブル化（10-9 ページ）
- 指定インターフェイスでの BPDU ガードのイネーブル化（10-10 ページ）

- BPDU フィルタリングのグローバルなイネーブル化（10-11 ページ）
- 指定インターフェイスでの BPDU フィルタリングのイネーブル化（10-12 ページ）
- ループ ガードのグローバルなイネーブル化（10-13 ページ）
- 指定インターフェイスでのループ ガードまたはルート ガードのイネーブル化（10-14 ページ）

STP 拡張機能の設定における注意事項

STP 拡張機能を設定する場合は、次の注意事項に従ってください。

- ホストに接続されたすべてのアクセス ポートとトランク ポートをエッジ ポートとして設定します。
- Bridge Assurance は、ポイントツーポイントのスパニングツリー ネットワーク ポート上だけで実行されます。この機能は、リンクの両端で設定する必要があります。
- ループ ガードは、スパニングツリー エッジ ポートでは動作しません。
- ポイントツーポイント リンクに接続していないポートでループ ガードをイネーブルにはできません。
- ルート ガードがイネーブルになっている場合、ループ ガードをイネーブルにはできません。

スパニングツリー ポート タイプのグローバルな設定

スパニングツリー ポート タイプの割り当ては、そのポートが接続されているデバイスのタイプによって次のように決まります。

- エッジ：エッジ ポートは、ホストに接続されるポートであり、アクセス ポートとトランク ポートのどちらかです。
- ネットワーク：ネットワーク ポートは、スイッチまたはブリッジだけに接続されます。
- 標準：標準ポートはエッジ ポートでもネットワーク ポートでもない、標準のスパニングツリー ポートです。標準ポートは、任意のタイプのデバイスに接続できます。

ポート タイプは、グローバル単位でもインターフェイス単位でも設定できます。デフォルトのスパニングツリー ポート タイプは「標準」です。

スパニングツリー ポート タイプを設定する前に、次の点を確認してください。

- STP が設定されていること。
- インターフェイスに接続されているデバイスのタイプに合わせてポートが正しく設定されていること。

スパニングツリー ポート タイプをグローバルに設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree port type edge default`	すべてのインターフェイスをエッジ ポートとして設定します。このコマンドでは、すべてのポートがホストまたはサーバに接続されているものとします。エッジ ポートは、リンク アップすると、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。デフォルトのスパニングツリー ポート タイプは「標準」です。
	`switch(config)# spanning-tree port type network default`	すべてのインターフェイスをスパニングツリー ネットワーク ポートとして設定します。このコマンドでは、すべてのポートがスイッチまたはブリッジに接続されているものとします。Bridge Assurance をイネーブルにすると、各ネットワーク ポート上で Bridge Assurance が自動的に実行されます。デフォルトのスパニングツリー ポート タイプは「標準」です。 **（注）** ホストに接続されているインターフェイスをネットワーク ポートとして設定すると、それらのポートは自動的にブロッキング ステートに移行します。

次に、ホストに接続されたアクセス ポートおよびトランク ポートをすべて、スパニングツリー エッジ ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# spanning-tree port type edge default
```

次に、スイッチまたはブリッジに接続されたポートをすべて、スパニングツリー ネットワーク ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# spanning-tree port type network default
```

指定インターフェイスでのスパニングツリー エッジ ポートの設定

指定インターフェイスにスパニングツリー エッジ ポートを設定できます。スパニングツリー エッジ ポートとして設定されたインターフェイスは、リンク アップ時に、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。

このコマンドには次の 4 つの状態があります。

- **spanning-tree port type edge**：このコマンドはアクセス ポートのエッジ動作を明示的にイネーブルにします。
- **spanning-tree port type edge trunk**：このコマンドはトランク ポートのエッジ動作を明示的にイネーブルにします。

（注）　**spanning-tree port type edge trunk** コマンドを入力すると、そのポートは、アクセス モードであってもエッジとして設定されます。

- **spanning-tree port type normal**：このコマンドは、ポートを標準スパニングツリー ポートとして明示的に設定しますが、フォワーディング ステートへの直接移行はイネーブルにしません。
- **no spanning-tree port type**：このコマンドは、**spanning-tree port type edge default** コマンドをグローバル コンフィギュレーション モードで定義した場合に、エッジ動作を暗黙的にイネーブルにします。エッジ ポートをグローバルに設定していない場合、**no spanning-tree port type** コマンドは、**spanning-tree port type disable** コマンドと同じです。

スパニングツリー ポート タイプを設定する前に、次の点を確認してください。

- STP が設定されていること。
- インターフェイスがホストに接続されていること。

指定インターフェイスにスパニングツリー エッジ ポート タイプを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface type slot/port`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# spanning-tree port type edge`	指定したアクセスインターフェイスをスパニングエッジ ポートに設定します。エッジ ポートは、リンク アップすると、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。デフォルトのスパニングツリー ポート タイプは「標準」です。

次に、アクセス インターフェイス Ethernet 1/4 をスパニングツリー エッジ ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree port type edge
```

指定インターフェイスでのスパニングツリー ネットワーク ポートの設定

指定インターフェイスにスパニングツリー ネットワーク ポートを設定できます。

Bridge Assurance は、スパニングツリー ネットワーク ポート上だけで実行されます。

このコマンドには次の 3 つの状態があります。

- **spanning-tree port type network**：このコマンドは指定したポートを明示的にネットワーク ポートとして設定します。Bridge Assurance をグローバルにイネーブルにすると、スパニングツリー ネットワーク ポート上で Bridge Assurance が自動的に実行されます。

- **spanning-tree port type normal**：このコマンドは、ポートを明示的に標準スパニングツリー ポートとして設定します。このインターフェイス上では Bridge Assurance は動作しません。
- **no spanning-tree port type**：このコマンドは、**spanning-tree port type network default** コマンドをグローバル コンフィギュレーション モードで定義した場合に、ポートを暗黙的にスパニングツリー ネットワーク ポートとしてイネーブルにします。Bridge Assurance をイネーブルにすると、このポート上で Bridge Assurance が自動的に実行されます。

（注） ホストに接続されているポートをネットワーク ポートとして設定すると、そのポートは自動的にブロッキング ステートに移行します。

スパニングツリー ポート タイプを設定する前に、次の点を確認してください。

- STP が設定されていること。
- インターフェイスがスイッチまたはルータに接続されていること。

指定インターフェイスにスパニングツリー ネットワーク ポート タイプを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface type slot/port`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスには、物理イーサネット ポートを指定できます。
ステップ 3	`switch(config-if)# spanning-tree port type network`	指定したインターフェイスをスパニング ネットワーク ポートに設定します。Bridge Assurance をイネーブルにすると、各ネットワーク ポート上で Bridge Assurance が自動的に実行されます。デフォルトのスパニングツリー ポート タイプは「標準」です。

次に、Ethernet インターフェイス 1/4 をスパニングツリー ネットワーク ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree port type network
```

BPDU ガードのグローバルなイネーブル化

BPDU ガードをデフォルトでグローバルにイネーブルにできます。BPDU ガードがグローバルにイネーブルにされると、システムは、BPDU を受信したエッジ ポートをシャット ダウンします。

（注） すべてのエッジ ポートで BPDU ガードをイネーブルにすることを推奨します。

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。
- 少なくとも一部のスパニングツリー エッジ ポートが設定済みであること。

BPDU ガードをグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree port type edge bpduguard default`	すべてのスパニングツリー エッジ ポートで、BPDU ガードを、デフォルトでイネーブルにします。デフォルトでは、グローバルな BPDU ガードはディセーブルです。

次に、すべてのスパニングツリー エッジ ポートで BPDU ガードをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# spanning-tree port type edge bpduguard default
```

指定インターフェイスでの BPDU ガードのイネーブル化

指定インターフェイスで、BPDU ガードをイネーブルにできます。BPDU ガードがイネーブルにされたポートは、BPDU を受信すると、シャットダウンされます。

BPDU ガードは、指定インターフェイスで次のように設定にできます。

- **spanning-tree bpduguard enable**：指定インターフェイスで BPDU ガードを無条件にイネーブルにします。
- **spanning-tree bpduguard disable**：指定インターフェイスで BPDU ガードを無条件にディセーブルにします。
- **no spanning-tree bpduguard**：動作中のエッジ ポート インターフェイスに **spanning-tree port type edge bpduguard default** コマンドが設定されている場合、そのインターフェイスで BPDU ガードをイネーブルにします。

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。

インターフェイスの BPDU ガードをイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface type slot/port`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# spanning-tree bpduguard {enable | disable}`	指定したスパニングツリー エッジ インターフェイスの BPDU ガードをイネーブルまたはディセーブルにします。デフォルトでは、BPDU ガードは、物理イーサネット インターフェイスではディセーブルです。

次に、エッジ ポート Ethernet 1/4 で BPDU ガードを明示的にイネーブルにする例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpduguard enable
```

インターフェイスの BPDU ガードをディセーブルにする手順は、次のとおりです。

コマンド	目的
`switch(config-if)# no spanning-tree bpduguard`	動作中のエッジ ポート インターフェイスに **spanning-tree port type edge bpduguard default** コマンドが設定されている場合、そのインターフェイスで BPDU ガードをイネーブルにします。

BPDU フィルタリングのグローバルなイネーブル化

スパニングツリー エッジ ポートで、BPDU フィルタリングをデフォルトでグローバルにイネーブルにできます。

BPDU フィルタリングがイネーブルにされたエッジ ポートは、BPDU を受信すると、エッジ ポートとしての動作ステータスを失い、通常の STP 状態遷移を再開します。ただし、このポートは、エッジ ポートとしての設定は保持したままです。

注意　このコマンドを使用するときは注意してください。このコマンドを誤って使用すると、ブリッジング ループに陥る可能性があります。

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。
- 少なくとも一部のスパニングツリー エッジ ポートが設定済みであること。

（注）　グローバルにイネーブルにされた BPDU フィルタリングは、動作中のエッジ ポート *だけ*に適用されます。ポートは数個の BPDU をリンクアップ時に送出してから、実際に、発信 BPDU のフィルタリングを開始します。エッジ ポートは、BPDU を受信すると、動作中のエッジ ポート ステータスを失い、BPDU フィルタリングはディセーブルになります。

BPDU フィルタリングをグローバルにイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree port type edge bpdufilter default`	すべてのスパニングツリー エッジ ポートで、BPDU フィルタリングを、デフォルトでイネーブルにします。デフォルトでは、グローバルな BPDU フィルタリングはディセーブルです。

次に、すべての動作中のスパニングツリー エッジ ポートで BPDU フィルタリングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# spanning-tree port type edge bpdufilter default
```

指定インターフェイスでの BPDU フィルタリングのイネーブル化

指定インターフェイスに BPDU フィルタリングを適用できます。BPDU フィルタリングを特定のインターフェイス上でイネーブルにすると、そのインターフェイスは BPDU を送信しなくなり、受信した BPDU をすべてドロップするようになります。この BPDU フィルタリング機能は、トランキング インターフェイスであるかどうかに関係なく、すべてのインターフェイスに適用されます。

注意　指定インターフェイスで **spanning-tree bpdufilter enable** コマンドを入力する場合は注意してください。ホストに接続されていないポートに BPDU フィルタリングを明示的に設定すると、ブリッジング ループに陥る可能性があります。というのは、そうしたポートは受信した BPDU をすべて無視して、フォワーディング ステートに移行するからです。

このコマンドを入力すると、指定インターフェイスのポート設定が上書きされます。

このコマンドには次の 3 つの状態があります。

- **spanning-tree bpdufilter enable**：指定インターフェイスで BPDU ガードを無条件にイネーブルにします。
- **spanning-tree bpdufilter disable**：指定インターフェイスで BPDU フィルタリングを無条件にディセーブルにします。
- **no spanning-tree bpdufilter**：動作中のエッジ ポート インターフェイスに **spanning-tree port type edge bpdufilter default** コマンドが設定されている場合、そのインターフェイスで BPDU フィルタリングをイネーブルにします。

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。

（注）　特定のポートだけで BPDU フィルタリングをイネーブルにすると、そのポートでの BPDU の送受信が禁止されます。

インターフェイスの BPDU フィルタリングをイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface type slot/port`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# spanning-tree bpdufilter {enable | disable}`	指定したスパニングツリー エッジ インターフェイスの BPDU フィルタリングをイネーブルまたはディセーブルにします。デフォルトでは、BPDU フィルタリングはディセーブルです。

次に、スパニング ツリー エッジ ポート Ethernet 1/4 で BPDU フィルタリングを明示的にイネーブルにする例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpdufilter enable
```

インターフェイスの BPDU フィルタリングをディセーブルにする手順は、次のとおりです。

コマンド	目的
`switch(config-if)# no spanning-tree bpdufilter`	動作中のスパニングツリー エッジ ポート インターフェイスに **spanning-tree port type edge bpdufilter default** コマンドが設定されている場合、そのインターフェイスで BPDU フィルタリングをイネーブルにします。

ループ ガードのグローバルなイネーブル化

ループ ガードは、デフォルトの設定により、すべてのポイントツーポイント スパニングツリーの標準およびネットワーク ポートで、グローバルにイネーブルにできます。ループ ガードは、エッジ ポートでは動作しません。

ループ ガードを使用すると、ブリッジ ネットワークのセキュリティを高めることができます。ループ ガードは、単方向リンクを引き起こす可能性のある障害が原因で、代替ポートまたはルート ポートが指定ポートになるのを防ぎます。

（注） 指定インターフェイスでループ ガード コマンドを入力すると、グローバルなループ ガード コマンドが上書きされます。

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。
- スパニングツリー標準ポートが存在し、少なくとも一部のネットワーク ポートが設定済みであること。

ループ ガードをグローバルにイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# spanning-tree loopguard default`	スパニングツリーのすべての標準およびネットワーク ポートで、ループ ガードを、デフォルトでイネーブルにします。デフォルトでは、グローバルなループ ガードはディセーブルです。

次に、スパニングツリーのすべての標準およびネットワーク ポートでループ ガードをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# spanning-tree loopguard default
```

指定インターフェイスでのループ ガードまたはルート ガードのイネーブル化

（注）　ループ ガードは、スパニングツリーの標準またはネットワーク ポート上で実行できます。ルート ガードは、すべてのスパニングツリー ポート（標準、エッジ、ネットワーク）上で実行できます。

ループ ガードまたはルート ガードは、指定インターフェイスでイネーブルにできます。

特定のポートでルート ガードをイネーブルにすると、そのポートはルート ポートになることを禁止されます。ループ ガードは、単方向リンクを発生させる可能性のある障害が原因で代替ポートまたはルート ポートが指定ポートになるのを防ぎます。

特定のインターフェイスでループ ガードおよびルート ガードの両機能をイネーブルにすると、そのインターフェイスが属するすべての VLAN に両機能が適用されます。

（注）　指定インターフェイスでループ ガード コマンドを入力すると、グローバルなループ ガード コマンドが上書きされます。

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。
- ループ ガードが、スパニングツリーの標準またはネットワーク ポート上で設定されていること。

ループ ガードまたはルート ガードを特定のインターフェイスでイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface type slot/port`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# spanning-tree guard {loop | root | none}`	ループ ガードまたはルート ガードを、指定インターフェイスでイネーブルまたはディセーブルにします。ルート ガードはデフォルトでディセーブル、ループ ガードも指定ポートでディセーブルになります。 （注）　ループ ガードは、スパニングツリーの標準およびネットワーク インターフェイスだけで動作します。

次に、Ethernet ポート 1/4 で、ルート ガードをイネーブルにする例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree guard root
```

STP 拡張機能の設定の確認

STP 拡張機能の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
switch# **show running-config spanning-tree** [**all**]	スイッチ上でスパニングツリーの最新ステータスを表示します。
switch# **show spanning-tree** [*options*]	最新のスパニングツリー設定について、指定した詳細情報を表示します。

CHAPTER 11

ポート チャネルの設定

この章では、ポート チャネルを設定し、Cisco NX-OS でポート チャネルをより有効に利用するために Link Aggregation Control Protocol（LACP）を適用して設定する手順を説明します。

この章は、次の項で構成されています。

- ポート チャネルについて（11-1 ページ）
- ポート チャネルの設定（11-8 ページ）
- ポート チャネルの設定の確認（11-13 ページ）

ポート チャネルについて

ポート チャネルは、最大 8 個のインターフェイスを 1 つのグループにバンドルしたもので、帯域幅を広げ冗長性を高めることができます。これらの集約された各物理インターフェイス間でトラフィックのロード バランシングも行います。ポート チャネルの物理インターフェイスが少なくとも 1 つ動作していれば、そのポート チャネルは動作しています。

ポート チャネルは、互換性のあるインターフェイスをバンドルすることによって作成します。スタティック ポート チャネルのほか、Link Aggregation Control Protocol（LACP）を実行するポート チャネルを設定して稼働させることができます（LACP の詳細については、「LACP について」セクション（11-5 ページ）を参照してください）。

変更した設定をポート チャネルに適用すると、そのポート チャネルのメンバ インターフェイスにもそれぞれ変更が適用されます。たとえば、スパニングツリー プロトコル（STP）パラメータをポート チャネルに設定すると、Cisco NX-OS はこれらのパラメータをポート チャネルのそれぞれのインターフェイスに適用します。

関連するプロトコルを使用せず、スタティック ポート チャネルを使用すれば、設定を簡略化できます。IEEE 802.3ad に規定されている Link Aggregation Control Protocol（LACP）を使用すると、ポート チャネルをより効率的に使用することができます。LACP を使用すると、リンクによってプロトコル パケットが渡されます。

この項では、次のトピックについて取り上げます。

- ポート チャネルの概要（11-2 ページ）
- 互換性要件（11-2 ページ）
- ポート チャネルを使ったロード バランシング（11-3 ページ）
- LACP について（11-5 ページ）

ポート チャネルの概要

Cisco NX-OS は、ポート チャネルを使用して、広い帯域幅、冗長性、チャネル全体のロードバランシングを実現します。

最大 8 個のポートを 1 つのスタティック ポート チャネルに集約するか、または Link Aggregation Control Protocol（LACP）をイネーブルにできます。LACP によるポート チャネルを設定する手順は、スタティック ポート チャネルの場合とは若干異なります（「ポート チャネルの設定」セクション（11-8 ページ）を参照）。

（注）　Cisco NX-OS は、ポート チャネルに対するポート集約プロトコル（PAgP）をサポートしていません。

ポート チャネルは、個々のリンクを 1 つのチャネル グループにバンドルしたもので、それにより最大 8 個の物理リンクの帯域幅を集約した単一の論理リンクが作成されます。ポート チャネル内のメンバー ポートに障害が発生すると、障害が発生したリンクで伝送されていたトラフィックはポート チャネル内のその他のメンバー ポートに切り替わります。

各ポートにはポート チャネルが 1 つだけあります。ポート チャネル内のすべてのポートには互換性が必要です。つまり、回線速度が同じであり、かつ全二重モードで動作する必要があります（「互換性要件」セクション（11-2 ページ）を参照）。スタティック ポート チャネルを LACP なしで稼働すると、個々のリンクがすべて on チャネル モードで動作します。このモードを変更するには、LACP をイネーブルにする必要があります（「ポート チャネル モード」セクション（11-6 ページ）を参照）。

（注）　チャネル モードを、on から active、または on から passive に変更することはできません。

ポート チャネル インターフェイスを作成することで、ポート チャネルを直接作成することができます。またチャネル グループを作成して個々のポートを 1 つに集約することもできます。インターフェイスをチャネル グループに関連付ける際、ポート チャネルがなければ、Cisco NX-OS では対応するポート チャネルが自動的に作成されます。最初にポート チャネルを作成することもできます。その場合、Cisco NX-OS では、ポート チャネルと同じチャネル数で空のチャネル グループが作成され、デフォルトの設定が適用されます。

（注）　少なくともメンバ ポートの 1 つがアップしており、かつそのポートのチャネルが有効であれば、ポート チャネルは動作上アップ状態にあります。メンバ ポートがすべてダウンしていれば、ポート チャネルはダウンしています。

互換性要件

チャネル グループにインターフェイスを追加すると、Cisco NX-OS は、特定のインターフェイス属性をチェックし、そのインターフェイスがチャネル グループと互換性があるかどうかを確認します。また Cisco NX-OS は、そのインターフェイスがポート チャネル集約に参加することを許可する前に、インターフェイスのさまざまな動作属性もチェックします。

互換性チェックの対象となる動作属性は次のとおりです。

- ポート モード
- アクセス VLAN

- トランク ネイティブ VLAN
- 許可 VLAN リスト
- 速度
- 802.3x フロー制御設定
- MTU

  Cisco Nexus 5000 シリーズ スイッチは、システム レベルの MTU のみをサポートするため、この属性は厳密には適用されません。
- ブロードキャスト/ユニキャスト/マルチキャスト ストーム制御設定
- プライオリティ フロー制御
- タグなし CoS

Cisco NX-OS で使用される完全な互換性チェック リストを確認するには、**show port-channel compatibility-parameters** コマンドを使用します。

チャネル モード セットを **on** に設定したインターフェイスだけをスタティック ポート チャネルに追加できます。また LACP を実行するポート チャネルには、チャネル モードが **active** または **passive** に設定されたインターフェイスだけを追加することもできます（ポート チャネル モードについては「ポート チャネル モード」セクション（11-6 ページ）を参照）。これらの属性は個別のメンバ ポートに設定できます。

インターフェイスがポート チャネルに参加すると、個々の一部のパラメータ値はポート チャネルの値に置き換わります。該当パラメータは次のとおりです。

- 帯域幅
- MAC address
- スパニングツリー プロトコル

多くのインターフェイス パラメータは、インターフェイスがポート チャネルに参加しても影響を受けません。該当パラメータは次のとおりです。

- 説明
- CDP
- LACP ポート プライオリティ
- デバウンス

ポート チャネルを使ったロード バランシング

Cisco NX-OS は、ポート チャネルを構成するすべての動作中インターフェイス間でトラフィックのロード バランスを実現します。フレーム内のアドレスから生成されたバイナリ パターンの一部を数値に圧縮変換し、それを使用してチャネル内の 1 つのリンクを選択することによってロードバランシングを行います。ポート チャネルではデフォルトでロード バランシングが行われます。また、基本設定では、次の基準によってリンクが選択されます。

- レイヤ 2 フレームの場合は、送信元および宛先の MAC アドレスを使用します。
- レイヤ 3 フレームの場合は、送信元および宛先の MAC アドレスと送信元および宛先の Internet Protocol（IP）アドレスを使用します。
- レイヤ 4 フレームの場合は、送信元および宛先の MAC アドレス、送信元および宛先の IP アドレス、送信元および宛先のポート番号を使用します。

次のいずれかに基づいてポート チャネル全体でのロード バランシングが行われるようにスイッチを設定することができます。

- 宛先 MAC アドレス
- 送信元 MAC アドレス
- 送信元および宛先 MAC アドレス
- 宛先 IP アドレス
- 送信元 IP アドレス
- 送信元および宛先 IP アドレス
- 宛先 TCP/UDP ポート番号
- 送信元 TCP/UDP ポート番号
- 送信元および宛先 TCP/UDP ポート番号

表 11-1 に、各設定で使用する基準を示します。

表 11-1　ポート チャネル ロードバランシング基準

設定	レイヤ 2 基準	レイヤ 3 基準	レイヤ 4 基準
宛先 MAC	宛先 MAC	宛先 MAC	宛先 MAC
送信元 MAC	送信元 MAC	送信元 MAC	送信元 MAC
送信元/宛先 MAC	送信元/宛先 MAC	送信元/宛先 MAC	送信元/宛先 MAC
宛先 IP	宛先 MAC	宛先 MAC、宛先 IP	宛先 MAC、宛先 IP
Source IP	送信元 MAC	送信元 MAC、送信元 IP	送信元 MAC、送信元 IP
送信元/宛先 IP	送信元/宛先 MAC	送信元/宛先 MAC、送信元/宛先 IP	送信元/宛先 MAC、送信元/宛先 IP
宛先 TCP/UDP ポート	宛先 MAC	宛先 MAC、宛先 IP	宛先 MAC、宛先 IP、宛先ポート
送信元 TCP/UDP ポート	送信元 MAC	送信元 MAC、送信元 IP	送信元 MAC、送信元 IP、送信元ポート
送信元および宛先 TCP/UDP ポート	送信元/宛先 MAC	送信元/宛先 MAC、送信元/宛先 IP	送信元/宛先 MAC、送信元/宛先 IP、送信元/宛先ポート

使用している設定で最も多様なバランス基準を提供するオプションを使用してください。たとえば、ポート チャネルのトラフィックが 1 つの MAC アドレスにだけ送られ、ポート チャネルでのロード バランシングの基準としてその宛先 MAC アドレスが使用されている場合、ポート チャネルでは常にそのポート チャネル内の同じリンクが選択されます。したがって、送信元アドレスまたは IP アドレスを使用すると、結果的により優れたロード バランシングが行われることになります。

LACP について

LACP では、最大 8 のインターフェイスを 1 つのポート チャネルに設定できます。

この項では、次のトピックについて取り上げます。

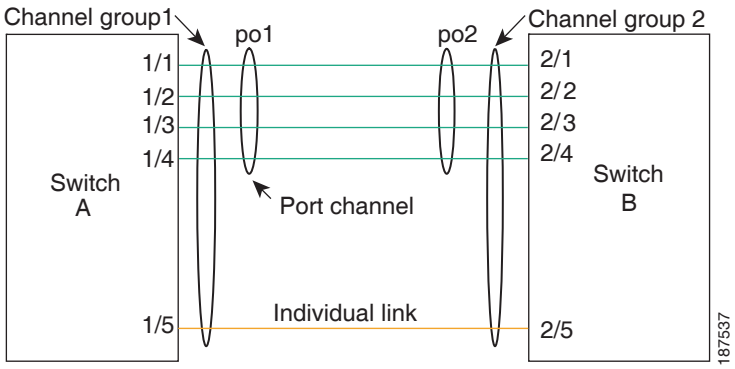
- LACP の概要（11-5 ページ）
- LACP ID パラメータ（11-6 ページ）
- ポート チャネル モード（11-6 ページ）
- LACP マーカー レスポンダ（11-7 ページ）
- LACP がイネーブルのポート チャネルとスタティック ポート チャネルの相違点（11-8 ページ）

LACP の概要

（注）　この機能を使用するには、LACP をイネーブルにする必要があります。

図 11-1 に、個別リンクを LACP ポート チャネルおよびチャネル グループに組み込み、個別リンクとして機能させる方法を示します。

図 11-1　　個別リンクをポート チャネルに組み込む



LACP を使用すると、最大 8 つのインターフェイスを 1 つのチャネル グループに束ねることができます。

（注）　ポート チャネルを削除すると、関連付けられたチャネル グループも Cisco NX-OS によって自動的に削除されます。すべてのメンバ インターフェイスは以前の設定に戻ります。

LACP 設定が 1 つでも存在する限り、LACP をディセーブルにはできません。

LACP ID パラメータ

LACP では次のパラメータが使用されます。

- LACP システム プライオリティ:LACP を稼働している各システムは、LACP システム プライオリティ値を持っています。このパラメータのデフォルト値である 32768 をそのまま使用するか、1 ～ 65535 の範囲で値を設定できます。LACP は、このシステム プライオリティと MAC アドレスを組み合わせてシステム ID を生成します。また、システム プライオリティを他のデバイスとのネゴシエーションにも使用します。システム プライオリティ値が大きいほど、プライオリティは低くなります。

  （注） LACP システム ID は、LACP システム プライオリティ値と MAC アドレスを組み合わせたものです。

- LACP ポート プライオリティ:LACP を使用するように設定された各ポートには、LACP ポート プライオリティが割り当てられます。デフォルト値である 32768 をそのまま使用するか、1 ～ 65535 の範囲で値を設定できます。LACP では、ポート プライオリティおよびポート番号によりポート ID が構成されます。また、互換性のあるポートのうち一部を束ねることができない場合に、どのポートをスタンバイ モードにし、どのポートをアクティブ モードにするかを決定するのに、ポート プライオリティを使用します。LACP では、ポート プライオリティ値が大きいほど、プライオリティは低くなります。指定ポートが、より低い LACP プライオリティを持ち、ホット スタンバイ リンクではなくアクティブ リンクとして選択される可能性が最も高くなるように、ポート プライオリティを設定できます。
- LACP 管理キー:LACP は、LACP を使用するように設定された各ポート上のチャネル グループ番号に等しい管理キー値を自動的に設定します。管理キーにより、他のポートとともに集約されるポートの機能が定義されます。他のポートとともに集約されるポートの機能は、次の要因によって決まります。
  - ポートの物理特性（データ レート、デュプレックス機能、ポイントツーポイントまたは共有メディア ステートなど）
  - ユーザが作成した設定に関する制約事項

ポート チャネル モード

ポート チャネルの個別インターフェイスは、チャネル モードで設定します。プロトコルを使用せずにスタティック ポート チャネルを稼働すると、そのチャネル モードは常に **on** に設定されます。デバイス上で LACP をグローバルにイネーブルにした後、各チャネルの LACP をイネーブルにします。それには、各インターフェイスのチャネル モードを **active** または **passive** に設定します。LACP チャネル グループを構成する個々のリンクについて、どちらかのチャネル モードを設定できます。

（注） **active** または **passive** のチャネル モードで、個々のインターフェイスを設定するには、まず、LACP をグローバルにイネーブルにする必要があります。

表 11-2 で、各チャネル モードについて説明します。

表 11-2　ポート チャネルの個別リンクのチャネル モード

チャネル モード	説明
passive	ポートをパッシブなネゴシエーション状態にする LACP モード。この状態では、ポートは受信した LACP パケットに応答はしますが、LACP ネゴシエーションを開始することはありません。
active	ポートをアクティブ ネゴシエーション ステートにする LACP モード。この場合ポートでは LACP パケットを送信することにより、他のポートとのネゴシエーションが開始されます。
on	すべてのスタティック ポート チャネル（つまり LACP を稼働していないポート チャネル）は、このモードのままになります。LACP をイネーブルにする前にチャネル モードを active または passive に変更しようとすると、デバイスがエラー メッセージを返します。 チャネルで LACP をイネーブルにするには、そのチャネルのインターフェイスでチャネル モードを **active** または **passive** に設定します。LACP は、**on** 状態のインターフェイスとネゴシエートする場合、LACP パケットを受信しないため、そのインターフェイスと個別のリンクを形成します。つまり、LACP チャネル グループには参加しません。

passive と active のどちらのモードでも、ポート速度やトランキング ステートなどの基準に基づいてポート チャネルを構成可能かどうかを判定するため、LACP によるポート間のネゴシエーションが行われます。passive モードは、リモート システム、つまり、パートナーが、LACP をサポートしているかどうかが不明な場合に便利です。

次の例に示したとおり、ポートは、異なる LACP モードであっても、それらのモード間で互換性があれば、LACP ポート チャネルを構成することができます。

- active モードのポートは、active モードの別のポートとともにポート チャネルを正しく形成できます。
- active モードのポートは、passive モードの別のポートとともにポート チャネルを形成できます。
- passive モードのポートは、どちらのポートもネゴシエーションを開始しないため、passive モードの別のポートとともにポート チャネルを形成できません。
- on モードのポートは LACP を実行していません。

LACP マーカー レスポンダ

ポート チャネルを使用すると、リンク障害やロード バランシング動作に伴って、データ トラフィックが動的に再配信される場合があります。LACP では、マーカー プロトコルを使用して、こうした再配信によってフレームが重複したり順序が変わったりしないようにします。Cisco NX-OS は、マーカー レスポンダだけをサポートしています。

LACP がイネーブルのポート チャネルとスタティック ポート チャネルの相違点

表 11-3 は、LACP がイネーブルのポート チャネルとスタティック ポート チャネルとの主な相違点をまとめたものです。

表 11-3　LACP がイネーブルのポート チャネルとスタティック ポート チャネル

	LACP がイネーブルのポート チャネル	スタティック ポート チャネル
適用されるプロトコル	グローバルにイネーブル化	なし。
リンクのチャネル モード	次のいずれか。 • Active • Passive	on モードのみ
チャネルを構成する最大リンク数	8	8

ポート チャネルの設定

デバイスに複数のポート チャネルを設定できます。

この項では、次のトピックについて取り上げます。

- ポート チャネルの作成（11-8 ページ）
- ポート チャネルへのポートの追加（11-9 ページ）
- ポート チャネルを使ったロード バランシングの設定（11-10 ページ）
- LACP のイネーブル化（11-11 ページ）
- ポート チャネル ポート モードの設定（11-12 ページ）
- LACP のシステム プライオリティおよびシステム ID の設定（11-12 ページ）
- LACP ポート プライオリティの設定（11-13 ページ）

ポート チャネルの作成

チャネル グループを作成する前にポート チャネルを作成します。Cisco NX-OS は、対応するチャネル グループを自動的に作成します。

LACP ベースのポート チャネルにする場合は、LACP をイネーブルにします（「LACP のイネーブル化」セクション（11-11 ページ）を参照）。

ポート チャネルを作成する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface port-channel channel-number`	設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。範囲は 1 ～ 4096 です。チャネル グループがまだ存在していなければ、Cisco NX-OS によって自動的に作成されます。 **（注）** 新規の（イーサネット ポート用）ポート チャネルを作成するには、未使用のチャネル番号を入力します。使用済みおよび未使用のチャネル番号の範囲を表示するには、**show port-channel usage** コマンドを使用します。

次の例は、ポート チャネルの作成方法を示しています。

```
switch# configure terminal
switch (config)# interface port-channel 1
```

ポート チャネル、および対応するチャネル グループを削除する手順は、次のとおりです。

コマンド	目的
`switch(config)# no interface port-channel channel-number`	ポート チャネルを削除し、関連するチャネル グループを削除します。ポート チャネルを削除したときのインターフェイス コンフィギュレーションの変化について詳しくは、「互換性要件」セクション（11-2 ページ）を参照してください。

ポート チャネルへのポートの追加

新規のチャネル グループ、または他のポートがすでに属しているチャネル グループにポートを追加できます。ポート チャネルがない場合は、Cisco NX-OS によって、このチャネル グループに関連付けられたポート チャネルが作成されます。

LACP ベースのポート チャネルにする場合は、LACP をイネーブルにします（「LACP のイネーブル化」セクション（11-11 ページ）を参照）。ポート チャネルを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface type slot/port`	チャネル グループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# switchport mode trunk`	（任意）指定インターフェイスをトランク ポートとして設定します。

	コマンド	目的
ステップ 4	switch(config-if)# **switchport trunk** {**allowed vlan** *vlan-id* | **native vlan** *vlan-id*}	(任意)トランク ポートに必要なパラメータを設定します。
ステップ 5	switch(config-if)# **channel-group** *channel-number*	チャネル グループ内にポートを設定し、モードを設定します。channel-number の指定できる範囲は 1 ～ 4096 です。ポート チャネルがない場合は、Cisco NX-OS によって、このチャネル グループに関連付けられたポート チャネルが作成されます。[1]

1. これを、暗黙的なポート チャネル作成と言います。

チャネル グループからポートを削除する手順は、次のとおりです。

コマンド	目的
switch(config)# **no channel-group**	チャネル グループからポートを削除します。チャネル グループから削除されたポートは元の設定に戻ります。

次に、イーサネット インターフェイス 1/4 をチャネル グループ 1 に追加する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# switchport mode trunk
switch(config-if)# channel-group 1
```

ポート チャネルを使ったロード バランシングの設定

デバイス全体に適用されるポート チャネル用のロードバランシング アルゴリズムを設定できます。

LACP ベースのポート チャネルにする場合は、LACP をイネーブルにします(「LACP のイネーブル化」セクション(11-11 ページ)を参照)。ポート チャネルを使用したロード バランシングを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **port-channel load-balance ethernet** {**destination-ip** | **destination-mac** | **destination-port** | **source-dest-ip** | **source-dest-mac** | **source-dest-port** | **source-ip** | **source-mac** | **source-port**}	デバイスのロード バランシング アルゴリズムを指定します。指定可能なアルゴリズムはデバイスによって異なります。デフォルトは **source-dest-mac** です。
ステップ 3	switch(config-router)# **show port-channel load-balance**	(任意)ポート チャネル ロード バランシング アルゴリズムを表示します。

次の例は、ポート チャネルに対して送信元 IP によるロード バランシングを設定する方法を示したものです。

```
switch# configure terminal
switch (config)# port-channel load-balance ethernet source-ip
```

デフォルトのロード バランシング アルゴリズムである、非 IP トラフィック用の source-dest-mac、および IP トラフィック用の source-dest-ip を復元する手順は、次のとおりです。

コマンド	目的
`switch(config)# no port-channel load-balance ethernet`	デフォルトのロード バランシング アルゴリズムを復元します。

（注）　**source-dest-ip**、**source-dest-mac**、**source-dest-port** の各キーワードは、Cisco NX-OS の 4.0(1a)N1 より以前のリリースの場合、それぞれ **source-destination-ip**、**source-destination-mac**、**source-destination-port** となります。

LACP のイネーブル化

LACP はデフォルトではディセーブルです。LACP の設定を開始するには、LACP をイネーブルにする必要があります。LACP 設定が 1 つでも存在する限り、LACP をディセーブルにはできません。

LACP は、LAN ポート グループの機能を動的に学習し、残りの LAN ポートに通知します。LACP では、適合する複数のイーサネット リンクが検出されると、これらのリンクが 1 つのポート チャネルにグループ化されます。次に、ポート チャネルは単一ブリッジ ポートとしてスパニングツリーに追加されます。

LACP をイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# feature lacp`	スイッチ上で LACP をイネーブルにします。
ステップ 3	`switch(config)# show system internal clis feature`	(任意) イネーブルにされた機能を表示します。

次に、LACP をイネーブルにする例を示します。

```
switch# configure terminal
switch (config)# feature lacp
```

ポート チャネル ポート モードの設定

LACP をイネーブルにしたら、LACP ポート チャネルのそれぞれのリンクのチャネル モードを **active** または **passive** に設定できます。このチャネル コンフィギュレーション モードを使用すると、リンクは LACP で動作可能になります。

関連するプロトコルを使用せずにポート チャネルを設定すると、リンク両端のすべてのインターフェイスでは **on** チャネル モードが維持されます。

LACP リンク モードを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface type slot/port`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# channel-group number mode {active | on | passive}`	ポート チャネルのリンクのポート モードを指定します。LACP をイネーブルにしたら、各リンクまたはチャネル全体を active または passive に設定します。 関連するプロトコルを使用せずにポート チャネルを実行する場合、ポート チャネル モードは常に on です。 デフォルトのポート チャネル モードは on です。
	`switch(config-if)# no channel-group number mode`	指定インターフェイスのポート モードを on に戻します

次に、チャネル グループ 5 のイーサネット インターフェイス 1/4 で、LACP がイネーブルなインターフェイスを active ポート チャネル モードに設定する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# channel-group 5 mode active
```

LACP のシステム プライオリティおよびシステム ID の設定

LACP システム ID は、LACP システム プライオリティ値と MAC アドレスを組み合わせたものです。

LACP システム プライオリティを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# lacp system-priority priority`	LACP で使用するシステム プライオリティを設定します。指定できる範囲は 1 ～ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。
ステップ 3	`switch(config-if)# show lacp system-identifier`	LACP システム識別子を表示します。

次に、LACP システム プライオリティを 2500 に設定する例を示します。

```
switch# configure terminal
switch(config)# lacp system-priority 2500
```

LACP ポート プライオリティの設定

LACP をイネーブルにしたら、ポート プライオリティの LACP ポート チャネルにそれぞれのリンクを設定できます。

LACP リンク モードとポート プライオリティを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** *type slot/port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **lacp port-priority** *priority*	LACP で使用するポート プライオリティを設定します。指定できる範囲は 1 ～ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。

次に、イーサネット インターフェイス 1/4 の LACP ポート プライオリティを 40000 に設定する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# lacp port priority 40000
```

ポート チャネルの設定の確認

ポート チャネルの設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
switch# **show interface port-channel** *channel-number*	ポート チャネル インターフェイスのステータスを表示します。
switch# **show system internal clis feature**	イネーブルにされた機能を表示します。
switch# **show lacp** {**counters** | **interface** *type slot/port* | **neighbor** | **port-channel** | **system-identifier**}	LACP 情報を表示します。
switch# **show port-channel compatibility-parameters**	ポート チャネルに追加するためにメンバ ポート間で同じにするパラメータを表示します。
switch# **show port-channel database** [**interface port-channel** *channel-number*]	1 つ以上のポート チャネル インターフェイスの集約状態を表示します。
switch# **show port-channel load-balance**	ポート チャネルで使用するロード バランシングのタイプを表示します。

コマンド	目的
`switch# show port-channel summary`	ポート チャネル インターフェイスのサマリーを表示します。
`switch# show port-channel traffic`	ポート チャネルのトラフィック統計情報を表示します。
`switch# show port-channel usage`	使用済みおよび未使用のチャネル番号の範囲を表示します。
`switch# show port-channel database`	現在実行中のポート チャネル機能に関する情報を表示します。

CHAPTER 12

アクセス インターフェイスとトランク インターフェイスの設定

イーサネット インターフェイスは、アクセス ポートまたはトランク ポートとして設定できます。トランクは単一のリンクを介して複数の VLAN トラフィックを伝送します。これにより、ネットワーク全体に VLAN を拡張できます。

この章は、次の項で構成されています。

- アクセス インターフェイスとトランク インターフェイスについて（12-1 ページ）
- アクセス インターフェイスとトランク インターフェイスの設定（12-4 ページ）
- インターフェイスの設定の確認（12-8 ページ）

アクセス インターフェイスとトランク インターフェイスについて

この項では、次のトピックについて取り上げます。

- アクセス インターフェイスとトランク インターフェイスの概要（12-1 ページ）
- IEEE 802.1Q カプセル化の概要（12-3 ページ）
- アクセス VLAN の概要（12-3 ページ）
- トランク ポートのネイティブ VLAN ID の概要（12-4 ページ）
- 許可 VLAN の概要（12-4 ページ）

（注） Cisco NX-OS では、IEEE 802.1Q タイプの VLAN トランク カプセル化だけをサポートしています。

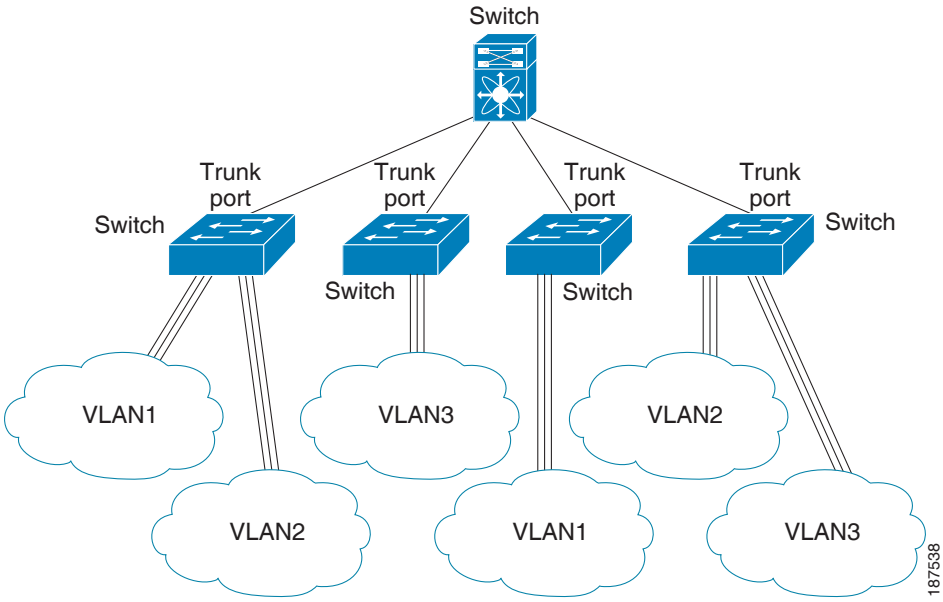
アクセス インターフェイスとトランク インターフェイスの概要

イーサネット インターフェイスは、次のように、アクセス ポートまたはトランク ポートとして設定できます。

- アクセス ポートはインターフェイス上に設定された 1 つの VLAN だけに対応し、1 つの VLAN のトラフィックだけを伝送します。
- トランク ポートはインターフェイス上に設定された 2 つ以上の VLAN に対応しているため、複数の VLAN のトラフィックを同時に伝送できます。

図 12-1 に、ネットワーク内でのトランク ポートの使用例を示します。トランク ポートは、2 つ以上の VLAN のトラフィックを伝送します。

図 12-1　　トランキング環境におけるデバイス



複数の VLAN に対応するトランク ポート上で正しくトラフィックを伝送するために、スイッチは、IEEE 802.1Q カプセル化、つまりタギング方式（詳細については、「IEEE 802.1Q カプセル化の概要」セクション（12-3 ページ）を参照してください）を使用します。

アクセス ポートでのパフォーマンスを最適化するには、そのポートをホスト ポートとして設定します。ホスト ポートとして設定されたポートは、自動的にアクセス ポートとして設定され、チャネル グループ化はディセーブルになります。ホスト ポートを使用すると、指定ポートがパケットの転送を開始するための所要時間を短縮できます。

（注）　ホスト ポートとして設定できるのは端末だけです。端末以外のポートをホストとして設定しようとするとエラーになります。

アクセス ポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元の MAC アドレスを学習せずにドロップします。

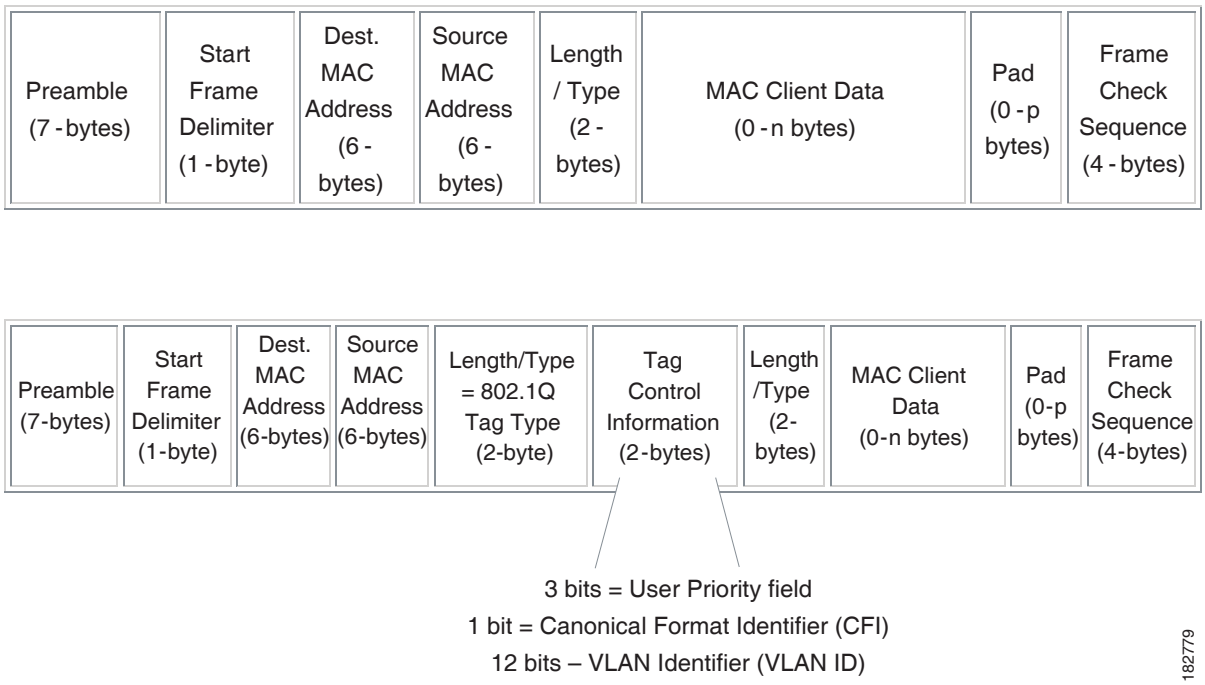
（注）　イーサネット インターフェイスはアクセス ポートまたはトランク ポートとして動作できますが、両方のポート タイプとして同時に動作することはできません。

IEEE 802.1Q カプセル化の概要

トランクは、デバイスと他のネットワーク デバイス間のポイントツーポイント リンクです。トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張することができます。

複数の VLAN に対応するトランク ポート上で正しくトラフィックを伝送するために、デバイスは、IEEE 802.1Q カプセル化、つまりタギング方式（フレーム ヘッダーに挿入されたタグを使用する方式）を使用します。このタグには、そのフレームおよびパケットが属する特定の VLAN に関する情報が含まれます。タグ方式を使用すると、複数の異なる VLAN 用にカプセル化されたパケットが、同じポートを通過しても、各 VLAN のトラフィックを区別することができます。また、VLAN タグのカプセル化を使用すると、同じ VLAN 上のネットワークを経由するエンドツーエンドでトラフィックを転送できます。

図 12-2　802.1Q タグが含まれているヘッダーと含まれていないヘッダー



アクセス VLAN の概要

（注）　アクセス VLAN を割り当て、プライベート VLAN のプライマリ VLAN としても動作させると、そのアクセス VLAN に対応するすべてのアクセス ポートが、プライベート VLAN モードのプライマリ VLAN 向けのすべてのブロードキャスト トラフィックを受信するようになります。

アクセス モードでポートを設定すると、そのインターフェイスのトラフィックを伝送する VLAN を指定できます。アクセス モードのポート（アクセス ポート）用に VLAN を設定しないと、そのインターフェイスはデフォルトの VLAN（VLAN1）のトラフィックだけを伝送します。

VLAN のアクセス ポート メンバーシップを変更するには、新しい VLAN を指定します。VLAN をアクセス ポートのアクセス VLAN として割り当てるには、まず、VLAN を作成する必要があります。アクセス ポート上のアクセス VLAN を、まだ作成されていない VLAN に変更すると、システムはそのアクセス ポートをシャット ダウンします。

アクセス ポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元の MAC アドレスを学習せずにドロップします。

トランク ポートのネイティブ VLAN ID の概要

（注）　ネイティブ VLAN ID 番号は、トランクの両端で*一致していなければなりません。*

トランク ポートは、タグなしのパケットと 802.1Q タグ付きのパケットを同時に伝送できます。デフォルトのポート VLAN ID をトランク ポートに割り当てると、すべてのタグなしトラフィックが、そのトランク ポートのデフォルトのポート VLAN ID で伝送され、タグなしトラフィックはすべてこの VLAN に属するものと見なされます。この VLAN のことを、トランク ポートのネイティブ VLAN ID といいます。ネイティブ VLAN ID とは、トランク ポート上でタグなしトラフィックを伝送する VLAN のことです。

トランク ポートは、デフォルトのポート VLAN ID と同じ VLAN が設定された出力パケットをタグなしで送信します。他のすべての出力パケットは、トランク ポートによってタグ付けされます。ネイティブ VLAN ID を設定しないと、トランク ポートはデフォルト VLAN を使用します。

許可 VLAN の概要

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックを送受信します。各トランク上では、すべての VLAN ID が許可されます。この包括的なリストから VLAN を削除することによって、特定の VLAN からのトラフィックが、そのトランクを通過するのを禁止できます。トランク経由でトラフィックを伝送したい VLAN を後でリストに戻すこともできます。

デフォルト VLAN のスパニングツリー プロトコル（STP）トポロジを分割するには、許可 VLAN のリストから VLAN1 を削除します。この分割を行わないと、VLAN1（デフォルトでは、すべてのポートでイネーブル）が非常に大きな STP トポロジを形成し、STP のコンバージェンス中に問題が発生する可能性があります。VLAN1 を削除すると、そのポート上で VLAN1 のデータ トラフィックはすべてブロックされますが、制御トラフィックは通過し続けます。

アクセス インターフェイスとトランク インターフェイスの設定

この項では、次のトピックについて取り上げます。

- イーサネット アクセス ポートとしての LAN インターフェイスの設定（12-5 ページ）
- アクセス ホスト ポートの設定（12-5 ページ）
- トランク ポートの設定（12-6 ページ）
- 802.1Q トランク ポートのネイティブ VLAN の設定（12-7 ページ）
- トランキング ポートの許可 VLAN の設定（12-8 ページ）

イーサネット アクセス ポートとしての LAN インターフェイスの設定

イーサネット ポートはアクセス ポートとして設定できます。アクセス ポートは、パケットを、1 つのタグなし VLAN 上だけで送信します。管理者は、そのインターフェイスで伝送する VLAN トラフィックを指定します。アクセス ポートの VLAN を指定しないと、そのインターフェイスは、デフォルト VLAN だけのトラフィックを伝送します。デフォルトの VLAN は VLAN 1 です。

VLAN をアクセス VLAN として指定するには、その VLAN が存在しなければなりません。システムは、存在しないアクセス VLAN に割り当てられたアクセス ポートをシャット ダウンします。

イーサネット アクセス ポートを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface {{type slot/port} | {port-channel number}}`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# switchport mode {access | trunk}`	トランキングなし、タグなしの単一 VLAN イーサネット インターフェイスとして、インターフェイスを設定します。アクセス ポートは、1 つの VLAN のトラフィックだけを伝送できます。デフォルトでは、アクセス ポートは VLAN1 のトラフィックを伝送します。異なる VLAN のトラフィックを伝送するようにアクセス ポートを設定するには、**switchport access vlan** コマンドを使用します。
ステップ 4	`switch(config-if)# switchport access vlan vlan-id`	このアクセス ポートでトラフィックを伝送する VLAN を指定します。このコマンドを入力しないと、アクセス ポートは VLAN1 だけのトラフィックを伝送します。このコマンドを使用して、アクセス ポートがトラフィックを伝送する VLAN を変更できます。

次に、イーサネット 1/10 を、VLAN 5 のトラフィックだけを伝送するイーサネット アクセス ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/10
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
```

アクセス ホスト ポートの設定

（注） **switchport host** コマンドは、エンド ステーションに接続されたインターフェイスだけに適用する必要があります。

エンド ステーションに接続されたアクセス ポートでのパフォーマンスを最適化するには、そのポートをホスト ポートとしても設定します。アクセス ホスト ポートは、エッジ ポートと同じようにスパニングツリー プロトコル（STP）を処理して、ブロッキング ステートおよびラーニング

ステートを経由せずに、フォワーディング ステートに直接移行します。インターフェイスをアクセス ホスト ポートとして設定すると、そのインターフェイス上でポート チャネル動作がディセーブルになります。

（注）　ポート チャネル インターフェイスの詳細については、第 11 章「ポート チャネルの設定」を、スパニングツリー プロトコルの詳細については、第 8 章「Rapid PVST+ の設定」を参照してください。

エンド ステーションのインターフェイスに接続された適切なインターフェイスを設定することを確認してください。

アクセス ホスト ポートを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface type slot/port`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# switchport host`	インターフェイスをアクセス ホスト ポートとして設定します。このポートはただちに、スパニングツリー フォワーディング ステートに移行し、このインターフェイスのポート チャネル動作をディセーブルにします。 **（注）**　このコマンドは端末だけに適用します。

次の例は、イーサネット 1/10 を、**PortFast がイネーブルにされ**、ポート チャネルがディセーブルにされたイーサネット アクセス ポートとして設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/10
switch(config-if)# switchport host
```

トランク ポートの設定

イーサネット ポートをトランク ポートとして設定できます。トランク ポートは、ネイティブ VLAN のタグなしパケット、および複数の VLAN のカプセル化されたタグ付きパケットを伝送します（カプセル化の詳細については、「IEEE 802.1Q カプセル化の概要」セクション（12-3 ページ）を参照してください）。

（注）　Cisco NX-OS は、IEEE 802.1Q カプセル化だけをサポートしています。

トランク ポートを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface {type slot/port | port-channel number}`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# switchport mode {access | trunk}`	インターフェイスをイーサネット トランク ポートとして設定します。トランク ポートは、同じ物理リンクで 1 つ以上の VLAN 内のトラフィックを伝送できます（各 VLAN はトランキングが許可された VLAN リストに基づいています）。デフォルトでは、トランク インターフェイスはすべての VLAN のトラフィックを伝送できます。特定のトランク上で特定の VLAN だけを許可するように指定するには、**switchport trunk allowed vlan** コマンドを使用します。

次の例は、イーサネット 3/1 をイーサネット トランク ポートとして設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport mode trunk
```

802.1Q トランク ポートのネイティブ VLAN の設定

このパラメータを設定しないと、トランク ポートは、デフォルト VLAN をネイティブ VLAN ID として使用します。

802.1Q トランク ポートのネイティブ VLAN を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface {type slot/port | port-channel number}`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# switchport trunk native vlan vlan-id`	802.1Q トランクのネイティブ VLAN を設定します。指定できる範囲は 1 ～ 4094 です（ただし、内部使用に予約されている VLAN は除きます）。デフォルト値は VLAN 1 です。

次の例は、イーサネット トランク ポート 3/1 のネイティブ VLAN を VLAN 5 に設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport trunk native vlan 5
```

トランキング ポートの許可 VLAN の設定

特定のトランク ポートで許可されている VLAN の ID を指定できます。

指定トランク ポートの許可 VLAN を設定する前に、正しいインターフェイスを設定していること、およびそのインターフェイスがトランクであることを確認してください。

トランク ポートの許可 VLAN を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface {type slot/port | port-channel number}`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# switchport trunk allowed vlan {vlan-list all | none [add |except | none | remove {vlan-list}]}`	トランク インターフェイスの許可 VLAN を設定します。デフォルトでは、トランク インターフェイス上のすべての VLAN（1 ～ 3967 および 4048 ～ 4094）が許可されます。VLAN 3968 ～ 4047 は、内部利用のためにデフォルトで予約されている VLAN です。この VLAN グループは設定できません。デフォルトでは、すべてのトランク インターフェイスですべての VLAN が許可されます。 **（注）** 内部で割り当て済みの VLAN を、トランク ポート上の許可 VLAN として追加することはできません。内部で割り当て済みの VLAN を、トランク ポートの許可 VLAN として登録しようとすると、メッセージが返されます。

次の例は、イーサネット トランク ポート 3/1 の許可 VLAN のリストに、VLAN 15 ～ 20 を追加する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport trunk allow vlan 15-20
```

インターフェイスの設定の確認

アクセス インターフェイスとトランク インターフェイスの設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
`switch# show interface`	インターフェイス設定を表示します。
`switch# show interface switchport`	すべてのイーサネット インターフェイス（アクセス インターフェイスとトランク インターフェイスを含む）の情報を表示します。
`switch# show interface brief`	インターフェイス設定情報を表示します。

CHAPTER 13

MAC アドレス テーブルの設定

すべてのイーサネット スイッチング ポートが、メディア アクセス コントロール（MAC）アドレス テーブルを保持しています。

この章は、次の項で構成されています。

- MAC アドレスに関する情報（13-1 ページ）
- MAC アドレスの設定（13-2 ページ）
- MAC アドレス設定の確認（13-4 ページ）

MAC アドレスに関する情報

LAN ポート間で効率的にフレームをスイッチングするために、スイッチはアドレス テーブルを保持しています。スイッチがフレームを受信すると、送信側のネットワーク デバイスの MAC アドレスを受信側の LAN ポートにアソシエートします。

スイッチは、受信したフレームの送信元 MAC アドレスを使用して、アドレス テーブルを動的に構築します。そのアドレス テーブルにリストされていない受信側 MAC アドレスのフレームを受信すると、そのフレームを、同一 VLAN のフレームを受信したポート以外のすべての LAN ポートへフラッディングします。送信先ステーションが応答したら、スイッチは、その関連の送信元 MAC アドレスとポート ID をアドレス テーブルに追加します。その後、スイッチは、以降のフレームを、すべての LAN ポートにフラッディングするのではなく単一の LAN ポートへと転送します。

MAC アドレスを手作業で入力することもできます。これは、テーブル内で、スタティック MAC アドレスとなります。このようなスタティック MAC エントリは、スイッチを再起動しても維持されます。

さらに、マルチキャスト アドレスを静的に設定された MAC アドレスとして入力することもできます。マルチキャスト アドレスは、複数のインターフェイスを送信先として受け付けることができます。

アドレス テーブルには、フレームを一切フラッディングさせることなく、複数のユニキャスト アドレス エントリおよびマルチキャスト アドレス エントリを格納できます（詳細については、「設定の制限値」セクション（51-1 ページ）を参照してください）。スイッチは設定可能なエージング タイマーによって定義されたエージング メカニズムを使用するため、アドレスが非アクティブなまま指定した秒数が経過すると、そのアドレスはアドレス テーブルから削除されます。

MAC アドレスの設定

この項では、次のトピックについて取り上げます。

- スタティック MAC アドレスの設定（13-2 ページ）
- MAC テーブルのエージング タイムの設定（13-3 ページ）
- MAC テーブルからのダイナミック アドレスの消去（13-3 ページ）

スタティック MAC アドレスの設定

スイッチの MAC アドレスは手動で設定できます。手動で設定したアドレスは、スタティック MAC アドレスとなります。

（注）スタティック MAC アドレスは、インターフェイス コンフィギュレーション モードでも VLAN コンフィギュレーション モードでも設定できます。

スタティック MAC アドレスを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config-)# mac-address-table static mac_address vlan vlan-id {drop | interface {type slot/port} | port-channel number} [auto-learn]`	MAC アドレス テーブルに追加するスタティック アドレスを指定します。 **auto-learn** オプションをイネーブルにすると、同じ MAC アドレスが別のポート上で見つかった場合には、スイッチがエントリを更新します。

次に、MAC アドレス テーブルにスタティック エントリを登録する例を示します。

```
switch# configure terminal
switch(config)# mac-address-table static 12ab.47dd.ff89 vlan 3 interface ethernet 2/1
```

スタティック MAC アドレスを削除する手順は、次のとおりです。

コマンド	目的
`switch(config-if)# no mac-address-table static mac_address vlan vlan-id`	MAC アドレス テーブルからスタティック エントリを削除するには、**no** 形式のコマンドを入力します。

mac-address-table static コマンドでは、スタティック MAC アドレスを仮想インターフェイスに割り当てることができます。

MAC テーブルのエージング タイムの設定

エントリ（パケット送信元の MAC アドレスとそのパケットが入ってきたポート）が MAC テーブル内に留まる時間を設定できます。

（注）　MAC 経過時間は、インターフェイス コンフィギュレーション モードでも VLAN コンフィギュレーション モードでも設定できます。

すべての MAC アドレスの経過時間を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# mac-address-table aging-time seconds [vlan vlan_id]`	エントリが無効になって、MAC アドレス テーブルから破棄されるまでの時間を指定します。指定できる範囲は 0 ～ 1000000 秒です。デフォルトは 300 秒です。0 を入力すると、MAC エージングがディセーブルになります。VLAN を指定しなかった場合、エージングの指定がすべての VLAN に適用されます。

次に、MAC アドレス テーブル内エントリのエージング タイムを 600 秒（10 分）に設定する例を示します。

```
switch# configure terminal
switch(config)# mac-address-table aging-time 600
```

MAC テーブルからのダイナミック アドレスの消去

MAC アドレス テーブルからすべてのダイナミック エントリを消去できます。

MAC アドレス テーブルを消去する手順は、次のとおりです。

コマンド	目的
`switch(config)# clear mac-address-table dynamic {address mac_addr} {interface [type slot/port | port-channel number]} {vlan vlan_id}`	MAC アドレス テーブルからダイナミック アドレス エントリを消去します。

次に、MAC アドレス テーブル内のダイナミック エントリを消去する例を示します。

```
switch# clear mac-address-table dynamic
```

MAC アドレス設定の確認

MAC アドレス設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
switch# **show mac-address-table aging-time**	スイッチ内で定義されているすべての VLAN の MAC アドレス エージング時間を表示します。
switch# **show mac-address-table**	MAC アドレス テーブルの内容を表示します。

次に、MAC アドレス テーブルを表示する例を示します。

```
switch# show mac-address-table
VLAN      MAC Address       Type    Age       Port
---------+-----------------+-------+---------+-----------------------------
1         0018.b967.3cd0    dynamic 10        Eth1/3
1         001c.b05a.5380    dynamic 200       Eth1/3
Total MAC Addresses: 2
```

次に、現在のエージング タイムを表示する例を示します。

```
switch# show mac-address-table aging-time
Vlan  Aging Time
----- ----------
1     300
13    300
42    300
```

CHAPTER 14

IGMP スヌーピングの設定

インターネット グループ管理プロトコル（IGMP）スヌーピングを使用すると、VLAN のマルチキャスト トラフィックの処理が簡素化されます。対象ホストからの IGMP メンバーシップ レポート メッセージを確認（スヌーピング）して、マルチキャスト トラフィックの範囲を当該ホストが接続されている各 VLAN インターフェイスの一部だけに限定します。

この章は、次の項で構成されています。

- IGMP スヌーピングの情報（14-1 ページ）
- IGMP スヌーピング パラメータの設定（14-4 ページ）
- IGMP スヌーピングの設定確認（14-7 ページ）

IGMP スヌーピングの情報

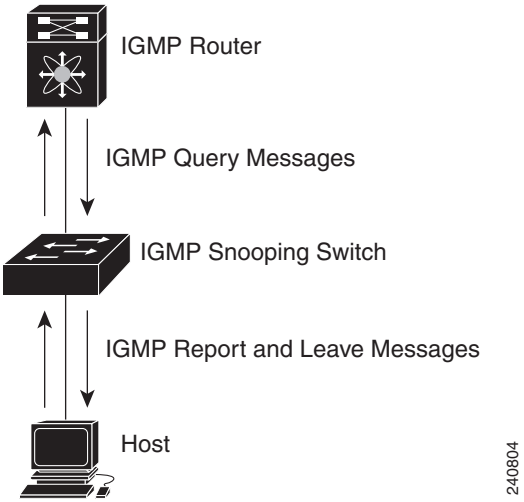
IGMP スヌーピング ソフトウェアは、VLAN 内の IGMP プロトコル メッセージを調べて、このトラフィックの受信に関連のあるホストまたはその他のデバイスに接続されているのはどのインターフェイスかを検出します。IGMP スヌーピングは、インターフェイス情報を使用して、マルチアクセス LAN 環境での帯域幅消費を減らすことができ、これによって VLAN 全体のフラッディングを防ぎます。IGMP スヌーピング機能は、どのポートがマルチキャスト対応ルータに接続されているかを追跡して、IGMP メンバーシップ レポートの転送管理を支援します。トポロジの変更通知には、IGMP スヌーピング ソフトウェアが応答します。

（注） IGMP スヌーピングは、すべてのイーサネット インターフェイスでサポートされます。*スヌーピング*という用語が使用されるのは、レイヤ 3 コントロール プレーン パケットが代行受信され、レイヤ 2 の転送決定に影響を与えるためです。

Cisco NX-OS は、IGMPv2 と IGMPv3 をサポートします。IGMPv2 は IGMPv1 をサポートし、IGMPv3 は IGMPv2 をサポートします。以前のバージョンの IGMP のすべての機能がサポートされるわけではありませんが、メンバーシップ クエリーとメンバーシップ レポートに関連した機能はすべての IGMP バージョンについてサポートされます。

図 14-1 に、ホストと IGMP ルータの間に置かれた IGMP スヌーピング スイッチを示します。IGMP スヌーピング スイッチは、IGMP メンバーシップ レポートと脱退メッセージをスヌーピングし、それらを必要な場合にだけ、接続されている IGMP ルータに転送します。

図 14-1　IGMP スヌーピング スイッチ



（注）　スイッチは、宛先マルチキャスト MAC アドレスのみに基づいて IGMPv3 スヌーピングをサポートしています。送信元 MAC アドレスやプロキシ レポートに基づいてスヌーピングをサポートすることはありません。

Cisco NX-OS IGMP スヌーピング ソフトウェアは、最適化されたマルチキャスト フラッディング（OMF）をサポートします。これは、不明トラフィックをルータだけに転送し、データ駆動の状態生成は一切実行しません。IGMP スヌーピングの詳細については、RFC 4541 を参照してください。

この項では、次のトピックについて取り上げます。

- IGMPv1 および IGMPv2（14-2 ページ）
- IGMPv3（14-3 ページ）
- IGMP スヌーピング クエリア（14-3 ページ）
- IGMP フォワーディング（14-3 ページ）

IGMPv1 および IGMPv2

IGMPv1 と IGMPv2 は両方とも、メンバーシップ レポート抑制をサポートします。つまり、同一サブネット上の 2 つのホストが同一グループのマルチキャスト データを受信する場合、他方のホストからメンバレポートを受信するホストは、そのレポートを送信しません。メンバーシップ レポート抑制は、同じポートを共有しているホスト間で発生します。

各 VLAN スイッチ ポートに接続されているホストが 1 つしかない場合は、IGMPv2 の高速脱退機能を設定できます。高速脱退機能を使用すると、最終メンバのクエリー メッセージがホストに送信されません。ソフトウェアは IGMP Leave メッセージを受信すると、ただちに該当するポートへのマルチキャスト データ転送を停止します。

IGMPv1 では、明示的な IGMP Leave メッセージが存在しないため、特定のグループについてマルチキャスト データを要求するホストが存続しないことを示すために、メンバーシップ メッセージ タイムアウトが利用されます。

（注）　高速脱退機能をイネーブルにすると、残っているホストのチェックを行わないため、Cisco NX-OS は、最後のメンバ クエリーの間隔の設定を無視します。

IGMPv3

スイッチ上の IGMPv3 スヌーピングの実装は、アップストリーム マルチキャスト ルータが送信元に基づいたフィルタリングを行えるように、IGMPv3 レポートを転送します。

ソフトウェアのデフォルト設定では、各 VLAN ポートに接続されたホストが追跡されます。この明示的なトラッキング機能は、高速脱退メカニズムをサポートしています。すべての IGMPv3 ホストがメンバーシップ レポートを送信するため、レポート抑制機能によって、スイッチが他のマルチキャスト対応ルータに送信するトラフィックの量が制限されます。レポート抑制をイネーブルにすると、過去にいずれの IGMPv1 ホストまたは IGMPv2 ホストからも対象のグループへの要求がなかった場合には、プロキシ レポートが作成されます。プロキシ機能は、ダウンストリーム ホストからのメンバーシップ レポートからグループの状態を構築し、アップストリーム クエリアからのクエリーに応答してメンバーシップ レポートを生成します。

IGMPv3 メンバーシップ レポートには LAN セグメント上のグループ メンバの一覧が含まれていますが、最終ホストが脱退すると、メンバーシップ クエリーが送信されます。最終メンバのクエリー インターバルについてパラメータを設定すると、タイムアウトまでにどのホストからも応答がなかった場合に、グループ ステートが解除されます。

IGMP スヌーピング クエリア

クエリーを発生させる VLAN 内にマルチキャスト ルータが存在しない場合、IGMP スヌーピング クエリアを設定して、メンバーシップ クエリーを送信させる必要があります。

IGMP スヌーピング クエリアがイネーブルな場合は、定期的に IGMP クエリーが送信されるため、IP マルチキャスト トラフィックを要求するホストから IGMP レポート メッセージが発信されます。IGMP スヌーピングはこれらの IGMP レポートを待ち受けて、適切な転送を確立します。

IGMP フォワーディング

Cisco Nexus 5000 シリーズ スイッチのコントロール プレーンは、IP アドレスを検出できますが、フォワーディングは MAC アドレスだけを使用して行われます。

スイッチに接続されているホストは、IP マルチキャスト グループに参加する場合に、参加する IP マルチキャスト グループを指定して、要求されていない IGMP 参加メッセージを送信します。それとは別に、スイッチは、接続されているルータから一般クエリーを受信したら、そのクエリーを、物理インターフェイスか仮想インターフェイスかにかかわらず、VLAN 内のすべてのインターフェイスに転送します。マルチキャスト グループに参加するホストは、スイッチに参加メッセージを送信することにより応答します。スイッチの CPU が、そのグループ用のマルチキャスト転送テーブル エントリを作成します（まだ存在しなかった場合）。また、CPU は、参加メッセージを受信したインターフェイスを、転送テーブルのエントリに追加します。そのインターフェイスと対応付けられたホストが、そのマルチキャスト グループ用のマルチキャスト トラフィックを受信します。

ルータは定期的にマルチキャスト一般クエリーを送信し、スイッチはそれらのクエリーを VLAN 内のすべてのポート経由で転送します。関心のあるホストがクエリーに応答します。VLAN 内の少なくとも 1 つのホストがマルチキャスト トラフィックを受信するようなら、ルータは、その VLAN へのマルチキャスト トラフィックの転送を続行します。スイッチは、そのマルチキャスト グループの転送テーブルにリストされているホストだけにマルチキャスト グループ トラフィックを転送します。

ホストがマルチキャスト グループから脱退するときには、ホストは、通知なしで脱退することもできれば、脱退メッセージを送信することもできます。スイッチは、ホストから脱退メッセージを受信したら、グループ固有のクエリーを送信して、そのインターフェイスに接続されているその他のデバイスの中に、そのマルチキャスト グループのトラフィックを受信するものがあるかどうかを調べます。スイッチはさらに、転送テーブルでその MAC グループの情報を更新し、そのグループのマルチキャスト トラフィックの受信に関心のあるホストだけが、転送テーブルに指定されるようにします。ルータが VLAN からレポートを受信しなかった場合、その VLAN 用のグループは IGMP キャッシュから削除されます。

IGMP スヌーピング パラメータの設定

IGMP スヌーピング プロセスの動作を管理するには、表 14-1 で説明する、省略可能な IGMP スヌーピング パラメータを設定します。

表 14-1　IGMP スヌーピング パラメータ

パラメータ	説明
IGMP スヌーピング	VLAN ごとに IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。 **（注）** グローバルな設定がディセーブルになっている場合は、すべての VLAN が、イネーブルかどうかに関係なくディセーブルと見なされます。
明示的な追跡	各ポートに接続されたそれぞれのホストから送信される IGMPv3 メンバーシップ レポートを、VLAN 別に追跡します。デフォルトではイネーブルになっています。
高速脱退	ソフトウェアが IGMP Leave レポートを受信した場合に、IGMP クエリー メッセージを送信することなく、グループ ステートを解除できるようにします。このパラメータは、IGMPv2 ホストに関して、各 VLAN ポート上のホストが 1 つしか存在しない場合に使用されます。デフォルトではディセーブルになっています。
最終メンバのクエリー インターバル	IGMP クエリーの送信後に待機する時間を設定します。この時間が経過すると、ソフトウェアは、特定のマルチキャスト グループについてネットワーク セグメント上に受信要求を行うホストが存在しないと見なします。いずれのホストからも応答がないまま、最終メンバのクエリー インターバルの期限が切れると、対応する VLAN ポートからグループが削除されます。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。
スヌーピング クエリア	クエリーを生成するマルチキャスト ルータが VLAN 内に存在しない場合に、インターフェイスのスヌーピング クエリアを設定します。デフォルトではディセーブルになっています。
レポート抑制	マルチキャスト対応ルータに送信されるメンバシップ レポート トラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトではイネーブルになっています。

表 14-1　IGMP スヌーピング パラメータ（続き）

パラメータ	説明
マルチキャスト ルータ	マルチキャスト ルータへのスタティック接続を設定します。ルータと接続するインターフェイスが、選択した VLAN に含まれている必要があります。
スタティック グループ	VLAN に属するインターフェイスを、マルチキャスト グループのスタティック メンバとして設定します。

IGMP スヌーピングを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# ip igmp snooping`	IGMP スヌーピングをグローバルにイネーブルにします。デフォルトではイネーブルになっています。 **（注）** グローバルな設定がディセーブルになっている場合は、すべての VLAN が、イネーブルかどうかに関係なくディセーブルと見なされます。
ステップ 3	`switch(config)# vlan vlan-id`	VLAN コンフィギュレーション モードを開始します。
ステップ 4	`switch(config-vlan)# ip igmp snooping`	現在の VLAN に対して IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。 **（注）** IGMP スヌーピングがグローバルにイネーブルになっている場合は、このコマンドは必要ありません。
	`switch(config-vlan)# ip igmp snooping explicit-tracking`	各ポートに接続されたそれぞれのホストから送信される IGMPv3 メンバーシップ レポートを、VLAN 別に追跡します。デフォルトは、すべての VLAN でイネーブルです。
	`switch(config-vlan)# ip igmp snooping fast-leave`	IGMPv2 プロトコルのホスト レポート抑制メカニズムのために、明示的に追跡できない IGMPv2 ホストをサポートします。高速脱退がイネーブルの場合、IGMP ソフトウェアは、各 VLAN ポートに接続されたホストが 1 つだけであると見なします。デフォルトは、すべての VLAN でディセーブルです。
	`switch(config-vlan)# ip igmp snooping last-member-query-interval seconds`	いずれのホストからも IGMP クエリー メッセージへの応答がないまま、最終メンバのクエリー インターバルの期限が切れた場合に、対応する VLAN ポートからグループを削除します。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。

コマンド	目的
switch(config-vlan)# **ip igmp snooping querier** *IP-address*	マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、スヌーピング クエリアを設定します。IP アドレスは、メッセージの送信元として使用します。デフォルトではディセーブルになっています。
switch(config-vlan)# **ip igmp snooping report-suppression**	マルチキャスト対応ルータに送信されるメンバシップ レポート トラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトではイネーブルになっています。
switch(config-vlan)# **ip igmp snooping mrouter interface** *interface*	マルチキャスト ルータへのスタティック接続を設定します。ルータと接続するインターフェイスが、選択した VLAN に含まれている必要があります。インターフェイスは、タイプと番号で指定できます。
switch(config-vlan)# **ip igmp snooping static-group** *group-ip-addr* [**source** *source*-ip-addr] **interface** *interface*	VLAN に属するインターフェイスを、マルチキャスト グループのスタティック メンバとして設定します。インターフェイスは、タイプと番号で指定できます。

次に、VLAN 5 の IGMP スヌーピング パラメータを設定する例を示します。

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# ip igmp snooping last-member-query-interval 3
switch(config-vlan)# ip igmp snooping querier 172.20.52.106
switch(config-vlan)# ip igmp snooping explicit-tracking
switch(config-vlan)# ip igmp snooping fast-leave
switch(config-vlan)# ip igmp snooping report-suppression
switch(config-vlan)# ip igmp snooping mrouter interface ethernet 1/10
switch(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface ethernet 1/10
switch(config-vlan)# end
switch#
```

IGMP スヌーピングは、グローバルにも、特定の VLAN に対してだけでもディセーブルにできます。IGMP スヌーピングをグローバルにディセーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **no ip igmp snooping**	IGMP スヌーピングをグローバルにディセーブル化します。デフォルトではイネーブルになっています。 **（注）** グローバルな設定がディセーブルになっている場合は、すべての VLAN が、イネーブルかどうかに関係なくディセーブルと見なされます。

	コマンド	目的
ステップ 3	switch(config)# **vlan** *vlan-id*	VLAN コンフィギュレーション モードを開始します。
ステップ 4	switch(config-vlan)# **no ip igmp snooping**	現在の VLAN に対して IGMP スヌーピングをディセーブル化します。デフォルトではイネーブルになっています。

次に、VLAN 5 だけの IGMP をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# no ip igmp snooping
```

IGMP スヌーピングの設定確認

IGMP スヌーピングの設定を確認するには、次のいずれかの作業を行います。

コマンド	説明
switch# **show ip igmp snooping** [[**vlan**] *vlan-id*]	VLAN ごとの IGMP スヌーピング設定。
switch# **show ip igmp snooping groups** [[**vlan**] *vlan-id*] [**detail**]	VLAN ごとのグループに関する IGMP スヌーピング情報。
switch# **show ip igmp snooping querier** [[**vlan**] *vlan-id*]	VLAN ごとの IGMP スヌーピング クエリア。
switch# **show ip igmp snooping mrouter** [[**vlan**] *vlan-id*]	VLAN ごとのマルチキャスト ルータ ポート。
switch# **show ip igmp snooping explicit-tracking vlan** *vlan-id*	VLAN ごとの IGMP スヌーピングの明示的な追跡情報。

次に、IGMP スヌーピング パラメータを確認する例を示します。

```
switch# show ip igmp snooping
Global IGMP Snooping Information:
  IGMP Snooping enabled

IGMP Snooping information for vlan 1
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  Explicit tracking enabled
  Fast leave disabled
  Report suppression enabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
IGMP Snooping information for vlan 5
IGMP snooping enabled
  IGMP querier present, address: 172.16.24.1, version: 3
  Querier interval: 125 secs
  Querier last member query interval: 10 secs
```

```
Querier robustness: 2
Switch-querier enabled, address 172.16.24.1, currently running
Explicit tracking enabled
Fast leave enabled
Report suppression enabled
Router port detection using PIM Hellos, IGMP Queries
Number of router-ports: 1
Number of groups: 1
```

CHAPTER 15

トラフィック ストーム制御の設定

この章では、Cisco Nexus 5000 シリーズ スイッチ上で、トラフィック ストーム制御を設定する方法について説明します。

この章は、次の項で構成されています。

- トラフィック ストーム制御の概要（15-1 ページ）
- 注意事項および制約事項（15-3 ページ）
- トラフィック ストーム制御の設定（15-3 ページ）
- トラフィック ストーム制御の設定（15-3 ページ）
- トラフィック ストーム制御カウンタの表示（15-4 ページ）
- トラフィック ストーム制御の設定例（15-4 ページ）
- デフォルト設定（15-5 ページ）

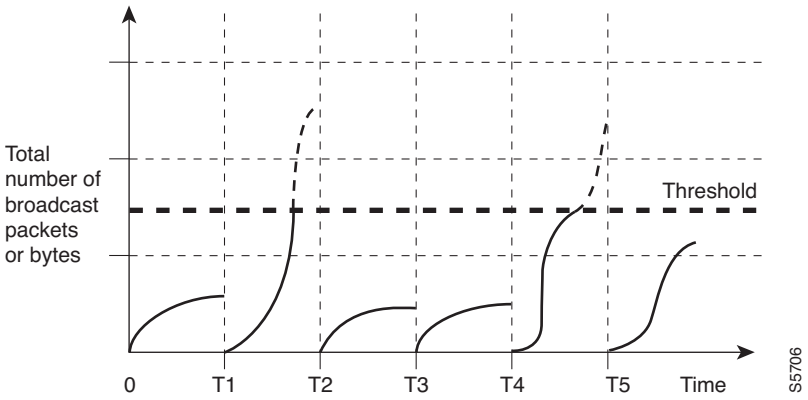
トラフィック ストーム制御の概要

トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御機能を使用すると、物理インターフェイス上におけるブロードキャスト、マルチキャスト、または未知のユニキャスト トラフィック ストームによって、レイヤ 2 ポート経由の通信が妨害されるのを防ぐことができます。

トラフィック ストーム制御（トラフィック抑制ともいう）では、ブロードキャスト、マルチキャスト、ユニキャストの着信トラフィックのレベルを 10 ミリ秒間隔で監視します。この間、トラフィック レベル（ポートの使用可能合計帯域幅に対するパーセンテージ）が、設定したトラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。

図 15-1 に、指定したタイム インターバル期間中におけるレイヤ 2 インターフェイス上でのブロードキャスト トラフィック パターンを示します。この例では、トラフィック ストーム制御が T1 と T2 時間の間、および T4 と T5 時間の間で発生します。これらの間隔中に、ブロードキャスト トラフィックの量が設定済みのしきい値を超過したためです。

図 15-1　　ブロードキャスト抑制



トラフィック ストーム制御のしきい値とタイム インターバルを使用することで、トラフィック ストーム制御アルゴリズムは、さまざまなレベルのパケット粒度で機能します。たとえば、しきい値が高いほど、より多くのパケットを通過させることができます。

Cisco Nexus 5000 シリーズ スイッチのトラフィック ストーム制御は、ハードウェアで実装されています。トラフィック ストーム制御は、レイヤ 2 インターフェイスからスイッチンブ バスに渡されるパケットを巡回モニタします。また、パケットの宛先アドレスに設定されている Individual/Group ビットを使用して、パケットがユニキャストかブロードキャストかを判断し、10 マイクロ秒以内の間隔で現在のパケット数を追跡します。パケット数がしきい値に到達したら、後続のパケットをすべて破棄します。

トラフィック ストーム制御では、トラフィック量の計測に帯域幅方式を使用します。制御対象のトラフィックが使用できる、利用可能な合計帯域幅に対するパーセンテージを設定します。パケットは一定の間隔で到着するわけではないので、10 マイクロ秒の間隔によって、トラフィック ストーム制御の動作が影響を受けることがあります。

次に、トラフィック ストーム制御の動作がどのような影響を受けるかを示します。

- ブロードキャスト トラフィック ストーム制御をイネーブルにした場合、ブロードキャスト トラフィックが 10 マイクロ秒のインターバル以内にしきい値レベルを超えると、トラフィック ストーム制御により、そのインターバルが終了するまですべてのブロードキャスト トラフィックがドロップされます。
- マルチキャスト トラフィック ストーム制御をイネーブルにした場合、マルチキャスト トラフィックが 10 マイクロ秒のインターバル以内にしきい値レベルを超えると、トラフィック ストーム制御により、そのインターバルが終了するまですべてのマルチキャスト トラフィックがドロップされます。
- ブロードキャストおよびマルチキャスト トラフィック ストーム制御をイネーブルにした場合、ブロードキャスト トラフィックが 10 マイクロ秒のインターバル以内にしきい値レベルを超えると、トラフィック ストーム制御により、そのインターバルが終了するまですべてのブロードキャスト トラフィックがドロップされます。
- ブロードキャストおよびマルチキャスト トラフィック ストーム制御をイネーブルにした場合、マルチキャスト トラフィックが 10 マイクロ秒のインターバル以内にしきい値レベルを超えると、トラフィック ストーム制御により、そのインターバルが終了するまですべてのマルチキャスト トラフィックがドロップされます。

デフォルトでは、Cisco NX-OS は、トラフィックが設定済みレベルを超えても是正のための処理を行いません。

注意事項および制約事項

トラフィック ストーム制御レベルを設定する場合は、次の注意事項と制限事項に留意してください。

- ポート チャネル インターフェイス上にトラフィック ストーム制御を設定できます。
- レベルをインターフェイスの帯域幅全体に対する割合として指定します。
  - レベルの指定範囲は 0 ～ 100 です。
  - 任意で、レベルの小数部を 0 ～ 99 の範囲で指定できます。
  - 100% は、トラフィック ストーム制御がないことを意味します。
  - 0.0% は、すべてのトラフィックを抑制します。

ハードウェアの制限およびサイズの異なるパケットがカウントされる方式のため、レベルの割合は概数になります。着信トラフィックを構成するフレームのサイズに応じて、実際に適用されるパーセンテージ レベルと設定したパーセンテージ レベルの間には、数パーセントの誤差がある可能性があります。

トラフィック ストーム制御の設定

制御対象のトラフィックが使用できる、利用可能な合計帯域幅に対するパーセンテージを設定できます。

（注） トラフィック ストーム制御では 10 マイクロ秒のインターバルを使用しており、このインターバルがトラフィック ストーム制御の動作に影響を及ぼす可能性があります。

トラフィック ストーム制御を特定のインターフェイスでイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 1	`switch(config)# interface {ethernet slot/port | port-channel number}`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	`switch(config-if)# storm-control {broadcast | multicast | unicast} level percentage[.fraction]`	インターフェイスを通過するトラフィックのトラフィック ストーム制御を設定します。デフォルトのステートはディセーブルです。

次に、ユニキャスト トラフィック ストーム制御を Ethernet 1/4 に設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# storm-control unicast level 40
```

トラフィック ストーム制御の設定の確認

トラフィック ストーム制御の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
switch# **show interface** [**ethernet** *slot/port* | **port-channel** *number*] **counters storm-control**	特定のインターフェイスについて、トラフィック ストーム制御の設定を表示します。
switch# **show running-config interface**	トラフィック ストーム制御の設定を表示します。

トラフィック ストーム制御カウンタの表示

Cisco Nexus 5000 シリーズ スイッチが保持している、トラフィック ストーム制御アクティビティに関するカウンタを表示できます。

（注） トラフィック ストーム制御では 10 マイクロ秒のインターバルを使用しており、このインターバルがトラフィック ストーム制御の動作に影響を及ぼす可能性があります。

トラフィック ストーム制御カウンタを特定のインターフェイスで表示する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **show interface** [**ethernet** *slot/port* | **port-channel** *number*] **counters storm-control**	トラフィック ストーム制御カウンタを表示します。

トラフィック ストーム制御の設定例

次に、トラフィック ストーム制御の設定例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# storm-control broadcast level 40
switch(config-if)# storm-control multicast level 40
switch(config-if)# storm-control unicast level 40
```

デフォルト設定

表 15-1に、トラフィック ストーム制御パラメータのデフォルト設定値を示します。

表 15-1　デフォルトのトラフィック ストーム制御パラメータ

パラメータ	デフォルト
トラフィック ストーム制御	ディセーブル
しきい値パーセンテージ	100

CHAPTER 16

AAA の設定

この章では、Cisco Nexus 5000 シリーズ スイッチに認証、許可、アカウンティング（AAA）を設定する方法を説明します。

この章は、次の項で構成されています。

- AAA について（16-1 ページ）
- リモート AAA の前提条件（16-6 ページ）
- AAA の注意事項および制約事項（16-6 ページ）
- AAA の設定（16-6 ページ）
- ローカル AAA アカウンティング ログの表示と消去（16-13 ページ）
- AAA の設定の確認（16-13 ページ）
- AAA の設定例（16-13 ページ）
- デフォルト設定（16-14 ページ）

AAA について

この項では、次のトピックについて取り上げます。

- AAA セキュリティ サービス（16-1 ページ）
- AAA を使用する利点（16-2 ページ）
- リモート AAA サービス（16-3 ページ）
- AAA サーバ グループ（16-3 ページ）
- AAA サービス設定オプション（16-3 ページ）
- ユーザ ログインのための認証および許可プロセス（16-4 ページ）

AAA セキュリティ サービス

AAA 機能は、Nexus 5000 シリーズ スイッチを管理するユーザの ID を確認し、アクセスを許可し、実行されたアクションを追跡します。Nexus 5000 シリーズ スイッチでは、Remote Access Dial-In User Service（RADIUS）プロトコルまたは Terminal Access Controller Access Control device Plus（TACACS+）プロトコルをサポートしています。

Nexus 5000 シリーズ スイッチは提示されたユーザ ID およびパスワードの組み合わせに基づき、ローカル データベースによるローカル認証またはローカル許可、あるいは AAA サーバによるリモート認証またはリモート許可を実行します。Nexus 5000 スイッチと AAA サーバ間の通信は、事前共有秘密キーによって保護されます。すべての AAA サーバ用または特定の AAA サーバ専用に共通秘密キーを設定できます。

AAA セキュリティは、次のサービスを実行します。

- 認証:ユーザを識別します。選択したセキュリティ プロトコルに応じて、ログインとパスワードのダイアログ、チャレンジ/レスポンス、メッセージング サポート、暗号化などが行われます。

  認証は、Nexus 5000 シリーズ スイッチにアクセスするユーザまたはデバイスの ID を確認するプロセスです。このプロセスは、Nexus 5000 スイッチにアクセスしようとするエンティティが入力したユーザ ID とパスワードの組み合わせに基づいて行われます。Nexus 5000 シリーズ スイッチでは、ローカル認証(ローカル ルックアップ データベースを使用)またはリモート認証(1 台または複数台の RADIUS サーバまたは TACACS+ サーバを使用)を実行できます。

- 許可:アクセス コントロールを実行します。

  AAA の許可は、ユーザが何を実行する権限を与えられるかを表す一連の属性を組み立てるプロセスです。Nexus 5000 シリーズ スイッチの許可機能は、AAA サーバからダウンロードされた属性によって提供されます。RADIUS や TACACS+ などのリモート セキュリティ サーバは、適切なユーザで該当する権利を定義した属性値(AV)のペアをアソシエートすることによって、ユーザに特定の権限を付与します。

- アカウンティング:課金、監査、レポートのための情報収集、ローカルでの情報のロギング、および AAA サーバへの情報の送信の方式を提供します。

  アカウンティング機能は、Nexus 5000 シリーズ スイッチへのアクセスに使用されるすべての管理セッションのログを追跡し、管理します。この情報を使用して、トラブルシューティングや監査のためのレポートを生成できます。アカウンティング ログは、ローカルに保存することもできれば、リモート AAA サーバに送信することもできます。

  アカウンティング ログ機能では、show コマンドは記録されません。たとえば、**show version** や **show module** コマンドは記録されません。

(注) Cisco NX-OS ソフトウェアは、認証、許可、アカウンティングをそれぞれ個別にサポートします。たとえば、アカウンティングは設定せずに、認証と許可を設定したりできます。

AAA を使用する利点

AAA は、次のような利点を提供します。

- アクセス設定の柔軟性と制御性の向上
- 拡張性
- 標準化された認証方式(RADIUS、TACACS+ など)
- 複数のバックアップ デバイス

リモート AAA サービス

RADIUS プロトコルおよび TACACS+ プロトコルを介して提供されるリモート AAA サービスには、ローカル AAA サービスと比べて次のような利点があります。

- ファブリック内の各 Nexus 5000 シリーズ スイッチのユーザ パスワード リストを簡単に管理できます。
- AAA サーバはすでに企業内に幅広く導入されており、簡単に AAA サービスに使用できます。
- ファブリック内のすべてのスイッチのアカウンティング ログを集中管理できます。
- スイッチ上のローカル データベースではなく、ファブリック内の各スイッチのユーザ属性を使用するため、管理が容易です。

AAA サーバ グループ

認証、許可、アカウンティングのためのリモート AAA サーバは、サーバ グループを使用して指定できます。サーバ グループとは、同じ AAA プロトコルを実装した一連のリモート AAA サーバです。サーバ グループの目的は、リモート AAA サーバが応答できなくなったときにフェールオーバー サーバを提供することです。グループ内の最初のリモート サーバが応答しなかった場合、いずれかのサーバが応答を送信するまで、グループ内の次のリモート サーバで試行が行われます。サーバ グループ内のすべての AAA サーバが応答しなかった場合、そのサーバ グループ オプションは障害が発生しているものと見なされます。必要に応じて、複数のサーバ グループを指定できます。最初のグループ内のサーバからエラーを受信すると、次のサーバ グループのサーバが試されます。

AAA サービス設定オプション

Nexus 5000 シリーズ スイッチでは、次の各サービスに、異なる AAA 設定を作成できます。

- User Telnet または Secure Shell（SSH）ログイン認証
- コンソール ログイン認証
- ユーザ管理セッション アカウンティング

表 16-1 に、各 AAA サービス設定オプションの CLI コマンドを示します。

表 16-1　AAA サービス コンフィギュレーション コマンド

AAA サービス コンフィギュレーション オプション	関連コマンド
Telnet または SSH ログイン	**aaa authentication login default**
コンソール ログイン	**aaa authentication login console**
ユーザ セッション アカウンティング	**aaa accounting default**

AAA サービスには、次の認証方式を指定できます。

- RADIUS サーバ グループ：RADIUS サーバのグローバル プールを認証に使用します。
- 特定のサーバ グループ：指定した RADIUS または TACACS+ サーバ グループを認証に使用します。

- ローカル:ユーザ名またはパスワードのローカル データベースを認証に使用します。
- なし(none):ユーザ名だけ使用します。

(注) 特定のサーバ グループではなく、すべての RADIUS サーバを使用する認証方式では、Nexus 5000 シリーズ スイッチは、設定済み RADIUS サーバのグローバル プールから設定順に RADIUS サーバを選択します。このグローバル プールのサーバは、Nexus 5000 シリーズ スイッチ上の RADIUS サーバ グループ内で選択的に設定可能なサーバです。

表 16-2 に、AAA サービス用に設定できる AAA 認証方式を示します。

表 16-2　AAA サービスのための AAA 認証方式

AAA サービス	AAA の方式
コンソール ログイン認証	サーバ グループ、ローカル、なし
ユーザ ログイン認証	サーバ グループ、ローカル、なし
ユーザ管理セッション アカウンティング	サーバ グループ、ローカル

(注) コンソール ログイン認証、ユーザ ログイン認証、ユーザ管理セッション アカウンティングの場合、Nexus 5000 シリーズ スイッチは、指定された順に各オプションを実行します。他の設定済みのオプションが失敗した場合は、「ローカル」がデフォルトの認証方式になります。

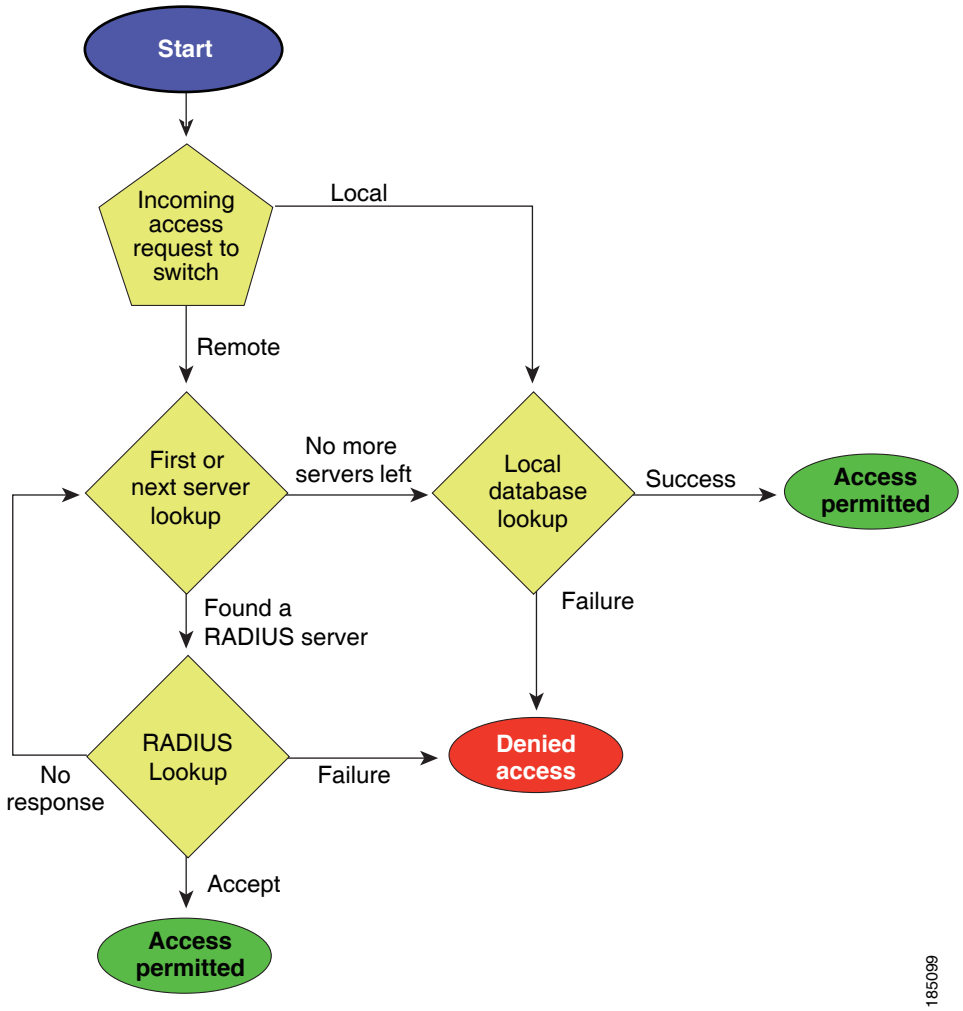
ユーザ ログインのための認証および許可プロセス

図 16-1 に、ユーザ ログインのための認証および許可プロセスのフローチャートを示します。次のプロセスが発生します。

1. 目的の Nexus 5000 シリーズ スイッチにログインするには、Telnet、SSH、Fabric Manager/Device Manager、またはコンソール ログインのいずれかを使用します。
2. サーバ グループ認証方式を使用する AAA サーバ グループを設定した場合、そのグループの最初の AAA サーバに認証要求が送信されます。
   a. その AAA サーバが応答しなかった場合、リモートのいずれかの AAA サーバが認証要求に応答するまで、試行が継続されます。
   b. そのサーバ グループ内のすべての AAA サーバが応答しなかった場合、次のサーバ グループ内のサーバで試行します。
   c. 設定されているすべての方式で応答が得られなかった場合、ローカル データベースが認証に使用されます。
3. Nexus 5000 シリーズ スイッチではリモートの AAA サーバによるユーザの認証に成功すると、次のいずれかの処理が行われます。
   a. AAA サーバ プロトコルが RADIUS の場合、cisco-av-pair 属性で指定されているユーザ ロールが認証応答とともにダウンロードされます。
   b. AAA サーバ プロトコルが TACACS+ の場合、シェルのカスタム属性として指定されているユーザ ロールを取得するために、もう 1 つの要求が同じサーバに送信されます。

4. ユーザ名とパスワードのローカル認証に成功すると、スイッチへのログインが認められ、ローカル データベースに設定されたロールが割り当てられます。

図 16-1　ユーザ ログインでの認証と許可のフロー



（注）「残りのサーバ グループなし」とは、すべてのサーバ グループのいずれのサーバからも応答がないということです。
「残りのサーバなし」とは、現在のサーバ グループ内のいずれのサーバからも応答がないということです。

リモート AAA の前提条件

リモート AAA サーバには、次の前提条件があります。

- 最低 1 つの RADIUS または TACACS+ サーバが IP で到達可能であること（「RADIUS サーバ ホストの設定」セクション（17-5 ページ）および「TACACS+ サーバ ホストの設定」セクション（18-6 ページ）を参照）。
- Nexus 5000 シリーズ スイッチが、AAA サーバのクライアントとして設定されていること。
- Nexus 5000 シリーズ スイッチおよびリモート AAA サーバ上に事前共有秘密キーが設定されていること。
- リモート サーバが Nexus 5000 シリーズ スイッチからの AAA 要求に応答すること（「RADIUS サーバまたはグループの手動でのモニタリング」セクション（17-14 ページ）および「TACACS+ サーバまたはグループの手動でのモニタリング」セクション（18-13 ページ）を参照）。

AAA の注意事項および制約事項

Nexus 5000 シリーズ スイッチは、TACACS+ または RADIUS で作成されたものであれ、あるいはローカルに作成されたものであれ、数字だけを使用したユーザ名をサポートしていません。また、数字だけを使用したローカル ユーザ名を作成することもありません。AAA サーバに数字だけのユーザ名が存在し、ログイン時にその名前を入力した場合、ユーザはログインを許可されます。

AAA の設定

AAA 認証とアカウンティングを設定する手順は、次のとおりです。

ステップ 1　リモートの RADIUS または TACACS+ サーバを使用して認証を行う場合は、Nexus 5000 シリーズ スイッチ上にホストを設定します。第 17 章「RADIUS の設定」および第 18 章「TACACS+ の設定」を参照してください。

ステップ 2　コンソール ログイン認証方式を設定します。「コンソール ログイン認証方式の設定」セクション（16-7 ページ）を参照してください。

ステップ 3　ユーザ ログインのためのデフォルトのログイン認証方式を設定します。「デフォルトのログイン認証方式の設定」セクション（16-8 ページ）を参照してください。

ステップ 4　デフォルト AAA アカウンティングのデフォルト方式を設定します。「AAA アカウンティングのデフォルト方式の設定」セクション（16-10 ページ）を参照してください。

次のトピックで、AAA の設定手順について詳しく説明します。

- コンソール ログイン認証方式の設定（16-7 ページ）
- デフォルトのログイン認証方式の設定（16-8 ページ）
- ログイン認証失敗メッセージのイネーブル化（16-9 ページ）
- MSCHAP 認証のイネーブル化（16-9 ページ）
- AAA アカウンティングのデフォルト方式の設定（16-10 ページ）
- Nexus 5000 シリーズ スイッチでの AAA サーバ VSA の使用（16-11 ページ）

（注）　Cisco IOS CLI に慣れている場合、この機能に対応する Nexus 5000 シリーズのコマンドは、通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

コンソール ログイン認証方式の設定

ここでは、コンソール ログインの認証方式を設定する方法を説明します。

認証方式には、次のものがあります。

- RADIUS サーバのグローバル プール
- RADIUS サーバまたは TACACS+ サーバの名前付きサブセット
- Nexus 5000 シリーズ スイッチ上のローカル データベース
- ユーザ名だけ（**none**）

デフォルトの方式は、ローカルです。

（注）　事前に設定されている一連の RADIUL サーバには、**aaa authentication** コマンドの **group radius** 形式および **group** *server-name* 形式を使用します。ホスト サーバを設定するには、**radius server-host** コマンドを使用します。サーバの名前付きグループを作成するには、**aaa group server radius** コマンドを使用します。

必要に応じて、コンソール ログイン認証方式を設定する前に RADIUS または TACACS+ サーバグループを設定します。コンソール ログイン認証方式を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# aaa authentication login console {group group-list [none]| local | none}`	コンソールのログイン認証方式を設定します。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • **radius**：RADIUS サーバのグローバル プールが認証に使用されます。 • *named-group*：TACACS+ サーバまたは RADIUS サーバの名前付きサブセットが認証に使用されます。 **local** 方式では、ローカル データベースが認証に使用されます。**none** 方式では、ユーザ名だけが使用されます。 デフォルトのコンソール ログイン方式は **local** です。この方式は、方式が一切設定されていない場合、および設定済みのどの方式でも応答が得られなかった場合に使用されます。
ステップ 3	`switch(config)# exit`	設定モードを終了します。

	コマンド	目的
ステップ 4	switch# **show aaa authentication**	(任意)コンソール ログイン認証方式の設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、コンソール ログインの認証方式を設定する例を示します。

```
switch# configure terminal
switch(config)# aaa authentication login console group radius
switch(config)# exit
switch# show aaa authentication
switch# copy running-config startup-config
```

デフォルトのログイン認証方式の設定

認証方式には、次のものがあります。

- RADIUS サーバのグローバル プール
- RADIUS サーバまたは TACACS+ サーバの名前付きサブセット
- Nexus 5000 シリーズ スイッチ上のローカル データベース
- ユーザ名だけ

デフォルトの方式は、ローカルです。

必要に応じて、デフォルトのログイン認証方式を設定する前に RADIUS または TACACS+ サーバ グループを設定します。デフォルトのログイン認証方式を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **aaa authentication login default** {**group** *group-list* [**none**]| **local** | **none**}	デフォルト認証方式を設定します。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • **radius**:RADIUS サーバのグローバル プールが認証に使用されます。 • *named-group*:TACACS+ サーバまたは RADIUS サーバの名前付きサブセットが認証に使用されます。 **local** 方式では、ローカル データベースが認証に使用されます。**none** 方式では、ユーザ名だけが使用されます。 デフォルトのログイン方式は **local** です。この方式は、方式が一切設定されていない場合、および設定済みのどの方式でも応答が得られなかった場合に使用されます。
ステップ 3	switch(config)# **exit**	設定モードを終了します。

	コマンド	目的
ステップ 4	switch# **show aaa authentication**	(任意)デフォルトのログイン認証方式の設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

ログイン認証失敗メッセージのイネーブル化

ユーザがログインして、リモート AAA サーバが応答しなかった場合は、ローカル ユーザ データベースによってログインが処理されます。ログイン失敗メッセージの表示をイネーブルにしておくと、次のメッセージが表示されます。

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

ログイン認証失敗メッセージをイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **aaa authentication login error-enable**	ログイン認証失敗メッセージをイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show aaa authentication**	(任意)ログイン失敗メッセージの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

MSCHAP 認証のイネーブル化

マイクロソフト チャレンジ ハンドシェーク認証プロトコル(MSCHAP)は、マイクロソフト版の CHAP です。リモート認証サーバ(RADIUS または TACACS+)を介して Nexus 5000 シリーズ スイッチにユーザ ログインするとき、MSCHAP を使用できます。

デフォルトでは、Nexus 5000 シリーズ スイッチは、スイッチとリモート サーバ間の認証に、パスワード認証プロトコル(PAP)を使用します。MSCHAP がイネーブルの場合は、MSCHAP ベンダー固有属性(Vendor-Specific Attribute)を認識するように RADIUS サーバを設定する必要があります。「Nexus 5000 シリーズ スイッチでの AAA サーバ VSA の使用」セクション(16-11 ページ)を参照してください。表 16-3 に、MSCHAP で必要とされる RADIUS VSA を示します。

表 16-3　MSCHAP RADIUS VSA

ベンダー ID 番号	ベンダー タイプ番号	VSA	説明
311	11	MSCHAP-Challenge	AAA サーバから MSCHAP ユーザに送信されるチャレンジを保持します。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。
211	11	MSCHAP-Response	チャレンジに対する応答として MSCHAP ユーザが入力した値を保持します。Access-Request パケットでしか使用されません。

MSCHAP 認証をイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# aaa authentication login mschap enable`	MS-CHAP 認証をイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	`switch(config)# exit`	設定モードを終了します。
ステップ 4	`switch# show aaa authentication login mschap`	(任意)MS-CHAP の設定を表示します。
ステップ 5	`switch# copy running-config startup-config`	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

AAA アカウンティングのデフォルト方式の設定

Nexus 5000 シリーズ スイッチは、TACACS+ および RADIUS によるアカウンティング方式をサポートしています。スイッチは、ユーザ アクティビティをアカウンティング レコードの形で TACACS+ セキュリティ サーバまたは RADIUS セキュリティ サーバに報告します。各アカウンティング レコードに、アカウンティング属性値(AV)のペアが入っており、それが AAA サーバに格納されます。

AAA アカウンティングをアクティブ化すると、これらの属性がアカウンティング レコードとしてレポートされ、セキュリティ サーバ上のアカウンティング ログに格納されます。

特定のアカウンティング方式を定義するデフォルト方式のリストを作成できます。それには次の方式があります。

- RADIUS サーバ グループ:RADIUS サーバのグローバル プールをアカウンティングに使用します。
- 特定のサーバ グループ:指定した RADIUS または TACACS+ サーバ グループをアカウンティングに使用します。
- ローカル:ユーザ名またはパスワードのローカル データベースをアカウンティングに使用します。

（注）　サーバ グループを設定しており、そのサーバ グループが応答しなかった場合は、デフォルトで、ローカル データベースが認証に使用されます。

必要に応じて、AAA アカウンティングのデフォルト方式を設定する前に RADIUS または TACACS+ サーバ グループを設定します。

AAA アカウンティングのデフォルト方式を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# aaa accounting default {group group-list | local}`	デフォルト アカウンティング方式を設定します。スペースで区切ったリストで、1 つまたは複数のサーバ グループ名を指定できます。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • **radius**：RADIUS サーバのグローバル プールがアカウンティングに使用されます。 • *named-group*：TACACS+ サーバまたは RADIUS サーバの名前付きサブセットがアカウンティングに使用されます。 **local** 方式では、アカウンティングにローカル データベースが使用されます。 デフォルトのアカウンティング方式は **local** です。サーバ グループが設定されていないとき、または設定済みのすべてのサーバ グループから応答がないときに、このデフォルトの方式が使用されます。
ステップ 3	`switch(config)# exit`	設定モードを終了します。
ステップ 4	`switch# show aaa accounting`	（任意）AAA アカウンティングのデフォルト方式の設定を表示します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

Nexus 5000 シリーズ スイッチでの AAA サーバ VSA の使用

VSA を使用して、Nexus 5000 シリーズのユーザ ロールと SNMPv3 パラメータを AAA サーバ上に指定できます。

この項では、次のトピックについて取り上げます。

- VSA について（16-12 ページ）
- VSA の形式（16-12 ページ）
- AAA サーバ上での Nexus 5000 シリーズ スイッチのユーザ ロールと SMNPv3 パラメータの指定（16-12 ページ）

VSA について

インターネット技術特別調査委員会（IETF）が、ネットワーク アクセス サーバと RADIUS サーバの間での VSA の通信のための方式を規定する標準を作成しています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、一般的な用途には適さない独自の拡張属性をサポートできます。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダー タイプは 1（名前付き cisco-av-pair）です。値は次の形式のストリングです。

```
protocol : attribute seperator value *
```

プロトコルは、特定のタイプの許可用のシスコ属性です。必須属性の区切り文字は等号（=）で、アスタリスク（*）は任意属性を示します。

Nexus 5000 シリーズ スイッチで認証に RADIUS サーバを使用する場合、RADIUS プロトコルは RADIUS サーバに対し、認証結果とともに許可情報などのユーザ属性を戻すように指示します。この許可情報は、VSA で指定されます。

VSA の形式

Nexus 5000 シリーズ スイッチでは、次の VSA プロトコル オプションがサポートされています。

- Shell：ユーザ プロファイル情報を提供する access-accept パケットで使用されます。
- Accounting：accounting-request パケットで使用されます。値にスペースが含まれている場合は、二重引用符で囲んでください。

Nexus 5000 シリーズ スイッチでは、次の属性がサポートされています。

- roles：ユーザに割り当てるすべてのロールをリストします。値フィールドは、グループ名を空白で区切ったリストの入ったストリングです。
- accountinginfo：標準の RADIUS アカウンティング プロトコルで処理される属性に加えて、追加のアカウンティング情報が格納されます。この属性が送信されるのは、スイッチ上の RADIUS クライアントからの Account-Request フレームの VSA 部分内だけです。この属性は、アカウンティング プロトコル関連の PDU でしか使用できません。

AAA サーバ上での Nexus 5000 シリーズ スイッチのユーザ ロールと SMNPv3 パラメータの指定

AAA サーバ上で VSA cisco-av-pair を使用して、Nexus 5000 シリーズ スイッチのユーザ ロールマッピングを指定できます。次の形式を使用します。

```
shell:roles="roleA roleB …"
```

cisco-av-pair 属性にロール オプションを指定しなかった場合のデフォルトのユーザ ロールは、network-operator です。

次のように SNMPv3 認証とプライバシー プロトコル属性を指定することもできます。

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

SNMPv3 認証プロトコルに指定できるオプションは、SHA と MD5 です。プライバシー プロトコルに指定できるオプションは、AES-128 と DES です。cisco-av-pair 属性にこれらのオプションを指定しなかった場合のデフォルトの認証プロトコルは、MD5 と DES です。

ユーザ ロールの詳細については、第 22 章「ユーザ アカウントと RBAC の設定」を参照してください。

ローカル AAA アカウンティング ログの表示と消去

Nexus 5000 シリーズ スイッチでは、AAA アカウンティング アクティビティのローカル ログを管理しています。このログを表示したり、消去したりする手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **show accounting log** [*size*] [**start-time** *year month day hh*:*mm*:*ss*]	アカウンティング ログを表示します。このコマンド出力には、デフォルトで最大 250,000 バイトのアカウンティング ログが表示されます。サイズ引数を指定すれば、コマンドの出力を制限できます。指定できる範囲は 0 ～ 250000 バイトです。ログ出力の開始時刻を指定することもできます。
ステップ 2	switch# **clear accounting log**	(任意)アカウンティング ログの内容を消去します。

（注）　アカウンティング ログ機能では、show コマンドは記録されません。たとえば、**show version** や **show module** コマンドは記録されません。

AAA の設定の確認

AAA の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show aaa accounting	AAA アカウンティングの設定を表示します。
show aaa authentication [login {error-enable | mschap}]	AAA 認証情報を表示します。
show aaa groups	AAA サーバ グループの設定を表示します。
show running-config aaa [all]	実行コンフィギュレーションの AAA 設定を表示します。
show startup-config aaa	スタートアップ コンフィギュレーションの AAA 設定を表示します。

AAA の設定例

次に、AAA を設定する例を示します。

```
aaa authentication login default group radius
aaa authentication login console group radius
aaa accounting default group radius
```

デフォルト設定

表 16-4 に、AAA パラメータのデフォルト設定を示します。

表 16-4　デフォルトの AAA パラメータ

パラメータ	デフォルト
コンソール認証方式	local
デフォルト認証方式	local
ログイン認証失敗メッセージ	Disabled
MSCHAP 認証	Disabled
デフォルト アカウンティング方式	local
アカウンティング ログの表示サイズ	250 KB

CHAPTER 17

RADIUS の設定

この章では、Nexus 5000 シリーズ スイッチ上で、Remote Access Dial-In User Service（RADIUS）プロトコルを設定する方法について説明します。

この章は、次の項で構成されています。

- RADIUS について（17-1 ページ）
- RADIUS の前提条件（17-4 ページ）
- 注意事項および制約事項（17-4 ページ）
- RADIUS サーバの設定（17-4 ページ）
- RADIUS サーバの統計情報の表示（17-14 ページ）
- RADIUS の設定例（17-15 ページ）
- デフォルト設定（17-15 ページ）

RADIUS について

RADIUS 分散クライアント/ サーバ システムを使用すると、不正アクセスからネットワークを保護できます。シスコの実装では、RADIUS クライアントは Nexus 5000 シリーズ スイッチで稼働し、すべてのユーザ認証情報およびネットワーク サービス アクセス情報が格納された中央の RADIUS サーバに認証要求およびアカウンティング要求を送信します。

この項では、次のトピックについて取り上げます。

- RADIUS ネットワーク環境（17-1 ページ）
- RADIUS の動作（17-2 ページ）
- ベンダー固有属性（17-3 ページ）

RADIUS ネットワーク環境

RADIUS は、高度なセキュリティを必要とし、同時にリモート ユーザのネットワーク アクセスを維持する必要があるさまざまなネットワーク環境に実装できます。

RADIUS は、アクセス セキュリティを必要とする次のネットワーク環境で使用します。

- RADIUS をサポートしている複数ベンダーのネットワーク デバイスを使用したネットワーク

  たとえば、複数ベンダーのネットワーク デバイスで、単一の RADIUS サーバ ベースのセキュリティ データベースを使用できます。

- すでに RADIUS を使用中のネットワーク。

  RADIUS を使用した Nexus 5000 シリーズ スイッチをネットワークに追加できます。この作業は、AAA サーバに移行するときの最初の手順になります。

- リソース アカウンティングが必要なネットワーク。

  RADIUS アカウンティングは、RADIUS 認証または RADIUS 認可とは個別に使用できます。RADIUS アカウンティング機能を使用すると、サービスの開始および終了時に、セッション中に使用したリソース（時間、パケット、バイトなど）の量を示すデータを送信できます。インターネット サービス プロバイダー（ISP）は、RADIUS アクセス コントロールおよびアカウンティング用ソフトウェアのフリーウェア版を使用して、特殊なセキュリティおよび課金ニーズに対応しています。

- 認証プロファイルをサポートするネットワーク

  ネットワークで RADIUS サーバを使用すると、AAA 認証を設定し、ユーザごとのプロファイルをセットアップできます。ユーザごとのプロファイルにより、Nexus 5000 シリーズ スイッチは、既存の RADIUS ソリューションを使用してポートを容易に管理できると同時に、共有リソースを効率的に管理してさまざまなサービス レベル アグリーメントを提供できます。

RADIUS の動作

ユーザがログインを試行し、RADIUS を使用して Nexus 5000 シリーズ スイッチに対する認証を行う際には、次のプロセスが実行されます。

1. ユーザが、ユーザ名とパスワードの入力を求められ、入力します。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由で RADIUS サーバに送信されます。
3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
   - ACCEPT：ユーザが認証されたことを表します。
   - REJECT：ユーザは認証されず、ユーザ名とパスワードの再入力を求められるか、アクセスを拒否されます。
   - CHALLENGE：RADIUS サーバによってチャレンジが発行されます。チャレンジは、ユーザから追加データを収集します。
   - CHANGE PASSWORD：RADIUS サーバからユーザに対して新しいパスワードの選択を求める要求が発行されます。

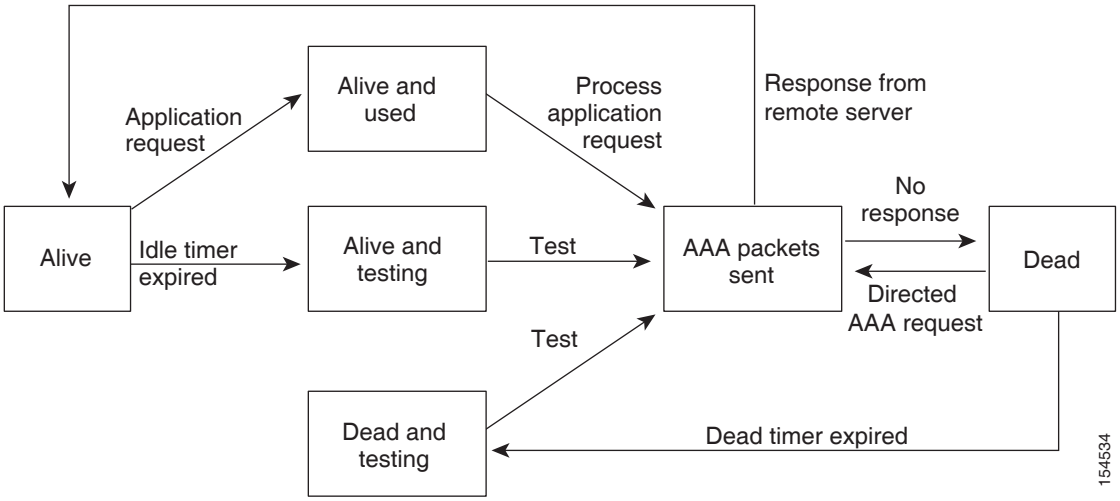
ACCEPT 応答または REJECT 応答には、EXEC 許可またはネットワーク許可に使用される追加データが含まれています。RADIUS 認可を使用するには、まず RADIUS 認証を完了する必要があります。ACCEPT または REJECT パケットに含まれる追加データの内容は次のとおりです。

- ユーザがアクセス可能なサービス（Telnet、rlogin、またはローカルエリア トランスポート（LAT）接続、ポイントツーポイント プロトコル（PPP）、シリアル ライン インターネット プロトコル（SLIP）、EXEC サービスなど）
- 接続パラメータ（ホストまたはクライアントの IPv4 または IPv6 アドレス、アクセス リスト、ユーザ タイムアウト）

RADIUS サーバのモニタリング

応答を返さない RADIUS サーバがあると、AAA 要求の処理に遅延が発生する可能性があります。AAA 要求の処理時間を節約するため、定期的に RADIUS サーバを監視し、RADIUS サーバが応答を返す（アライブ）かどうかチェックするように、Nexus 5000 シリーズ スイッチを設定できます。Nexus 5000 シリーズ スイッチは、応答を返さない RADIUS サーバをデッド（dead）としてマークし、デッド RADIUS サーバには AAA 要求を送信しません。また、定期的にデッド RADIUS サーバをモニタリングし、それらが応答を返したらアライブ状態に戻します。このモニタリング プロセスでは、実際の AAA 要求が送信される前に、RADIUS サーバが稼働状態であることを確認します。RADIUS サーバの状態がデッドまたはアライブに変わると、簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、スイッチによって、障害が発生したことを知らせるエラー メッセージが表示されます。図 17-1を参照してください。

図 17-1　RADIUS サーバの状態



（注） アライブ サーバとデッド サーバのモニタリング間隔は異なります。これらはユーザが設定できます。RADIUS サーバ モニタリングを実行するには、テスト認証要求を RADIUS サーバに送信します。

ベンダー固有属性

Internet Engineering Task Force（IETF）ドラフト標準には、ネットワーク アクセス サーバと RADIUS サーバ間でのベンダー固有属性（VSA）の通信方式が規定されています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、一般的な用途には適さない独自の拡張属性をサポートできます。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダー タイプは 1（名前付き cisco-av-pair）です。値は次の形式のストリングです。

```
protocol : attribute separator value *
```

プロトコルは、特定のタイプの許可用のシスコ属性です。必須属性の区切り文字は等号（=）で、アスタリスク（*）は任意属性を示します。

Nexus 5000 シリーズ スイッチで認証に RADIUS サーバを使用する場合、RADIUS プロトコルは RADIUS サーバに対し、認証結果とともに許可情報などのユーザ属性を戻すように指示します。この許可情報は、VSA で指定されます。

Nexus 5000 シリーズ スイッチでは、次の VSA プロトコル オプションがサポートされています。

- Shell：ユーザ プロファイル情報を提供する access-accept パケットで使用されます。
- Accounting：accounting-request パケットで使用されます。値にスペースが含まれている場合は、二重引用符で囲む必要があります。

Nexus 5000 シリーズ スイッチでは、次の属性がサポートされています。

- roles：ユーザが属するすべてのロールの一覧です。値フィールドは、スペースで区切られたロール名を一覧表示したストリングです。
- accountinginfo：標準の RADIUS アカウンティング プロトコルで処理される属性に加えて、アカウンティング情報が格納されます。この属性は、スイッチ上の RADIUS クライアントからの Account-Request フレームの VSA 部分だけに送信されます。この属性と共に使用できるのは、アカウンティングの Protocol Data Unit（PDU; プロトコル データ ユニット）だけです。

RADIUS の前提条件

RADIUS には、次の前提条件があります。

- RADIUS サーバの IP アドレス（IPv4 または IPv6）またはホスト名を取得していること。
- RADIUS サーバから事前共有キーを取得していること。
- Nexus 5000 シリーズ スイッチが、AAA サーバの RADIUS クライアントとして設定されていること。

注意事項および制約事項

RADIUS に関する注意事項と制約事項は次のとおりです。

- Nexus 5000 シリーズ スイッチ上に設定できる RADIUS サーバの数は最大 64 個です。

RADIUS サーバの設定

RADIUS サーバを設定するには、次の作業を行います。

ステップ 1　Nexus 5000 シリーズ スイッチと RADIUS サーバとの接続を確立します。

「RADIUS サーバ ホストの設定」セクション（17-5 ページ）を参照してください。

ステップ 2　RADIUS サーバの事前共有秘密キーを設定します。

「グローバルな事前共有キーの設定」セクション（17-6 ページ）を参照してください。

ステップ 3　必要に応じて、AAA 認証方式用に、RADIUS サーバのサブセットを使用して RADIUS サーバ グループを設定します。

「ログイン時にユーザによる RADIUS サーバの指定を許可」セクション（17-9 ページ）および「AAA の設定」セクション（16-6 ページ）を参照してください。

ステップ 4　必要に応じて、次のオプションのパラメータを設定します。

- デッドタイム間隔

  「次に、RADIUS サーバの定期的なモニタリングを設定する例を示します。」セクション（17-13 ページ）を参照してください。

- ログイン時に RADIUS サーバの指定を許可

  「ログイン時にユーザによる RADIUS サーバの指定を許可」セクション（17-9 ページ）を参照してください。

- 送信リトライ回数とタイムアウト間隔

  「グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定」セクション（17-9 ページ）を参照してください。

- アカウンティングおよび認証属性

  「RADIUS サーバのアカウンティングおよび認証属性の設定」セクション（17-11 ページ）を参照してください。

ステップ 5　必要に応じて、定期的に RADIUS サーバをモニタリングするよう設定します。
「RADIUS サーバの定期的モニタリングの設定」セクション（17-12 ページ）を参照してください。

次のトピックで、RADIUS の設定手順について詳しく説明します。

- RADIUS サーバ ホストの設定（17-5 ページ）
- グローバルな事前共有キーの設定（17-6 ページ）
- RADIUS サーバの事前共有キーの設定（17-7 ページ）
- RADIUS サーバ グループの設定（17-8 ページ）
- ログイン時にユーザによる RADIUS サーバの指定を許可（17-9 ページ）
- グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定（17-9 ページ）
- サーバに対する RADIUS 送信リトライ回数とタイムアウト間隔の設定（17-10 ページ）
- RADIUS サーバのアカウンティングおよび認証属性の設定（17-11 ページ）
- RADIUS サーバの定期的モニタリングの設定（17-12 ページ）
- デッド タイム間隔の設定（17-13 ページ）
- RADIUS サーバまたはグループの手動でのモニタリング（17-14 ページ）

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

RADIUS サーバ ホストの設定

認証に使用する各 RADIUS サーバについて、IP アドレス（IPv4 または IPv6）、あるいはホスト名を設定する必要があります。すべての RADIUS サーバ ホストは、デフォルトの RADIUS サーバ グループに追加されます。最大 64 の RADIUS サーバを設定できます。

RADIUS サーバ ホストを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config) #radius-server host {ipv4-address | ipv6-address | host-name}`	RADIUS サーバの IPv4 または IPv6 アドレス、またはホスト名を指定します。
ステップ 3	`switch(config)# exit`	設定モードを終了します。
ステップ 4	`switch# show radius-server`	(任意)RADIUS サーバの設定を表示します。
ステップ 5	`switch# copy running-config startup-config`	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、RADIUS サーバ ホストを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

グローバルな事前共有キーの設定

Nexus 5000 シリーズ スイッチで使用するすべてのサーバでは、グローバル レベルで事前共有キーを設定できます。事前共有キーとは、Nexus 5000 シリーズ スイッチと RADIUS サーバ ホスト間の共有秘密テキスト ストリングです。

グローバルな事前共有キーを設定するには、リモートの RADIUS サーバの事前共有キー値を取得した上で、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# radius-server key [0 | 7] key-value`	すべての RADIUS サーバで使用する事前共有キーを指定します。クリア テキスト形式(**0**)または暗号化形式(**7**)の事前共有キーを指定できます。デフォルトの形式はクリア テキストです。最大で 63 文字です。 デフォルトでは、事前共有キーは設定されません。

	コマンド	目的
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show radius-server**	(任意)RADIUS サーバの設定を表示します。 **(注)** 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、リモートの RADIUS サーバから事前共有キーの値を取得する例を示します。

```
switch# configure terminal
switch(config)# radius-server key 0 QsEfThUkO
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

RADIUS サーバの事前共有キーの設定

RADIUS サーバの事前共有キーを設定できます。事前共有キーとは、Nexus 5000 シリーズ スイッチと RADIUS サーバ ホスト間の共有秘密テキスト ストリングです。

RADIUS サーバの事前共有キーを設定するには、リモートの RADIUS サーバの事前共有キー値を取得した上で、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **7**] *key-value*	特定の RADIUS サーバの事前共有キーを指定します。クリア テキスト形式(**0**)または暗号化形式(**7**)の事前共有キーを指定できます。デフォルトの形式はクリア テキストです。最大で 63 文字です。 この事前共有キーがグローバル事前共有キーの代わりに使用されます。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show radius-server**	(任意)RADIUS サーバの設定を表示します。 **(注)** 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、RADIUS サーバの事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

RADIUS サーバ グループの設定

サーバ グループを使用して、1 台または複数台のリモート AAA サーバによる認証を指定できます。グループのメンバーはすべて、RADIUS プロトコルに属している必要があります。設定した順序に従ってサーバが試行されます。

これらのサーバ グループはいつでも設定できますが、設定したグループを有効にするには、AAA サービスに適用する必要があります。AAA サービスについては、「リモート AAA サービス」セクション（16-3 ページ）を参照してください。

RADIUS サーバ グループを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# aaa group server radius` *group-name*	RADIUS サーバ グループを作成し、そのグループの RADIUS サーバ グループ コンフィギュレーション サブモードを開始します。*group-name* 引数は、最大 127 文字の長さの英数字のストリングで、大文字小文字が区別されます。
ステップ 3	`switch(config-radius)# server` {*ipv4-address* | *ipv6-address* | *server-name*}	RADIUS サーバを、RADIUS サーバ グループのメンバーとして設定します。 **ヒント**　指定した RADIUS サーバが見つからない場合は、**radius-server host** コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	`switch(config-radius)# deadtime` *minutes*	（任意）モニタリング デッド タイムを設定します。デフォルト値は 0 分です。指定できる範囲は 1 ～ 1440 です。 **（注）**　RADIUS サーバ グループのデッド タイム間隔が 0 より大きい場合は、この値がグローバルなデッド タイム値より優先されます。RADIUS サーバの定期的なモニタリングを設定する例を参照してください。
ステップ 5	`switch(config-radius)# exit`	設定モードを終了します。
ステップ 6	`switch(config) #show radius-server group [GROUP-NAME]`	（任意）RADIUS サーバ グループの設定を表示します。
ステップ 7	`switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、RADIUS サーバ グループを設定する例を示します。

```
switch# configure terminal
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 10.10.1.1
switch(config-radius)# deadtime 30
switch(config-radius)# use-vrf management
switch(config-radius)# exit
switch(config)# show radius-server group
switch(config)# copy running-config startup-config
```

ログイン時にユーザによる RADIUS サーバの指定を許可

（注）デフォルトでは、Nexus 5000 シリーズ スイッチは、デフォルトの AAA 認証方式に基づいて認証要求をフォワーディングします。ユーザが VRF と RADIUS サーバを指定して認証要求を送信できるように Nexus 5000 シリーズ スイッチを設定するには、directed-request オプションをイネーブルにします。このオプションをイネーブルにすると、ユーザは *username@hostname* としてログインできます。ここで、*hostname* は設定済みの RADIUS サーバの名前です。ユーザ指定のログインは、Telnet セッションでのみサポートされます。

ユーザがログイン時に RADIUS サーバを指定できるようにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# switch(config)# radius-server directed-request`	ログイン時にユーザが認証要求の送信先となる RADIUS サーバを指定できるようにします。デフォルトでは無効になっています。
ステップ 3	`switch(config)# exit`	設定モードを終了します。
ステップ 4	`switch# show radius-server directed-request`	(任意)指定された要求設定を表示します。
ステップ 5	`switch# copy running-config startup-config`	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定

すべての RADIUS サーバに対するグローバルな再送信リトライ回数とタイムアウト間隔を設定できます。デフォルトでは、スイッチはローカル認証に戻す前に、RADIUS サーバへの送信を 1 回だけ再試行します。このリトライの回数は、サーバごとに最大 5 回まで増やすことができます。タイムアウト間隔は、スイッチがタイムアウト エラーを宣言する前に、RADIUS サーバからの応答を待機する時間を決定します。

グローバルな RADIUS 送信リトライ回数とタイムアウト間隔を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **radius-server retransmit** *count*	すべての RADIUS サーバの再送信回数を指定します。デフォルトの再送信回数は 1 で、範囲は 0 ～ 5 です。
ステップ 3	switch(config)# **radius-server timeout** *seconds*	RADIUS サーバの送信タイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒で、範囲は 1 ～ 60 秒です。
ステップ 4	switch(config)# **exit**	設定モードを終了します。
ステップ 5	switch# **show radius-server**	(任意)RADIUS サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

サーバに対する RADIUS 送信リトライ回数とタイムアウト間隔の設定

デフォルトでは、Nexus 5000 シリーズ スイッチはローカル認証に戻す前に、RADIUS サーバへの送信を 1 回だけ再試行します。このリトライの回数は、サーバごとに最大 5 回まで増やすことができます。Nexus 5000 シリーズ スイッチが、タイムアウト エラーを宣言する前に、RADIUS サーバからの応答を待機するタイムアウト間隔も設定できます。

サーバに対する RADIUS 送信リトライ回数とタイムアウト間隔を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	#switch(config)# **radius-server host** {*ipv4-address* |*ipv6-address* | *host-name*} **retransmit** *count*	特定のサーバに対する再送信回数を指定します。デフォルトはグローバル値です。 **(注)** 特定の RADIUS サーバ用の再送信回数は、ステップ 2 で指定したすべての RADIUS サーバ用の(グローバルな)再送信回数を上書きします。
ステップ 3	switch(config)# switch(config)# **radius-server host** {*ipv4-address* |*ipv6-address* | *host-name*} **timeout** *seconds*	特定のサーバの送信タイムアウト間隔を指定します。デフォルトはグローバル値です。 **(注)** 特定の RADIUS サーバ用のタイムアウト間隔値は、ステップ 3 で指定したすべての RADIUS サーバ用の(グローバルな)タイムアウト間隔値を上書きします。
ステップ 4	switch(config)# **exit**	設定モードを終了します。

	コマンド	目的
ステップ 5	switch# **show radius-server**	(任意)RADIUS サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、サーバに対する RADIUS 送信リトライ回数とタイムアウト間隔を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host server1 retransmit 3
switch(config)# radius-server host server1 timeout 10
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

RADIUS サーバのアカウンティングおよび認証属性の設定

RADIUS サーバをアカウンティング専用、または認証専用に使用するかを指定できます。デフォルトでは、RADIUS サーバはアカウンティングと認証の両方に使用されます。RADIUS のアカウンティングおよび認証メッセージの宛先 UDP ポート番号も指定できます。

RADIUS サーバのアカウンティング属性と認証属性を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config) #**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **acct-port** *udp-port*	(任意)RADIUS アカウンティング メッセージ用の UDP ポートを指定します。デフォルトの UDP ポートは 1812 です。範囲は 0 ～ 65535 です。
ステップ 3	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **accounting**	(任意)特定の RADIUS サーバをアカウンティング用にのみ使用することを指定します。デフォルトでは、アカウンティングと認証の両方に使用されます。
ステップ 4	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **auth-port** *udp-port*	(任意)RADIUS 認証メッセージ用の UDP ポートを指定します。デフォルトの UDP ポートは 1812 です。範囲は 0 ～ 65535 です。
ステップ 5	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **authentication**	(任意)特定の RADIUS サーバを認証用にのみ使用することを指定します。デフォルトでは、アカウンティングと認証の両方に使用されます。
ステップ 6	switch(config)# **exit**	設定モードを終了します。
ステップ 7	switch(config)# **show radius-server**	(任意)RADIUS サーバの設定を表示します。
ステップ 8	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、RADIUS サーバのアカウンティング属性と認証属性を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 acct-port 2004
switch(config)# radius-server host 10.10.1.1 accounting
switch(config)# radius-server host 10.10.2.2 auth-port 2005
switch(config)# radius-server host 10.10.2.2 authentication
switch(config)# exit
switch(config)# show radius-server
switch# copy running-config startup-config
```

RADIUS サーバの定期的モニタリングの設定

RADIUS サーバの可用性をモニタリングできます。パラメータとして、サーバに使用するユーザ名とパスワード、およびアイドル タイマーがあります。アイドル タイマーには、RADIUS サーバが要求を受信しなくなってから、Nexus 5000 シリーズ スイッチがテスト パケットを送信するまでの間隔を指定します。このオプションを設定することで、サーバを定期的にテストできます。

（注） セキュリティ上の理由から、RADIUS データベース内の既存のユーザ名と同じテスト ユーザ名を設定しないことを推奨します。

テスト アイドル タイマーには、RADIUS サーバが要求を受信しなくなってから、Nexus 5000 シリーズ スイッチがテスト パケットを送信するまでの間隔を指定します。

（注） デフォルトのアイドル タイマー値は 0 分です。アイドル タイム間隔が 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません

RADIUS サーバの定期的なモニタリングを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# radius-server host {ipv4-address | ipv6-address | host-name} test {idle-time minutes | password password [idle-time minutes] | username name [password password [idle-time minutes]]}`	サーバ モニタリング用のパラメータを指定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。デフォルトのアイドル タイマー値は 0 分です。指定できる範囲は 0 ～ 1440 分です。 **（注）** RADIUS サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	`switch(config)# radius-server deadtime minutes`	Nexus 5000 シリーズ スイッチが、前回応答しなかった RADIUS サーバをチェックするまでの時間（分）を指定します。デフォルト値は 0 分です。有効な範囲は 1 ～ 1440 分です。
ステップ 4	`switch(config)# exit`	設定モードを終了します。
ステップ 5	`switch# show radius-server`	（任意）RADIUS サーバの設定を表示します。
ステップ 6	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、RADIUS サーバの定期的なモニタリングを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH
idle-time 3
switch(config)# radius-server deadtime 5
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

デッド タイム間隔の設定

すべての RADIUS サーバのデッド タイム間隔を設定できます。デッド タイム間隔には、Nexus 5000 シリーズ スイッチが RADIUS サーバをデッドとして宣言したあと、そのサーバがアライブ状態に戻ったかどうかを判断するためにテスト パケットを送信するまでの間隔を指定します。デフォルト値は 0 分です。

（注）　デッド タイム間隔が 0 分の場合、RADIUS サーバは、応答を返さない場合でも、デットとしてマークされません。RADIUS サーバ グループのデッドタイム間隔を設定することができます（「RADIUS サーバ グループの設定」セクション（17-8 ページ）を参照）。

デッド タイム間隔を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`#switch(config)# radius-server deadtime`	デッド タイム間隔を設定します。デフォルト値は 0 分です。有効な範囲は 1 ～ 1440 分です。
ステップ 3	`switch(config)# exit`	設定モードを終了します。
ステップ 4	`switch# show radius-server`	（任意）RADIUS サーバの設定を表示します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

RADIUS サーバまたはグループの手動でのモニタリング

RADIUS サーバまたはサーバ グループにテスト メッセージを手動で送信する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **test aaa server radius** {*ipv4-address* | *ipv6-address* | *server-name*} [**vrf** *vrf-name*] *username password*	RADIUS サーバにテスト メッセージを送信して可用性を確認します。
ステップ 1	switch# **test aaa group** *group-name username password*	RADIUS サーバ グループにテスト メッセージを送信して可用性を確認します。

次に、RADIUS サーバに手動でテスト メッセージを送信する例を示します。

```
switch# test aaa server radius 10.10.1.1 user1 Ur2Gd2BH
switch# test aaa group RadGroup user2 As3He3CI
```

RADIUS の設定の確認

RADIUS の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config radius [**all**]	実行コンフィギュレーションの RADIUS 設定を表示します。
show startup-config radius	スタートアップ コンフィギュレーションの RADIUS 設定を表示します。
show radius-server [*server-name* | *ipv4-address* | *ipv6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	設定済みのすべての RADIUS サーバのパラメータを表示します。

このコマンドの出力に表示される各フィールドの詳細については、『*Cisco Nexus 5000 シリーズ Command Reference*』を参照してください。

RADIUS サーバの統計情報の表示

Cisco Nexus 5000 シリーズ スイッチが RADIUS サーバのアクティビティについて保持している統計情報を表示するには、次の作業を行います。

	コマンド	目的
ステップ 1	switch# switch# **show radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}	RADIUS 統計情報を表示します。

次に、統計情報を表示する例を示します。

```
switch# show radius-server statistics 10.10.1.1
```

RADIUS の設定例

次に、RADIUS を設定する例を示します。

```
radius-server key 7 "ToIkLhPpG"
radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
aaa group server radius RadServer
    server 10.10.1.1
use-vrf management
```

デフォルト設定

表 17-1 に、RADIUS パラメータのデフォルト設定を示します。

表 17-1　デフォルトの RADIUS パラメータ

パラメータ	デフォルト
サーバの役割	認証とアカウンティング
デッド タイマー間隔	0 分
再送信回数	1
再送信タイマー間隔	5 秒
アイドル タイマー間隔	0 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	test

CHAPTER 18

TACACS+ の設定

この章では、Nexus 5000 シリーズ スイッチ上で、Terminal Access Controller Access Control System Plus（TACACS+）プロトコルを設定する方法について説明します。

この章は、次の項で構成されています。

- TACACS+ について（18-1 ページ）
- TACACS+ の前提条件（18-4 ページ）
- 注意事項および制約事項（18-4 ページ）
- TACACS+ の設定（18-4 ページ）
- TACACS+ 統計情報の表示（18-14 ページ）
- TACACS+ の設定の確認（18-15 ページ）
- TACACS+ の設定例（18-15 ページ）
- デフォルト設定（18-15 ページ）

TACACS+ について

TACACS+ セキュリティ プロトコルを使用すると、Nexus 5000 シリーズ スイッチへのアクセスを試みるユーザの検証を集中的に処理できます。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されます。Nexus 5000 シリーズ スイッチ上で設定済みの TACACS+ 機能を使用するには、TACACS+ サーバへのアクセス権を持ち、かつこのサーバを設定しておく必要があります。

TACACS+ では、認証、許可、アカウンティングの各ファシリティを個別に提供します。TACACS+ を使用すると、単一のアクセス コントロール サーバ（TACACS+ デーモン）で、各サービス（認証、許可、アカウンティング）を個別に提供できます。各サービスは固有のデータベースにアソシエートされており、デーモンの機能に応じて、そのサーバまたはネットワーク上で使用可能な他のサービスを利用できます。

TACACS+ クライアント/サーバ プロトコルでは、トランスポート要件を満たすため TCP（TCP ポート 49）を使用します。Nexus 5000 シリーズ スイッチは、TACACS+ プロトコルを使用して集中型の認証を行います。

この項では、次のトピックについて取り上げます。

- TACACS+ の利点（18-2 ページ）
- TACACS+ を使用したユーザ ログイン（18-2 ページ）
- デフォルトの TACACS+ サーバ暗号化タイプと事前共有キー（18-3 ページ）
- TACACS+ サーバのモニタリング（18-3 ページ）

TACACS+ の利点

TACACS+ には、RADIUS 認証にはない次の利点があります。

- 独立した AAA ファシリティを提供する。たとえば、Nexus 5000 シリーズ スイッチは、認証を行わずにアクセスを許可できます。
- AAA クライアントとサーバ間のデータ送信に TCP トランスポート プロトコルを使用しているため、コネクション型プロトコルによる確実な転送を実行します。
- スイッチと AAA サーバ間でプロトコル ペイロード全体を暗号化して、高度なデータ機密性を実現します。RADIUS プロトコルはパスワードだけを暗号化します。

TACACS+ を使用したユーザ ログイン

ユーザが TACACS+ を使用して、Nexus 5000 シリーズ スイッチに対しパスワード認証プロトコル（PAP）によるログインを試行すると、次のプロセスが実行されます。

1. Nexus 5000 シリーズ スイッチが接続を確立すると、TACACS+ デーモンにアクセスして、ユーザ名とパスワードを取得します。

   （注） TACACS+ では、デーモンがユーザを認証するために十分な情報を得られるまで、デーモンとユーザとの自由な対話を許可します。この動作では通常、ユーザ名とパスワードの入力が要求されますが、ユーザの母親の旧姓など、その他の項目の入力が要求されることもあります。

2. Nexus 5000 シリーズ スイッチが、TACACS+ デーモンから次のいずれかの応答を受信します。
   - ACCEPT：ユーザの認証に成功したので、サービスを開始します。Nexus 5000 シリーズ スイッチがユーザの許可を要求している場合は、許可が開始されます。
   - REJECT：ユーザの認証に失敗しました。TACACS+ デーモンは、ユーザに対してそれ以上のアクセスを拒否するか、ログイン シーケンスを再試行するよう要求します。
   - ERROR：認証中に、デーモン内、またはデーモンと Nexus 5000 シリーズ スイッチ間のネットワーク接続でエラーが発生しました。Nexus 5000 シリーズ スイッチは ERROR 応答を受信すると、代わりのユーザ認証方式を試します。

   Nexus 5000 シリーズ スイッチで許可がイネーブルになっている場合は、この後、許可フェーズの処理が実行されます。ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

3. TACACS+ 許可が必要な場合、Nexus 5000 シリーズ スイッチは、再度、TACACS+ デーモンにアクセスします。デーモンは ACCEPT または REJECT 許可応答を返します。ACCEPT 応答には、ユーザに対する EXEC または NETWORK セッションの送信に使用される属性が含まれます。また ACCEPT 応答により、ユーザがアクセス可能なサービスが決まります。

   この場合のサービスは次のとおりです。
   - Telnet、rlogin、ポイントツーポイント プロトコル（PPP）、シリアル ライン インターネット プロトコル（SLIP）、EXEC サービス
   - 接続パラメータ（ホストまたはクライアントの IP アドレス（IPv4 または IPv6）、アクセス リスト、ユーザ タイムアウト）

デフォルトの TACACS+ サーバ暗号化タイプと事前共有キー

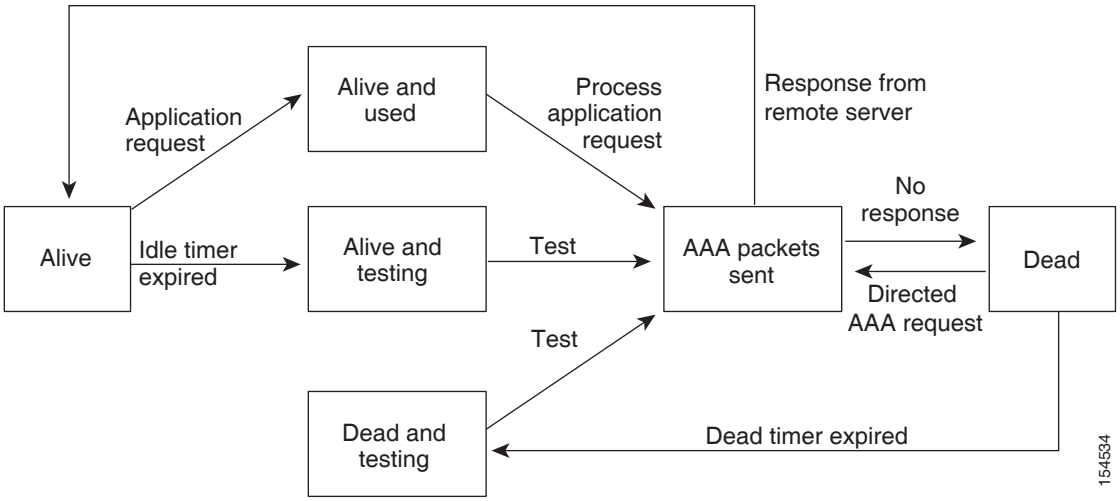
TACACS+ サーバに対してスイッチを認証するには、TACACS+ 事前共有鍵を設定する必要があります。事前共有キーとは、Nexus 5000 シリーズ スイッチと TACACS+ サーバ ホスト間で共有される秘密テキスト ストリングです。キーの長さは 63 文字で、出力可能な任意の ASCII 文字を含めることができます（スペースは使用できません）。Nexus 5000 シリーズ スイッチ上のすべての TACACS+ サーバ設定で使用されるグローバルな事前共有秘密キーを設定できます。

グローバルな事前共有キーの割り当ては、個々の TACACS+ サーバの設定時に明示的に **key** オプションを使用することによって無効にできます。

TACACS+ サーバのモニタリング

応答を返さない TACACS+ サーバがあると、AAA 要求の処理に遅延が発生する可能性があります。Nexus 5000 シリーズ スイッチは、AAA 要求の処理時間を節約するため、定期的に TACACS+ サーバを監視し、TACACS+ サーバが応答を返す（アライブ）かどうかをチェックします。また、応答を返さない TACACS+ サーバをデッド（dead）としてマークし、デッド TACACS+ サーバには AAA 要求を送信しません。Nexus 5000 シリーズ スイッチは定期的にデッド TACACS+ サーバを監視し、応答があった場合、アライブ状態に戻します。このモニタリング プロセスでは、実際の AAA 要求が送信される前に、TACACS+ サーバが稼働状態であることを確認します。TACACS+ サーバの状態がデッドまたはアライブに変わると、簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、Nexus 5000 シリーズ スイッチによって、パフォーマンスに影響が出る前に、障害が発生していることを知らせるエラー メッセージが表示されます。図 18-1を参照してください。

図 18-1　TACACS+ サーバの状態



（注）　アライブ サーバとデッド サーバのモニタリング間隔は異なります。これらはユーザが設定できます。TACACS+ サーバ モニタリングを実行するには、テスト認証要求を TACACS+ サーバに送信します。

TACACS+ の前提条件

TACACS+ には、次の前提条件があります。

- TACACS+ サーバの IP アドレス（IPv4 または IPv6）またはホスト名を取得していること
- TACACS+ サーバから事前共有キーを取得していること。
- Nexus 5000 シリーズ スイッチが、AAA サーバの TACACS+ クライアントとして設定されていること

注意事項および制約事項

TACACS+ に関する注意事項と制約事項は次のとおりです。

- Nexus 5000 シリーズ スイッチ上に設定できる TACACS+ サーバの数は最大 64 個です。

TACACS+ の設定

この項では、次のトピックについて取り上げます。

- TACACS+ サーバの設定プロセス（18-5 ページ）
- TACACS+ のイネーブル化（18-5 ページ）
- TACACS+ サーバ ホストの設定（18-6 ページ）
- グローバルな事前共有キーの設定（18-7 ページ）
- TACACS+ サーバの事前共有キーの設定（18-8 ページ）
- TACACS+ サーバ グループの設定（18-8 ページ）
- ログイン時の TACACS+ サーバの指定（18-9 ページ）
- グローバルな TACACS+ タイムアウト間隔の設定（18-10 ページ）
- サーバのタイムアウト間隔の設定（18-10 ページ）
- TCP ポートの設定（18-11 ページ）
- TACACS+ サーバの定期的モニタリングの設定（18-12 ページ）
- デッド タイム間隔の設定（18-13 ページ）
- TACACS+ サーバまたはグループの手動でのモニタリング（18-13 ページ）
- TACACS+ のディセーブル化（18-14 ページ）

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

TACACS+ サーバの設定プロセス

TACACS+ サーバを設定するには、次の作業を行います。

ステップ 1　TACACS+ をイネーブルにします。

「TACACS+ のイネーブル化」セクション（18-5 ページ）を参照してください。

ステップ 2　TACACS+ サーバと Nexus 5000 シリーズ スイッチとの接続を確立します。

「TACACS+ サーバ ホストの設定」セクション（18-6 ページ）を参照してください。

ステップ 3　TACACS+ サーバの事前共有秘密キーを設定します。

「グローバルな事前共有キーの設定」セクション（18-7 ページ）および「TACACS+ サーバの事前共有キーの設定」セクション（18-8 ページ）を参照してください。

ステップ 4　必要に応じて、AAA 認証方式用に、TACACS+ サーバのサブセットを使用して TACACS+ サーバグループを設定します。

「TACACS+ サーバ グループの設定」セクション（18-8 ページ）および「AAA の設定」セクション（16-6 ページ）を参照してください。

ステップ 5　必要に応じて、次のオプションのパラメータを設定します。

- デッドタイム間隔
- ログイン時に TACACS+ サーバの指定を許可
- タイムアウト間隔

  「グローバルな TACACS+ タイムアウト間隔の設定」セクション（18-10 ページ）を参照してください。
- TCP ポート

  「TCP ポートの設定」セクション（18-11 ページ）を参照してください。

ステップ 6　必要に応じて、定期的に TACACS+ サーバをモニタリングするよう設定します。

「TACACS+ サーバの定期的モニタリングの設定」セクション（18-12 ページ）を参照してください。

TACACS+ のイネーブル化

デフォルトでは、Nexus 5000 シリーズ スイッチで TACACS+ 機能はディセーブルに設定されています。TACACS+ 機能を明示的にイネーブルにして、認証用のコンフィギュレーション コマンドおよび確認コマンドにアクセスする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# feature tacacs+`	TACACS+ をイネーブルにします。

	コマンド	目的
ステップ 3	`switch(config)# exit`	設定モードを終了します。
ステップ 4	`switch# copy running-config startup-config`	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

TACACS+ サーバ ホストの設定

リモートの TACACS+ サーバにアクセスするには、Nexus 5000 シリーズ スイッチ上に、TACACS+ サーバの IP アドレス(IPv4 または IPv6)またはホスト名を設定する必要があります。すべての TACACS+ サーバ ホストは、デフォルトの TACACS+ サーバ グループに追加されます。最大 64 個の TACACS+ サーバを設定できます。

設定済みの TACACS+ サーバに事前共有キーが設定されておらず、グローバル キーも設定されていない場合は、警告メッセージが表示されます。TACACS+ サーバ キーが設定されていない場合は、グローバル キー(設定されている場合)が該当サーバで使用されます(「グローバルな事前共有キーの設定」セクション(18-7 ページ)および「TACACS+ サーバの事前共有キーの設定」セクション(18-8 ページ)を参照)。

TACACS+ サーバ ホストを設定する前に、次の点を確認してください。

- TACACS+ がイネーブルになっていること(「TACACS+ のイネーブル化」セクション(18-5 ページ)を参照)。
- リモート TACACS+ サーバの IP アドレス(IPv4 または IPv6)またはホスト名を取得していること。

TACACS+ サーバ ホストを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# tacacs-server host {ipv4-address | ipv6-address|host-name}`	TACACS+ サーバの IP アドレス(IPv4 または IPv6)、またはホスト名を指定します。
ステップ 3	`switch(config)# exit`	設定モードを終了します。
ステップ 4	`switch# show tacacs-server`	(任意)TACACS+ サーバの設定を表示します。
ステップ 5	`switch# copy running-config startup-config`	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

サーバ グループから TACACS+ サーバ ホストを削除できます。

グローバルな事前共有キーの設定

Nexus 5000 シリーズ スイッチで使用するすべてのサーバでは、グローバル レベルで事前共有キーを設定できます。事前共有キーとは、Nexus 5000 シリーズ スイッチと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

事前共有キーを設定する前に、次の点を確認してください。

- TACACS+ がイネーブルになっていること（「TACACS+ のイネーブル化」セクション（18-5 ページ）を参照）。
- リモートの TACACS+ サーバの事前共有キー値を取得していること。

グローバルな事前共有キーを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# tacacs-server key [0|7] key-value`	すべての TACACS+ サーバで使用する事前共有キーを指定します。クリア テキスト形式（**0**）または暗号化形式（**7**）の事前共有キーを指定できます。デフォルトの形式はクリア テキストです。最大で 63 文字です。 デフォルトでは、事前共有キーは設定されません。
ステップ 3	`switch(config)# exit`	設定モードを終了します。
ステップ 4	`switch# show tacacs-server`	（任意）TACACS+ サーバの設定を表示します。 **（注）** 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、グローバルな事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server key 0 QsEfThUkO
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

TACACS+ サーバの事前共有キーの設定

TACACS+ サーバの事前共有キーを設定できます。事前共有キーとは、Nexus 5000 シリーズ スイッチと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

TACACS+ 事前共有キーを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# tacacs-server host {ipv4-address|ipv6-address|host-name} key [0|7] key-value`	特定の TACACS+ サーバの事前共有キーを指定します。クリア テキスト形式（**0**）または暗号化形式（**7**）の事前共有キーを指定できます。デフォルトの形式はクリア テキストです。最大で 63 文字です。 この事前共有キーがグローバル事前共有キーの代わりに使用されます。
ステップ 3	`switch(config)# exit`	設定モードを終了します。
ステップ 4	`switch# show tacacs-server`	（任意）TACACS+ サーバの設定を表示します。 **（注）** 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、TACACS+ 事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 key 0 PlIjUhYg
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

TACACS+ サーバ グループの設定

サーバ グループを使用して、1 台または複数台のリモート AAA サーバによるユーザ認証を指定することができます。グループのメンバーはすべて、TACACS+ プロトコルに属している必要があります。設定した順序に従ってサーバが試行されます。

これらのサーバ グループはいつでも設定できますが、設定したグループを有効にするには、AAA サービスに適用する必要があります。AAA サービスについては、「リモート AAA サービス」セクション（16-3 ページ）を参照してください。

TACACS+ サーバ グループを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# aaa group server tacacs+ group-name`	TACACS+ サーバ グループを作成し、そのグループのTACACS+ サーバ グループ コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-tacacs+)# server {ipv4-address|ipv6-address|host-name}`	TACACS+ サーバを、TACACS+ サーバ グループのメンバーとして設定します。 **ヒント**　指定した TACACS+ サーバが見つからない場合は、**tacacs-server host** コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	`switch(config-tacacs+)# deadtime minutes`	(任意)モニタリング デッド タイムを設定します。デフォルト値は 0 分です。指定できる範囲は 0 ～ 1440 です。 **(注)**　TACACS+ サーバ グループのデッド タイム間隔が 0 より大きい場合は、その値がグローバルなデッド タイム値より優先されます。
ステップ 5	`switch(config-tacacs+)# exit`	設定モードを終了します。
ステップ 6	`switch(config)# show tacacs-server groups`	(任意)TACACS+ サーバ グループの設定を表示します。
ステップ 7	`switch(config)# copy running-config startup-config`	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、TACACS+ サーバ グループを設定する例を示します。

```
switch# configure terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
switch(config-tacacs+)# deadtime 30
switch(config-tacacs+)# exit
switch(config)# show tacacs-server groups
switch(config)# copy running-config startup-config
```

ログイン時の TACACS+ サーバの指定

認証要求の送信先 TACACS+ サーバをユーザが指定できるようにスイッチを設定するには、directed-request オプションをイネーブルにします。デフォルトでは、Nexus 5000 シリーズ スイッチは、デフォルトの AAA 認証方式に基づいて認証要求をフォワーディングします。このオプションをイネーブルにすると、ユーザは *username@hostname* としてログインできます。ここで、*hostname* は設定済みの RADIUS サーバの名前です。

（注）　ユーザ指定のログインは、Telnet セッションでのみサポートされます。

ログイン時に TACACS+ サーバを指定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **tacacs-server directed-request**	ログイン時にユーザが認証要求の送信先となる TACACS+ サーバを指定できるようにします。デフォルトでは無効になっています。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show tacacs-server directed-request**	(任意)TACACS+ の directed request の設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

グローバルな TACACS+ タイムアウト間隔の設定

Nexus 5000 シリーズ スイッチが、すべての TACACS+ サーバからの応答を待機するグローバルなタイムアウト間隔を設定できます。この時間が経過してもサーバから応答がない場合は、タイムアウト エラーが宣言されます。タイムアウト間隔は、Nexus 5000 シリーズ スイッチがタイムアウト エラーを宣言する前に、TACACS+ サーバからの応答を待機する時間を決定します。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **tacacs-server timeout** *seconds*	TACACS+ サーバのタイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒で、範囲は 1 ～ 60 秒です。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show tacacs-server**	(任意)TACACS+ サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

サーバのタイムアウト間隔の設定

Nexus 5000 シリーズ スイッチが、TACACS+ サーバからの応答を待機するタイムアウト間隔を設定できます。この時間が経過してもサーバから応答がない場合は、タイムアウト エラーが宣言されます。タイムアウト間隔は、Nexus 5000 シリーズ スイッチがタイムアウト エラーを宣言する前に、TACACS+ サーバからの応答を待機する時間を決定します。

サーバのタイムアウト間隔を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# switch(config)# **tacacs-server host** {*ipv4-address*|*ipv6-address*|*host-name*} **timeout** *seconds*	特定のサーバのタイムアウト間隔を指定します。デフォルトはグローバル値です。 **（注）** 特定の TACACS+ サーバに指定したタイムアウト間隔は、すべての TACACS+ サーバに指定したタイムアウト間隔より優先されます。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show tacacs-server**	（任意）TACACS+ サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

TCP ポートの設定

別のアプリケーションとポート番号が競合している場合は、TACACS+ サーバ用に別の TCP ポートを設定できます。デフォルトでは、Nexus 5000 シリーズ スイッチは、すべての TACACS+ 要求に 49 番ポートを使用します。

TCP ポートを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-address*|*ipv6-address*|*host-name*} **port** *tcp-port*	TACACS+ アカウンティング メッセージ用の UDP ポートを指定します。デフォルトの TCP ポートは 49 です。有効な範囲は 1 ～ 65535 です。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show tacacs-server**	（任意）TACACS+ サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、TCP ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 port 2
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

TACACS+ サーバの定期的モニタリングの設定

TACACS+ サーバの可用性をモニタリングできます。パラメータとして、サーバに使用するユーザ名とパスワード、およびアイドル タイマーがあります。アイドル タイマーには、TACACS+ サーバが要求を受信しなかった場合に Nexus 5000 シリーズ スイッチがテスト パケットを送信するまでの間隔を指定します。このオプションを設定して、サーバを定期的にテストできます。また、1 回だけテストを実行することもできます。

（注） ネットワークのセキュリティ保護のため、TACACS+ データベース内の既存のユーザ名と同じユーザ名を使用しないことを推奨します。

テスト アイドル タイマーには、TACACS+ サーバが要求を受信しなくなってから、Nexus 5000 シリーズ スイッチがテスト パケットを送信するまでの間隔を指定します。

（注） デフォルトのアイドル タイマー値は 0 分です。アイドル タイム間隔が 0 分の場合、TACACS+ サーバの定期的なモニタリングは実行されません。

TACACS+ サーバの定期的なモニタリングを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configure terminal`**	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`tacacs-server host`** {*ipv4-address* | *ipv6-address* | *host-name*} **`test`** {**`idle-time`** *minutes* | **`password`** *password* [**`idle-time`** *minutes*] | **`username`** *name* [**`password`** *password* [**`idle-time`** *minutes*]]}	サーバ モニタリング用のパラメータを指定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。アイドル タイマーのデフォルト値は 0 分、指定できる範囲は 0 ～ 1440 分です。 **（注）** TACACS+ サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	`switch(config)#` **`tacacs-server dead-time`** *minutes*	Nexus 5000 シリーズ スイッチが、前回応答しなかった TACACS+ サーバをチェックするまでの時間（分）を指定します。デフォルト値は 0 分、指定できる範囲は 0 ～ 1440 分です。
ステップ 4	`switch(config)#` **`exit`**	設定モードを終了します。
ステップ 5	`switch#` **`show tacacs-server`**	（任意）TACACS+ サーバの設定を表示します。
ステップ 6	`switch#` **`copy running-config startup-config`**	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、TACACS+ サーバの定期的モニタリングを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 test username user1 password Ur2Gd2BH
idle-time 3
switch(config)# tacacs-server dead-time 5
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

デッド タイム間隔の設定

すべての TACACS+ サーバのデッド タイム間隔を設定できます。デッドタイム間隔には、Nexus 5000 シリーズ スイッチが TACACS+ サーバをデッドとして宣言したあと、そのサーバがアライブ状態に戻ったかどうかを判断するためのテスト パケットを送信するまでの間隔を指定します。

（注）　デッド タイム間隔が 0 分の場合、TACACS+ サーバは、応答を返さない場合でも、デットとしてマークされません。デッド タイマーはグループ単位で設定できます（「TACACS+ サーバ グループの設定」セクション（18-8 ページ）を参照）。

すべての TACACS+ サーバのデッド タイム間隔を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# tacacs-server deadtime minutes`	グローバルなデッド タイム間隔を設定します。デフォルト値は 0 分です。有効な範囲は 1 ～ 1440 分です。
ステップ 3	`switch(config)# exit`	設定モードを終了します。
ステップ 4	`switch# show tacacs-server`	（任意）TACACS+ サーバの設定を表示します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

TACACS+ サーバまたはグループの手動でのモニタリング

TACACS+ サーバまたはサーバ グループにテスト メッセージを手動で送信する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# test aaa server tacacs+ {ipv4-address|ipv6-address|host-name} [vrf vrf-name] username password`	TACACS+ サーバにテスト メッセージを送信して可用性を確認します。
ステップ 1	`switch# test aaa group group-name username password`	TACACS+ サーバ グループにテスト メッセージを送信して可用性を確認します。

次に、手動でテスト メッセージを送信する例を示します。

```
switch# test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH
switch# test aaa group TacGroup user2 As3He3CI
```

TACACS+ のディセーブル化

TACACS+ をディセーブルにできます。

注意 TACACS+ 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。

TACACS+ をディセーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# feature tacacs+`	TACACS+ をイネーブルにします。
ステップ 3	`switch(config)# exit`	設定モードを終了します。
ステップ 4	`switch# copy running-config startup-config`	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

TACACS+ 統計情報の表示

Nexus 5000 シリーズ スイッチが TACACS+ のアクティビティについて保持している統計情報を表示する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# show tacacs-server statistics {hostname|ipv4-address|ipv6-address}`	TACACS+ 統計情報を表示します。

このコマンドの出力フィールドの詳細については、『*Cisco Nexus 5000 シリーズ Command Reference*』を参照してください。

TACACS+ の設定の確認

TACACS+ の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config tacacs [**all**]	実行コンフィギュレーションの TACACS+ 設定を表示します。
show startup-config tacacs	スタートアップ コンフィギュレーションの TACACS+ 設定を表示します。
show tacacs-server [*host-name* | *ipv4-address* | *ipv6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	設定済みのすべての TACACS+ サーバのパラメータを表示します。

TACACS+ の設定例

次に、TACACS+ を設定する例を示します。

```
feature tacacs+
tacacs-server key 7 "ToIkLhPpG"
tacacs-server host 10.10.2.2 key 7 "ShMoMhTl"
aaa group server tacacs+ TacServer
    server 10.10.2.2
use-vrf management
```

デフォルト設定

表 18-1 に、TACACS+ パラメータのデフォルト設定を示します。

表 18-1　TACACS+ のデフォルト パラメータ

パラメータ	デフォルト
TACACS+	ディセーブル
デッド タイマー間隔	0 分
タイムアウト間隔	5 秒
アイドル タイマー間隔	0 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	test

CHAPTER 19

SSH および Telnet の設定

この章では、Nexus 5000 シリーズ スイッチ上で、セキュア シェル（SSH）プロトコルおよび Telnet を設定する方法について説明します。

この章は、次の項で構成されています。

- SSH および Telnet について（19-1 ページ）
- SSH の前提条件（19-2 ページ）
- 注意事項および制約事項（19-3 ページ）
- SSH の設定（19-3 ページ）
- Telnet の設定（19-8 ページ）
- SSH および Telnet の設定の確認（19-9 ページ）
- SSH の設定例（19-9 ページ）
- デフォルト設定（19-10 ページ）

SSH および Telnet について

この項では、次のトピックについて取り上げます。

- SSH サーバ（19-1 ページ）
- SSH クライアント（19-2 ページ）
- SSH サーバ キー（19-2 ページ）
- Telnet サーバ（19-2 ページ）

SSH サーバ

SSH サーバ機能を使用すると、SSH クライアントが Nexus 5000 シリーズ スイッチに対して、セキュアで暗号化された接続を確立できます。SSH は強化暗号化を使用して認証を行います。Nexus 5000 シリーズ スイッチの SSH サーバは、無償あるいは商用の SSH クライアントと連係して動作します。

SSH がサポートするユーザ認証メカニズムには、RADIUS、TACACS+、およびローカルに格納されたユーザ名とパスワードを使用した認証があります。

SSH クライアント

SSH クライアント機能は、SSH プロトコルを介して実行されるアプリケーションで、認証と暗号化を行います。SSH クライアントを使用すると、Nexus 5000 シリーズ スイッチは、別の Nexus 5000 シリーズ スイッチまたは SSH サーバを稼働している他の任意のデバイスと、セキュアで暗号化された接続を確立できます。この接続は、暗号化されたアウトバウンド接続を実現します。認証と暗号化により、SSH クライアントは、セキュリティ保護されていないネットワーク上でもセキュアな通信を実現できます。

Nexus 5000 シリーズ スイッチの SSH クライアントは、無償あるいは商用の SSH サーバと連係して動作します。

SSH サーバ キー

SSH では、Nexus 5000 シリーズ スイッチとのセキュアな通信を行うためにサーバ キーが必要です。SSH キーは、次の SSH オプションに使用できます。

- Rivest, Shamir, and Adelman（RSA）公開キー暗号化を使用した SSH バージョン 2
- Digital System Algrorithm（DSA）を使用した SSH バージョン 2

SSH サービスをイネーブルにする前に、適切なバージョンの SSH サーバ キー ペアを取得してください。使用中の SSH クライアント バージョンに応じて、SSH サーバ キー ペアを生成します。SSH サービスでは、SSH バージョン 2 に対応する 2 とおりのキー ペアを使用できます。

- **dsa** オプションを使用すると、SSH バージョン 2 プロトコルに対応する DSA キーペアが生成されます。
- **rsa** オプションを使用すると、SSH バージョン 2 プロトコルに対応する RSA キーペアが生成されます。

デフォルトでは、Nexus 5000 シリーズ スイッチは 1024 ビットの RSA キーを生成します。

注意　SSH キーをすべて削除すると、SSH サービスを開始できません。

Telnet サーバ

Telnet プロトコルは、ホストとの TCP/IP 接続を確立します。Telnet を使用すると、あるサイトのユーザが別サイトのログイン サーバとの TCP 接続を確立して、システム間でキーストロークをやり取りできます。Telnet は、リモート システムのアドレスとして、IP アドレスまたはドメイン名を受け取ります。

Nexus 5000 シリーズ スイッチでは、デフォルトで Telnet サーバがイネーブルです。

SSH の前提条件

SSH には次の前提条件があります。

- レイヤ 3 インターフェイス上に IP 接続、mgmt 0 インターフェイス上にアウトオブバンド接続、イーサネット インターフェイス上にインバンド接続が設定されていること。

注意事項および制約事項

SSH 設定時の注意事項と制約事項は次のとおりです。

- Nexus 5000 シリーズ スイッチは、SSH バージョン 2（SSHv2）だけサポートしています。

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

SSH の設定

ここでは、次の内容について説明します。

- SSH サーバ キーの生成（19-3 ページ）
- ユーザ アカウント用 SSH 公開キーの指定（19-4 ページ）
- リモート デバイスとの SSH セッションの開始（19-6 ページ）
- SSH ホストのクリア（19-6 ページ）
- SSH サーバのディセーブル化（19-6 ページ）
- SSH サーバ キーの削除（19-7 ページ）
- SSH セッションのクリア（19-7 ページ）

SSH サーバ キーの生成

セキュリティ要件に基づいて SSH サーバ キーを生成できます。デフォルトの SSH サーバ キーは、1024 ビットで生成される RSA キーです。SSH サーバ キーを生成する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# ssh key {dsa [force] | rsa [bits [force]]}`	SSH サーバ キーを生成します。 *bits* 引数には、キーの生成に使用するビット数を指定します。指定できる範囲は 768 ～ 2048 ビットで、デフォルトは 1024 ビットです。 既存のキーを置き換える場合は、キーワード **force** を使用します。
ステップ 3	`switch(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 4	`switch# show ssh key`	（任意）SSH サーバ キーを表示します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、SSH サーバ キーを生成する例を示します。

```
switch# configure terminal
switch(config)# ssh key rsa 2048
switch(config)# exit
switch# show ssh key
switch# copy running-config startup-config
```

ユーザ アカウント用 SSH 公開キーの指定

SSH 公開キーを設定すると、パスワードを要求されることなく、SSH クライアントを使用してログインできます。SSH 公開キーは、次の 3 種類のいずれかの形式で指定できます。

- Open SSH 形式
- Internet Engineering Task Force（IETF）SECSH 形式
- Privacy Enhanced Mail（PEM）形式の公開キー証明書

Open SSH 形式による SSH 公開キーの指定

ユーザ アカウント用に SSH 形式で SSH 公開キーを指定できます。

Open SSH 形式で SSH 公開キーを指定するには、Open SSH 形式で SSH 公開キーを生成し、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# username` *`username`* `sshkey` *`ssh-key`*	SSH 形式で SSH 公開キーを設定します。
ステップ 3	`switch(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 4	`switch# show user-account`	（任意）ユーザ アカウントの設定を表示します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、Open SSH 形式で SSH 公開キーを指定する例を示します。

```
switch# configure terminal
switch(config)# switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/
DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH
3UD/vKyziEh5S4Tplx8=
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

IETF SECSH 形式による SSH 公開キーの指定

ユーザ アカウント用に IETF SECSH 形式で SSH 公開キーを指定できます。

IETF SECSH 形式で SSH 公開キーを指定するには、IETF SECSH 形式で SSH 公開キーを生成し、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **copy** server-file **bootflash:***filename*	サーバから IETF SECSH 形式の SSH キーを含むファイルをダウンロードします。File Transfer Protocol（FTP）、SCP、SSH File Transfer Protocol（SFTP）、または Trivial File Transfer Protocol（TFTP）サーバを利用できます。
ステップ 2	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 3	switch(config)# **username** *username* **sshkey file** *filename*	SSH 形式で SSH 公開キーを設定します。
ステップ 4	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 5	switch# **show user-account**	（任意）ユーザ アカウントの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、IETF SECSH 形式で SSH 公開キーを指定する例を示します。

```
switch# copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub
switch# configure terminal
switch(config)# username User1 sshkey file bootflash:secsh_file.pub
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

PEM フォーマット化された公開キー証明書形式による SSH 公開キーの指定

ユーザ アカウント用に PEM フォーマット化された公開キー証明書形式で SSH 公開キーを指定できます。

PEM フォーマット化された公開キー証明書形式で SSH 公開キーを指定するには、PEM フォーマット化された公開キー証明書形式で SSH 公開キーを生成し、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **copy** server-file **bootflash:***filename*	サーバから PEM フォーマット化された公開キー証明書形式の SSH キーを含むファイルをダウンロードします。FTP、SCP、SFTP、または TFTP サーバを利用できます。
ステップ 2	switch# **configure terminal**	コンフィギュレーション モードに入ります。

	コマンド	目的
ステップ 3	switch# **show user-account**	(任意)ユーザ アカウントの設定を表示します。
ステップ 4	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、PEM フォーマット化された公開キー証明書形式で SSH 公開キーを指定する例を示します。

```
switch# copy tftp://10.10.1.1/cert.pem bootflash:cert.pem
switch# configure terminal
switch# show user-account
switch# copy running-config startup-config
```

リモート デバイスとの SSH セッションの開始

Nexus 5000 シリーズ スイッチからリモート デバイスに接続する SSH セッションを開始できます。

	コマンド	目的
ステップ 1	switch# **ssh** {*hostname* | *username*@*hostname*} [**vrf** *vrf-name*]	リモート デバイスとの SSH セッションを作成します。引数 *hostname* には、IPv4 アドレス、IPv6 アドレス、またはデバイス名を指定します。

SSH ホストのクリア

SCP または SFTP を使用してサーバからファイルをダウンロードする場合は、サーバと信頼性のある SSH 関係を確立します。ユーザ アカウント用の信頼性のある SSH サーバのリストをクリアする手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **clear ssh hosts**	SSH ホスト セッションをクリアします。

SSH サーバのディセーブル化

Nexus 5000 シリーズ スイッチでは、デフォルトで SSH サーバがイネーブルになっています。

SSH サーバをディセーブルにしてスイッチへの SSH アクセスを禁止する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **[no] feature ssh**	SSH サーバをイネーブル/ディセーブルにします。デフォルトではイネーブルになっています。

	コマンド	目的
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 4	switch# **show ssh server**	(任意)SSH サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

SSH サーバ キーの削除

SSH サーバをディセーブルにした後、SSH サーバ キーを削除できます。

(注) SSH を再度イネーブルにするには、まず、SSH サーバ キーを生成する必要があります(「SSH サーバ キーの生成」セクション(19-3 ページ)を参照)。

SSH サーバ キーを削除する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **[no] feature ssh**	SSH サーバをイネーブル/ディセーブルにします。
ステップ 3	switch(config)# **no ssh key** [**dsa** | **rsa**]	SSH サーバ キーを削除します。 デフォルトでは、すべての SSH キーが削除されます。
ステップ 4	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 5	switch# **show ssh key**	(任意)SSH サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

SSH セッションのクリア

Nexus 5000 シリーズ スイッチから SSH セッションをクリアするには、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **show users**	ユーザ セッション情報を表示します。
ステップ 2	switch(config)# **clear line** *vty-line*	ユーザ SSH セッションをクリアします。

Telnet の設定

この項では、次のトピックについて取り上げます。

- SSH セッションのクリア（19-7 ページ）
- リモート デバイスとの Telnet セッションの開始（19-8 ページ）
- SSH セッションのクリア（19-7 ページ）

Telnet サーバのディセーブル化

デフォルトでは、Telnet サーバはイネーブルに設定されています。Nexus 5000 シリーズ スイッチ上の Telnet サーバをディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# [no] feature telnet`	Telnet サーバをイネーブル/ディセーブルにします。デフォルトではイネーブルになっています。

Telnet サーバをイネーブルに戻す手順は、次のとおりです。

コマンド	目的
`switch(config)# telnet server enable`	Telnet サーバを再度イネーブルにします。

リモート デバイスとの Telnet セッションの開始

Telnet セッションを開始してリモート デバイスに接続する前に、次の作業を行う必要があります。

- リモート デバイスのホスト名を取得し、必要に応じて、リモート デバイスのユーザ名も取得します。
- Nexus 5000 シリーズ スイッチ上で Telnet サーバをイネーブルにします。
- リモート デバイス上で Telnet サーバをイネーブルにします。

Telnet セッションを開始して、Nexus 5000 シリーズ スイッチからリモート デバイスに接続するには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# telnet hostname`	リモート デバイスとの Telnet セッションを作成します。引数 *hostname* には、IPv4 アドレス、IPv6 アドレス、またはデバイス名を指定します。

次に、Telnet セッションを開始してリモート デバイスに接続する例を示します。

```
switch# telnet 10.10.1.1
Trying 10.10.1.1...
Connected to 10.10.1.1.
Escape character is '^]'.
switch login:
```

Telnet セッションのクリア

Nexus 5000 シリーズ スイッチから Telnet セッションをクリアするには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# show users`	ユーザ セッション情報を表示します。
ステップ 2	`switch(config)# clear line vty-line`	ユーザ Telnet セッションをクリアします。

SSH および Telnet の設定の確認

SSH の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ssh key [dsa | rsa]	SSH サーバ キー ペアの情報を表示します。
show running-config security [all]	実行コンフィギュレーション内の SSH とユーザ アカウントの設定を表示します。キーワード **all** を指定すると、SSH およびユーザ アカウントのデフォルト値が表示されます。
show ssh server	SSH サーバの設定を表示します。
show user-account	ユーザ アカウント情報を表示します。

SSH の設定例

次に、SSH を設定する例を示します。

ステップ 1　SSH サーバ キーを生成します。

```
switch(config)# ssh key rsa
generating rsa key(1024 bits).....
.
generated rsa key
```

ステップ 2　SSH サーバをイネーブルにします。

```
switch# configure terminal
switch(config)# ssh server enable
```

ステップ 3　SSH サーバ キーを表示します。

```
switch(config)# show ssh key
rsa Keys generated:Sat Sep 29 00:10:39 2007

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvWhEBsF55oaPHNDBnpXOTw6+/OdHoLJZKr+MZm99n2U0
ChzZG4svRWmHuJY4PeDWl0e5yE3g3EO3pjDDmt923siNiv5aSga60K36lr39HmXL6VgpRVn1XQFiBwn4
na+H1d3Q0hDt+uWEA0tka2uOtXlDhliEmn4HVXOjGhFhoNE=

bitcount:1024
fingerprint:
51:6d:de:1c:c3:29:50:88:df:cc:95:f0:15:5d:9a:df
*************************************
could not retrieve dsa key information
*************************************
```

ステップ 4　Open SSH 形式による SSH 公開キーを指定します。

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/
DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH
3UD/vKyziEh5S4Tplx8=
```

ステップ 5　設定を保存します。

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

デフォルト設定

表 19-1 に、SSH パラメータのデフォルト設定を示します。

表 19-1　デフォルトの SSH パラメータ

パラメータ	デフォルト
SSH サーバ	イネーブル
SSH サーバ キー	1024 ビットで生成された RSA キー
RSA キー生成ビット数	1024
Telnet サーバ	イネーブル

CHAPTER 20

ACL の設定

この章では、アクセス コントロール リスト（ACL）の設定方法について説明します。

この章は、次の項で構成されています。

- ACL について（20-1 ページ）
- IP ACL の設定（20-5 ページ）
- MAC ACL の設定（20-10 ページ）
- VLAN ACL について（20-14 ページ）
- VACL の設定（20-15 ページ）
- デフォルト設定（20-18 ページ）

ACL について

ACL とは、トラフィックのフィルタリングに使用する順序付きのルール セットのことです。各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。スイッチは、あるパケットに対してある ACL を適用するかどうかを判断するとき、そのパケットを ACL 内のすべてのルールの条件に対してテストします。一致する条件が最初に見つかった時点で、パケットを許可するか拒否するかが決まります。一致する条件が見つからないと、スイッチは適用可能なデフォルトのルールを適用します。許可されたパケットについては処理が続行され、拒否されたパケットはドロップされます。詳細については、「暗黙のルール」セクション（20-3 ページ）を参照してください。

ACL を使用すると、ネットワークおよび特定のホストを、不要なトラフィックや望ましくないトラフィックから保護できます。たとえば、ACL を使用して、厳重にセキュリティ保護されたネットワークからインターネットにハイパー テキスト トランスファ プロトコル（HTTP）トラフィックが流入するのを禁止できます。また、特定のサイトへの HTTP トラフィックだけを許可することもできます。その場合は、サイトの IP アドレスが、IP ACL に指定されているかどうかによって判定します。

ここでは、次の内容について説明します。

- IP ACL のタイプと適用（20-2 ページ）
- ルール（20-2 ページ）

IP ACL のタイプと適用

Cisco Nexus 5000 シリーズ スイッチは、セキュリティ トラフィック フィルタリング用に、IPv4、IPv6、MAC の各 ACL をサポートしています。また、IP ACL を、ポート ACL および VLAN ACL として使用することもできます（表 20-1を参照）。

表 20-1　セキュリティ ACL の適用

アプリケーション	サポートするインターフェイス	サポートする ACL のタイプ
ポート ACL	ACL は、次のいずれかに適用した場合、ポート ACL と見なされます。 • イーサネット インターフェイス • イーサネット ポート チャネル インターフェイス ポート ACL をトランク ポートに適用すると、その ACL は、当該トランク ポート上のすべての VLAN 上のトラフィックをフィルタリングします。	IPv4 ACL IPv6 ACL MAC ACL
VLAN ACL（VACL）	アクセス マップを使用して ACL をアクションにアソシエートし、そのアクセス マップを VLAN に適用する場合、その ACL は VACL と見なされます。	IPv4 ACL IPv6 ACL MAC ACL

適用順序

スイッチは、パケットを処理するとき、そのパケットの転送パスを決定します。このパスによって、スイッチがトラフィックに適用する ACL が決まります。スイッチは、次の順序で ACL を適用します。

- ポート ACL

ルール

アクセス リスト コンフィギュレーション モードでルールを作成するには、**permit** または **deny** コマンドを使用します。スイッチは、許可ルールに指定された基準に一致するトラフィックを許可し、拒否ルールに指定された基準に一致するトラフィックをブロックします。ルールに一致するためにトラフィックが満たさなければならない基準を設定するためのオプションが多数用意されています。

この項では、次のトピックについて取り上げます。

- 送信元と宛先（20-3 ページ）
- プロトコル（20-3 ページ）
- 暗黙のルール（20-3 ページ）
- その他のフィルタリング オプション（20-3 ページ）
- シーケンス番号（20-3 ページ）
- 論理演算子と論理演算ユニット（20-4 ページ）

送信元と宛先

各ルールには、ルールに一致するトラフィックの送信元と宛先を指定します。指定する送信元および宛先には、特定のホスト、ホストのネットワークまたはグループ、あるいは任意のホストを使用できます。

プロトコル

ACL では、プロトコルによってトラフィックを識別できます。指定の際の手間を省くために、一部のプロトコルは名前で指定できます。たとえば、IPv4 ACL では、ICMP を名前で指定できます。

プロトコルはすべて番号で指定できます。IPv4 ACL では、インターネット プロトコル番号を表す整数でプロトコルを指定できます。たとえば、レイヤ 2 トンネリング プロトコル（L2TP）を指定するには、115 を使用します。

暗黙のルール

IP ACL には暗黙のルールがあります。暗黙のルールとは、実行コンフィギュレーションには（明示的には）指定されていないが、ACL の他のルールが一致しないとき、トラフィックに適用されるルールのことです。

すべての IPv4 ACL には、次の暗黙のルールがあります。

```
deny ip any any
```

この暗黙のルールによって、どの条件にも一致しない IP トラフィックは拒否されます。

その他のフィルタリング オプション

追加のオプションを使用してトラフィックを識別できます。IPv4 ACL には、次の追加フィルタリング オプションが用意されています。

- レイヤ 4 プロトコル
- TCP/UDP ポート
- ICMP タイプおよびコード
- IGMP タイプ
- 優先レベル
- DiffServ コード ポイント（DSCP）値
- ACK、FIN、PSH、RST、SYN、または URG ビットがセットされた TCP パケット
- 確立済み TCP 接続

シーケンス番号

本スイッチでは、ルールにシーケンス番号を付けることができます。入力されたすべてのルールには、ユーザによって、またはスイッチによって自動的に、シーケンス番号が付けられます。シーケンス番号によって、次の ACL 設定作業が容易になります。

- 既存のルールの間に新規のルールを追加する：シーケンス番号を指定することによって、ACL 内での新規ルールの挿入場所を指定します。たとえば、ルール番号 100 と 110 の間に新しいルールを挿入する必要がある場合は、シーケンス番号 105 を新しいルールに割り当てます。

- ルールを削除する：シーケンス番号を使用しない場合は、ルールを削除するのに、次のようにルール全体を入力する必要があります。

  ```
  switch(config-acl)# no permit tcp 10.0.0.0/8 any
  ```

  このルールに 101 番のシーケンス番号が付いていれば、次コマンドだけでルールを削除できます。

  ```
  switch(config-acl)# no 101
  ```

- ルールを移動する：シーケンス番号を使用すれば、同じ ACL 内の異なる場所にルールを移動する必要がある場合に、そのルールのコピーをシーケンス番号で正しい位置に挿入してから、元のルールを削除できます。この方法により、トラフィックを中断せずにルールを移動できます。

シーケンス番号なしでルールを入力すると、そのルールは ACL の末尾に追加され、直前のルールのシーケンス番号に 10 を足した番号が付けられます。たとえば、ACL の最後のルールのシーケンス番号が 225 の場合にシーケンス番号なしでルールを追加すると、新しいルールにシーケンス番号 235 が付けられます。

また、Nexus 5000 シリーズ スイッチでは、ACL 内ルールのシーケンス番号を再割り当てできます。シーケンス番号の再割り当ては、ACL 内に、100、101 のように連続するシーケンス番号のルールがある場合、それらのルールの間に 1 つ以上のルールを挿入する必要があるときに便利です。

論理演算子と論理演算ユニット

TCP および UDP トラフィックの IP ACL ルールでは、論理演算子を使用して、ポート番号に基づきトラフィックをフィルタリングできます。

スイッチは、演算子とオペランドの組み合わせを、論理演算ユニット（LOU）と呼ばれるレジスタ内に格納します。

eq 演算子で LOU を使用しても、LOU への格納は行われません。range 演算子は境界値も含みます。

演算子とオペランドの組み合わせが LOU に格納されるかどうかの判断基準を次に示します。

- 演算子またはオペランドが、他のルールで使用されている演算子とオペランドの組み合わせと異なる場合、この組み合わせは LOU に格納されます。

  たとえば、演算子とオペランドの組み合わせ gt 10 と gt 11 は、それぞれ LOU の半分を使用して別々に格納されます。gt 10 と lt 10 も別々に格納されます。

- 演算子とオペランドの組み合わせがルール内の送信元ポートと宛先ポートのうちどちらに適用されるかは、LOU の使用方法に影響を与えます。同じ組み合わせの一方が送信元ポートに、他方が宛先ポートに別々に適用される場合は、2 つの同じ組み合わせが別々に格納されます。

  たとえば、あるルールによって、演算子とオペランドの組み合わせ gt 10 が送信元ポートに、別のルールによって同じ組み合わせ gt 10 が宛先ポートに適用される場合、両方の組み合わせが LOU の半分に格納され、結果として 1 つの LOU 全体が使用されることになります。このため、gt 10 を使用するルールが追加されても、それ以上 LOU は使用されません。

IP ACL の設定

この項では、次のトピックについて取り上げます。

- IP ACL の作成（20-5 ページ）
- IP ACL の変更（20-6 ページ）
- IP ACL の削除（20-7 ページ）
- IP ACL 内のシーケンス番号の変更（20-7 ページ）
- IP ACL のポート ACL としての適用（20-8 ページ）
- IP ACL の VACL としての適用（20-9 ページ）
- IP ACL の設定の確認（20-9 ページ）
- IP ACL 統計情報の表示と消去（20-9 ページ）

IP ACL の作成

スイッチに IPv4 ACL を作成し、その ACL にルールを追加できます。IP ACL を作成する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configure terminal`**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)#` **`ip access-list`** *`name`*	IP ACL を作成して、IP ACL コンフィギュレーション モードを開始します。*name* 引数は 64 文字以内で指定します。
ステップ 3	`switch(config-acl)#` [*`sequence-number`*] {**`permit`**|**`deny`**} *`protocol source destination`*	IP ACL 内にルールを作成します。多数のルールを作成できます。*sequence-number* 引数には、1 ～ 4294967295 の整数を指定します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細は、『*Cisco Nexus 5000 シリーズ Command Reference*』を参照してください。
ステップ 4	`switch(config-acl)#` **`statistics`**	（任意）ACL に規定されたルールに一致するパケットのグローバルな統計情報をスイッチ内に保持するように指定します。
ステップ 5	`switch(config-acl)#` **`show ip access-lists`** *`name`*	（任意）IP ACL の設定を表示します。
ステップ 6	`switch(config-acl)#` **`copy running-config startup-config`**	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、IPv4 ACL を作成する例を示します。

```
switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
switch(config-acl)# statistics
switch(config-acl)# show ip access-lists acl-01
switch(config-acl)# copy running-config startup-config
```

IP ACL の変更

既存の IPv4 ACL に対してルールの追加または削除を行うことができます。既存のルールは変更できません。ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの間に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。詳細については、「IP ACL 内のシーケンス番号の変更」セクション（20-7 ページ）を参照してください。

IP ACL を変更する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# ip access-list name`	名前で指定した ACL の IP ACL コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-acl)# [sequence-number] {permit|deny} protocol source destination`	（任意）IP ACL 内にルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。*sequence-number* 引数には、1 ～ 4294967295 の整数を指定します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細は、『*Cisco Nexus 5000 シリーズ Command Reference*』を参照してください。
ステップ 4	`switch(config-acl)# no {sequence-number | {permit|deny} protocol source destination}`	（任意）指定したルールを IP ACL から削除します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細は、『*Cisco Nexus 5000 シリーズ Command Reference*』を参照してください。
ステップ 5	`switch(config-acl)# [no] statistics`	（任意）ACL に規定されたルールに一致するパケットのグローバルな統計情報をスイッチ内に保持するように指定します。 **no** オプションを指定すると、ACL のグローバルな統計情報がスイッチ内に保持されなくなります。

	コマンド	目的
ステップ 6	switch(config-acl)# **show ip access-lists** *name*	(任意)IP ACL の設定を表示します。
ステップ 7	switch(config-acl)# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

IP ACL の削除

スイッチから IP ACL を削除できます。

スイッチから IP ACL を削除する前に、ACL がインターフェイスに適用されているかどうかを確認してください。削除できるのは、現在適用されている ACL だけです。ACL を削除しても、その ACL が適用されていたインターフェイスの設定は影響を受けません。スイッチは、削除対象の ACL が空であると見なします。

スイッチから IP ACL を削除する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no ip access-list** *name*	名前で指定した IP ACL を実行コンフィギュレーションから削除します。
ステップ 3	switch(config)# **show running-config**	(任意)ACL の設定を表示します。削除された IP ACL は表示されないはずです。
ステップ 4	switch(config)# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

IP ACL 内のシーケンス番号の変更

IP ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。シーケンス番号を変更する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **resequence ip access-list** *name starting-sequence-number increment*	ACL 内に記述されているルールにシーケンス番号を付けます。指定した開始シーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。*starting-sequence-number* 引数と *increment* 引数は、1 ～ 4294967295 の整数で指定します。

	コマンド	目的
ステップ 3	switch(config)# **show ip access-lists** *name*	(任意)IP ACL の設定を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

IP ACL のポート ACL としての適用

IPv4 ACL は、物理イーサネット インターフェイスまたはポート チャネルに適用できます。これらのインターフェイス タイプに適用された ACL は、ポート ACL と見なされます。IP ACL を適用する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface ethernet** *slot/port*	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
	switch(config)# **interface port-channel** *channel-number*	ポート チャネルのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config)# **interface ethernet** *slot/port* switch(config-if)# **ipv6 port traffic-filter <name> in**	IPv6 ポート アクセス リストを適用します。
ステップ 4	switch(config-if)# **ip port access-group access-list in**	IPv4 ACL を、インターフェイスまたはポート チャネルに適用します。ポート ACL では、インバウンド フィルタリングだけがサポートされています。1 つのインターフェイスに 1 つのポート ACL を適用できます。
ステップ 5	switch(config-if)# **show running-config**	(任意)ACL の設定を表示します。
ステップ 6	switch(config-if)# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、IPv4 ACL または IPv6 ACL をポート チャネルに適用する例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 5
switch(config-if)# ip port access-group acl-l2-marketing-group in
switch(config-if)# show running-config
switch(config-if)# copy running-config startup-config
```

次に、acl-01 という名前の IPv4 ACL を作成して、Ethernet インターフェイス 2/1(レイヤ 2 インターフェイス)に適用する例を示します。

```
ip access-list acl-01
  permit ip 192.168.2.0/24 any
interface ethernet 2/1
  ip access-group acl-01 in
```

IP ACL の VACL としての適用

VACL の設定については、「VACL の設定」セクション（20-15 ページ）を参照してください。

IP ACL の設定の確認

IP ACL 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show running-config	ACL の設定（IP ACL の設定と IP ACL が適用されるインターフェイス）を表示します。
show ip access-lists	IP ACL の設定を表示します。
show running-config interface	ACL が適用されたインターフェイスの設定を表示します。

これらのコマンドの出力に表示される各フィールドの詳細については、『*Cisco Nexus 5000 シリーズ Command Reference*』を参照してください。

IP ACL 統計情報の表示と消去

IP ACL に関する統計情報（各ルールに一致したパケットの数など）を表示するには、**show ip access-lists** コマンドを使用します。このコマンドの出力に表示される各フィールドの詳細については、『*Cisco Nexus 5000 シリーズ Command Reference*』を参照してください。

（注）　MAC アクセス リストは、非 IPv4 および非 IPv6 トラフィックだけに適用可能です。

VACL 統計情報を表示または消去するには、次のいずれかの作業を実行します。

コマンド	目的
show ip access-lists	IP ACL の設定を表示します。IP ACL に **statistics** コマンドが指定されている場合は、**show ip access-lists** コマンドの出力に、各ルールに一致したパケットの数が表示されます。
clear ip access-list counters	すべての IP ACL、または特定の IP ACL の統計情報を消去します。

これらのコマンドの詳細については、『*Cisco Nexus 5000 シリーズ Command Reference*』を参照してください。

MAC ACL の設定

この項では、次のトピックについて取り上げます。

- MAC ACL の作成（20-10 ページ）
- MAC ACL の変更（20-11 ページ）
- MAC ACL の削除（20-12 ページ）
- MAC ACL 内のシーケンス番号の変更（20-12 ページ）
- MAC ACL のポート ACL としての適用（20-13 ページ）
- MAC ACL の VACL としての適用（20-13 ページ）
- MAC ACL の設定の確認（20-13 ページ）
- MAC ACL 統計情報の表示と消去（20-14 ページ）

MAC ACL の作成

MAC ACL を作成し、その MAC ACL にルールを追加する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`switch# mac access-list name`	MAC ACL を作成して、ACL コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-mac-acl)# {permit | deny} source destination protocol`	MAC ACL 内にルールを作成します。 **permit** オプションと **deny** オプションには、トラフィックを識別するための多くの方法が用意されています。詳細は、『*Cisco Nexus 5000 シリーズ Command Reference*』を参照してください。
ステップ 4	`switch(config-mac-acl)# statistics`	（任意）ACL に規定されたルールに一致するパケットのグローバルな統計情報をスイッチ内に保持するように指定します。
ステップ 5	`switch(config-mac-acl)# show mac access-lists name`	（任意）MAC ACL の設定を表示します。
ステップ 6	`switch(config-mac-acl)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、MAC ACL を作成して、ルールを追加する例を示します。

```
switch# configure terminal
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any
switch(config-mac-acl)# statistics
switch(config-mac-acl)# show mac access-lists acl-mac-01
switch(config-mac-acl)# copy running-config startup-config
```

MAC ACL の変更

既存の MAC ACL 内で、ルールを追加および削除できます。既存のルールは変更できません。ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの間に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。詳細については、「IP ACL 内のシーケンス番号の変更」セクション（20-7 ページ）を参照してください。

MAC ACL を変更する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# mac access-list name`	名前で指定した ACL の ACL コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-mac-acl)# [sequence-number] {permit|deny} source destination protocol`	（任意）MAC ACL 内にルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。
ステップ 4	`switch(config-mac-acl)# no {sequence-number | {permit|deny} source destination protocol}`	（任意）MAC ACL から指定したルールを削除します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。
ステップ 5	`switch(config-mac-acl)# [no] statistics`	（任意）ACL に規定されたルールに一致するパケットのグローバルな統計情報をスイッチ内に保持するように指定します。 **no** オプションを指定すると、ACL のグローバルな統計情報がスイッチ内に保持されなくなります。
ステップ 6	`switch(config-mac-acl)# show mac access-lists name`	（任意）MAC ACL の設定を表示します。
ステップ 7	`switch(config-mac-acl)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、MAC ACL を変更する例を示します。

```
switch# configure terminal
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# 100 permit mac 00c0.4f00.00 0000.00ff.ffff any
switch(config-mac-acl)# statistics
switch(config-mac-acl)# show mac access-lists acl-mac-01
switch(config-mac-acl)# copy running-config startup-config
```

MAC ACL の削除

スイッチから MAC ACL を削除できます。

ACL がインターフェイスに適用されているかどうかを確認してください。削除できるのは、現在適用されている ACL だけです。ACL を削除しても、その ACL が適用されていたインターフェイスの設定は影響を受けません。スイッチは、削除対象の ACL が空であると見なします。

MAC ACL を削除する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no mac access-list** *name*	名前で指定した MAC ACL を実行コンフィギュレーションから削除します。
ステップ 3	switch(config)# **show mac access-lists**	(任意)MAC ACL の設定を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

MAC ACL 内のシーケンス番号の変更

MAC ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。ACL にルールを挿入する必要がある場合で、シーケンス番号が不足しているときは、再割り当てすると便利です。詳細については、「ルール」セクション(20-2 ページ)を参照してください。

MAC ACL 内のルールに付けられたすべてのシーケンス番号を変更する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **resequence mac access-list** *name starting-sequence-number increment*	ACL 内に記述されているルールにシーケンス番号を付けます。starting-sequence number に指定したシーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。
ステップ 3	switch(config)# **show mac access-lists** *name*	(任意)MAC ACL の設定を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

MAC ACL のポート ACL としての適用

MAC ACL をポート ACL として、次のいずれかのインターフェイス タイプに適用できます。

- レイヤ 2 インターフェイス
- ポートチャネル インターフェイス

適用する ACL が存在しており、この適用で要求されているとおりにトラフィックをフィルタリングするように設定されていることを確認してください。MAC ACL の設定の詳細については、「IP ACL の設定」セクション（20-5 ページ）を参照してください。

MAC ACL をポート ACL として適用する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# interface ethernet slot/port`	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
	`switch(config)# interface port-channel channel-number}`	ポート チャネル インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# mac port access-group access-list`	MAC ACL をインターフェイスに適用します。
ステップ 4	`switch(config-if)# show running-config`	（任意）ACL の設定を表示します。
ステップ 5	`switch(config-if)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

MAC ACL の VACL としての適用

MAC ACL を VACL として適用できます。MAC ACL を使用して VACL を作成する方法の詳細については、「VACL の作成または変更」セクション（20-15 ページ）を参照してください。

MAC ACL の設定の確認

MAC ACL 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show mac access-lists	MAC ACL の設定を表示します。
show running-config	ACL の設定（MAC ACL と MAC ACL が適用されるインターフェイス）を表示します。
show running-config interface	ACL を適用したインターフェイスの設定を表示します。

MAC ACL 統計情報の表示と消去

MAC ACL に関する統計情報（各ルールに一致したパケットの数など）を表示するには、**show mac access-lists** コマンドを使用します。

MAC ACL 統計情報を表示または消去するには、次のいずれかの作業を実行します。

コマンド	目的
show mac access-lists	MAC ACL の設定を表示します。MAC ACL に **statistics** コマンドが指定されている場合は、**show mac access-lists** コマンドの出力に、各ルールに一致したパケットの数が表示されます。
clear mac access-list counters	すべての MAC ACL、または特定の MAC ACL の統計情報を消去します。

次に、acl-mac-01 という名前の MAC ACL を作成して、Ethernet インターフェイス 2/1（レイヤ 2 インターフェイス）に適用する例を示します。

```
mac access-list acl-mac-01
  permit 00c0.4f00.0000 0000.00ff.ffff any
interface ethernet 2/1
  mac access-group acl-mac-01
```

VLAN ACL について

VLAN ACL（VACL）は、MAC ACL または IP ACL の適用例の 1 つです。VACL を設定して、VLAN 内でブリッジされているすべてのパケットに適用できます。VACL は、セキュリティ パケットのフィルタリングだけに使用します。VACL は方向（入力または出力）で定義されることはありません。

ACL の種類と適用例の詳細については、「ACL について」セクション（20-1 ページ）を参照してください。

この項では、次のトピックについて取り上げます。

- VACL とアクセス マップ（20-14 ページ）
- VACL とアクション（20-15 ページ）
- 統計情報（20-15 ページ）

VACL とアクセス マップ

VACL では、アクセス マップを使用して、IP ACL または MAC ACL をアクションとリンクさせます。スイッチは、VACL によって許可されたパケットに設定されているアクションを実行します。

VACL とアクション

アクセス マップ コンフィギュレーション モードでは、**action** コマンドを使用して、次のいずれかのアクションを指定します。

- フォワード：スイッチの通常の動作によって決定された宛先にトラフィックを送信します。
- ドロップ：トラフィックをドロップします。

統計情報

スイッチは、VACL 内の各ルールについて、グローバルな統計情報を保持できます。VACL を複数の VLAN に適用した場合、保持されるルール統計情報は、その VACL が適用されている各インターフェイス上で一致（ヒット）したパケットの総数になります。

（注）　Cisco Nexus 5000 シリーズ スイッチでは、インターフェイス単位の VACL 統計情報はサポートしていません。

設定する各 VLAN アクセス マップごとに、VACL の統計情報をスイッチ内に保持するかどうかを指定できます。これにより、VACL によってフィルタリングされたトラフィックをモニタリングするため、あるいは VLAN アクセス マップの設定のトラブルシューティングを行うために、VACL 統計情報の収集のオン/オフを必要に応じて切り替えることができます。

VACL 統計情報の表示の詳細については、「IP ACL 統計情報の表示と消去」セクション（20-9 ページ）を参照してください。

VACL の設定

この項では、次のトピックについて取り上げます。

- VACL の作成または変更（20-15 ページ）
- VACL の削除（20-16 ページ）
- VACL の VLAN への適用（20-17 ページ）
- VACL の設定の確認（20-17 ページ）
- VACL 統計情報の表示と消去（20-17 ページ）

VACL の作成または変更

VACL を作成または変更できます。VACL の作成には、IP ACL または MAC ACL を、一致したトラフィックに適用するアクションとアソシエートさせるアクセス マップの作成が含まれます。

VACL を作成または変更する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **vlan access-map** *map-name*	指定したアクセス マップのアクセス マップ コンフィギュレーション モードを開始します。
ステップ 3	switch(config-access-map)# **match ip address** *ip-access-list*	マップの IPv4 および IPV6 ACL を指定します。
	switch(config-access-map)# **match mac address** *mac-access-list*	マップの MAC ACL を指定します。
ステップ 4	switch(config-access-map)# **action** {**drop**|**forward** }	スイッチが、ACL に一致したトラフィックに適用するアクションを指定します。
ステップ 5	switch(config-access-map)# [**no**] **statistics**	(任意)VACL に規定されたルールに一致するパケットのグローバルな統計情報をスイッチ内に保持するように指定します。 **no** オプションを指定すると、VACL のグローバルな統計情報がスイッチ内に保持されなくなります。
ステップ 6	switch(config-access-map)# **show running-config**	(任意)ACL の設定を表示します。
ステップ 7	switch(config-access-map)# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

VACL の削除

VACL を削除できます。これにより、VLAN アクセス マップも削除されます。

VACL が VLAN に適用されているかどうかを確認してください。削除できるのは、現在適用されている VACL だけです。VACL を削除しても、その VACL が適用されていた VLAN の設定は影響を受けません。スイッチは、削除対象の VACL が空であると見なします。

VACL を削除する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no vlan access-map** *map-name*	指定したアクセス マップの VLAN アクセス マップの設定を削除します。
ステップ 3	switch(config)# **show running-config**	(任意)ACL の設定を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

VACL の VLAN への適用

VACL を VLAN に適用できます。VACL ドロップダウン リストが [Advanced Settings] セクションに表示されます。

VACL を VLAN に適用する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# [no] vlan filter map-name vlan-list list`	指定したリストによって、VACL を VLAN に適用します。**no** を使用すると、VACL の適用が解除されます。 vlan-list コマンドで指定できる VLAN は最大 32 個ですが、複数の vlan-list コマンドを設定すると、32 個を超える VLAN を指定できます。
ステップ 3	`switch(config)# show running-config`	(任意)ACL の設定を表示します。
ステップ 4	`switch(config)# copy running-config startup-config`	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

VACL の設定の確認

VACL 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show running-config aclmgr	VACL 関連の設定を含む、ACL の設定を表示します。
show vlan filter	VLAN に適用されている VACL の情報を表示します。
show vlan access-map	VLAN アクセス マップに関する情報を表示します。

VACL 統計情報の表示と消去

VACL 統計情報を表示または消去するには、次のいずれかの作業を実行します。

コマンド	目的
show vlan access-list	VACL の設定を表示します。VLAN アクセス マップに **statistics** コマンドが指定されている場合は、**show vlan access-list** コマンドの出力に、各ルールに一致したパケットの数が表示されます。
clear vlan access-list counters	すべての VACL、または特定の VACL の統計情報を消去します。

次に、acl-ip-01 という名前の IP ACL によって許可されたトラフィックを転送するように VACL を設定し、その VACL を VLAN 50 ～ 82 に適用する例を示します。

```
configure terminal
vlan access-map acl-ip-map
  match ip address acl-ip-01
  action forward
vlan filter acl-ip-map vlan-list 50-82
```

デフォルト設定

表 20-2 に、IP ACL パラメータのデフォルト設定を示します。

表 20-2　IP ACL のデフォルト パラメータ

パラメータ	デフォルト
IP ACL	デフォルトの IP ACL は存在しません。
ACL ルール	すべての ACL に暗黙のルールが適用されます。 「暗黙のルール」セクション（20-3 ページ）を参照してください。

表 20-3 に、MAC ACL パラメータのデフォルト設定値を示します。

表 20-3　MAC ACL のデフォルト パラメータ

パラメータ	デフォルト
MAC ACL	デフォルトの MAC ACL は存在しません。
ACL ルール	すべての ACL に暗黙のルールが適用されます。 「暗黙のルール」セクション（20-3 ページ）を参照してください。

表 20-4 に、VACL パラメータのデフォルト設定値を示します。

表 20-4　デフォルトの VACL パラメータ

パラメータ	デフォルト
VACL	デフォルトの IP ACL は存在しません。
ACL ルール	すべての ACL に暗黙のルールが適用されます。 「暗黙のルール」セクション（20-3 ページ）を参照してください。

CHAPTER 21

CFS の使用

Cisco Nexus 5000 シリーズ スイッチは、Cisco Fabric Services（CFS）機能を備えています。この機能は、構成情報をネットワーク内のすべてのスイッチに自動的に配信して、プロビジョニングを簡素化します。

スイッチ機能は CFS インフラストラクチャを使用して、機能が必要とする機能データまたは設定データを配信します。

この章の内容は、次のとおりです。

- CFS について（21-1 ページ）
- CFS 配信（21-2 ページ）
- アプリケーションの CFS サポート（21-6 ページ）
- CFS リージョン（21-10 ページ）
- IP を介した CFS の設定（21-13 ページ）
- CFS 配信情報の表示（21-15 ページ）
- デフォルト設定（21-17 ページ）

CFS について

Cisco Nexus 5000 シリーズ スイッチの一部の機能は、正常に動作するため、ネットワーク内の他のスイッチとの設定の同期化を必要とします。ネットワーク内のスイッチごとに手動設定によって同期化を行うことは、面倒で、エラーが発生しやすくなります。

CFS はネットワーク内の自動設定同期化に対して共通のインフラストラクチャを提供します。また、トランスポート機能、および機能に対する共通サービスのセットを提供します。CFS にはネットワーク内の CFS 対応スイッチを検出する機能が備わっており、すべての CFS 対応スイッチの機能能力を検出できます。

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

CFS には次の機能があります。

- CFS レイヤでクライアント/サーバ関係を持たないピアツーピア プロトコル
- ファイバ チャネル、IPv4、または IPv6 ネットワークを介した CFS メッセージ配信

- 3 つの配信モード
  - 協調型配信：ネットワーク内でいつでも使用できる配信は 1 つだけです。
  - 非協調型配信：協調型配信が実行中の場合を除き、ネットワーク内で複数の同時配信を使用できます。
  - 無制限の非協調型配信：既存の協調型配信がある場合にネットワーク内で複数の同時配信が許可されます。無制限の非協調型配信は、他のすべての配信タイプの配信と同時に実行できます。

IP を介した CFS 配信では、次の機能がサポートされます。

- IP ネットワークを介した配信の 1 つの範囲：
  - 物理範囲：IP ネットワーク全体に配信されます。

ファイバ チャネル SAN を介した CFS 配信では、次の機能がサポートされます。

- SAN ファブリックを介した配信の 3 つの範囲：
  - 論理範囲：VSAN の範囲内で配信されます。
  - 物理範囲：物理トポロジ全体に配信されます。
  - 選択した VSAN セット間：一部の機能では、特定の VSAN 間で設定配信を必要とします。これらの機能では、CFS に対して、配信を制限する VSAN のセットを指定できます。
- ファブリックの結合イベント時（2 つの独立したファブリックが結合する場合）に機能設定の結合を実現する結合プロトコルのサポート

CFS 配信

CFS 配信機能は、下位層の転送とは無関係です。Cisco Nexus 5000 シリーズ スイッチは、IP を介した CFS 配信とファイバ チャネル上の CFS 配信をサポートします。CFS を使用する機能は、下位層の転送を認識しません。

その他の詳細については、次の項で説明します。

- CFS の配信モード（21-2 ページ）
- スイッチの CFS 配信のイネーブル化/ディセーブル化（21-3 ページ）
- CFS 配信ステータスの確認（21-4 ページ）
- IP を介した CFS 配信（21-4 ページ）
- ファイバ チャネルを介した CFS 配信（21-5 ページ）
- CFS 配信の範囲（21-5 ページ）
- CFS 結合のサポート（21-6 ページ）

CFS の配信モード

CFS では異なる機能要件をサポートするために、3 つの配信モードをサポートします。常に 1 つのモードだけを適用できます。CFS 配信モードについては、次の項で説明します。

- 非協調型配信（21-3 ページ）
- 協調型配信（21-3 ページ）
- 無制限の非協調型配信（21-3 ページ）

非協調型配信

非協調型配信は、ピアからの情報と競合させたくない情報を配信する場合に使用されます。1 つの機能に対して非協調的な並列配信を適用できます。

協調型配信

協調型配信は、いかなる時も 1 つの機能配信だけ適用できます。CFS はロックを使用してこの機能を実行します。ネットワーク内のいずれかの機能でロックが取得されていれば、協調型配信は開始できません。協調型配信は、次の 3 段階で構成されています。

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

協調型配信には、次の 2 種類があります。

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

  協調型配信は、複数のスイッチから操作および配信が可能な情報を配信するのに使用されます。たとえば、ポート セキュリティの設定です。

無制限の非協調型配信

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

スイッチの CFS 配信のイネーブル化/ディセーブル化

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

物理接続を維持したまま、スイッチ上で CFS をグローバルにディセーブルにし、ネットワーク全体の配信から CFS を使用する機能を隔離できます。スイッチ上で CFS がグローバルにディセーブルにされている場合、CFS 動作はそのスイッチに限定されます。

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

	コマンド	目的
ステップ 1	`switch#` **`configure`** `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`no cfs distribute`**	スイッチ上のすべてのアプリケーションに対して、CFS配信（ファイバ チャネル または IP を介した CFS）をグローバルにディセーブルにします。
	`switch(config)#` **`cfs distribute`**	スイッチの CFS 配信をイネーブルにします（デフォルト）。

CFS 配信ステータスの確認

show cfs status コマンドを実行すると、スイッチの CFS 配信ステータスが表示されます。

```
switch# show cfs status
Distribution : Enabled
Distribution over IP : Disabled
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4653
```

IP を介した CFS 配信

IP を介した CFS 配信は次の機能をサポートしています。

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

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

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

（注） CFS は同じスイッチから IPv4 と IPv6 の両方を介しては配信できません。

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

図 21-1 に、ファイバ チャネル接続と IP 接続の両方を持つネットワークを示します。ノード A はファイバ チャネルを介してノード B にイベントを転送します。ノード B はユニキャスト IP を使用してノード C とノード D にイベントを転送します。ノード C はファイバ チャネルを介してノード E にイベントを転送します。

図 21-1　ファイバ チャネル接続と IP 接続を持つネットワーク例 1

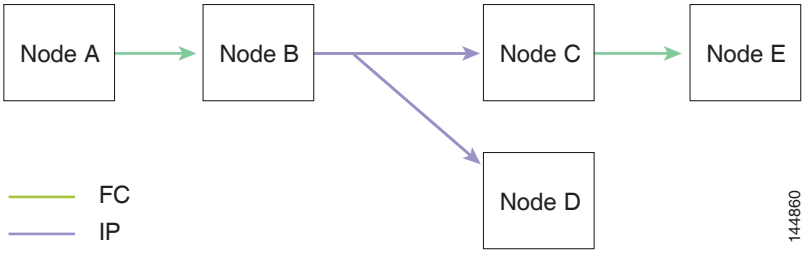


図 21-2 は、ノード C とノード D がファイバ チャネルを使用して接続されていることを除き、図 21-1 と同じです。ノード B にはノード C とノード D の IP 用配信リストがあるので、この例のすべてのプロセスは同じです。ノード D はすでにノード B からの配信リストに入っているため、ノード C はノード D に転送しません。

図 21-2　ファイバ チャネル接続と IP 接続を持つネットワーク例 2

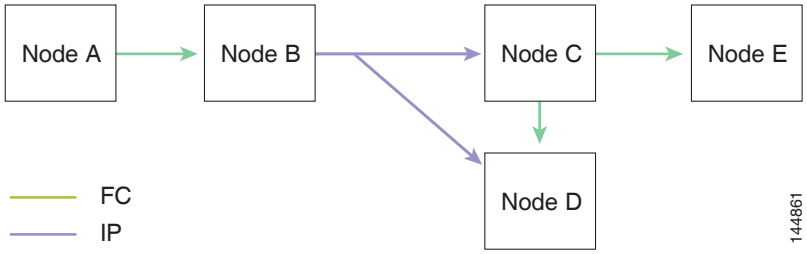
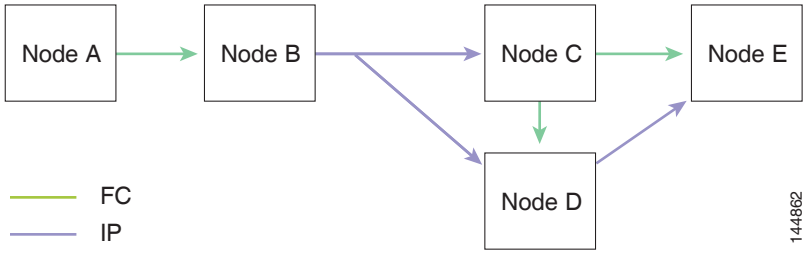


図 21-3 は、ノード D とノード E が IP を使用して接続されていることを除き、図 21-2 と同じです。ノード E はノード B からの配信リストに入っていないため、ノード C とノード D はイベントをノード E に転送します。

図 21-3　ファイバ チャネル接続と IP 接続を持つネットワーク例 3



ファイバ チャネルを介した CFS 配信

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

CFS 配信の範囲

Cisco Nexus 5000 シリーズ スイッチの各種アプリケーションは、次のさまざまなレベルで設定を配信する必要があります。ファイバ チャネルを介した CFS 配信を使用する場合、次のレベルが使用できます。

- VSAN レベル（論理スコープ）

  VSAN の範囲内で動作するアプリケーションは、設定の配信が VSAN に限定されます。アプリケーション例は、VSAN 内だけでコンフィギュレーション データベースを適用できる場合のポート セキュリティです。

（注）　IP を介した CFS 配信では、論理範囲はサポートされません。

- 物理トポロジ レベル（物理スコープ）

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

  一部のアプリケーションはネットワーク内の選択したスイッチ間でだけ動かせます。

CFS 結合のサポート

CFS 結合は、ファイバ チャネルを介した CFS 配信でサポートされます。

アプリケーションは、CFS を通じて SAN ファブリック内の同期化された設定を保ちます。このような 2 つのファブリック間で ISL を起動すると、これらのファブリックがマージされることがあります。これらの 2 つのファブリック内の設定情報セットが異なっている時は、マージ イベント中に調停する必要があります。CFS は、アプリケーション ピアがオンラインになるたびに通知を送信します。M のアプリケーション ピアを持つファブリックが N のアプリケーション ピアを持つ別のファブリックと結合し、アプリケーションが通知のたびに結合アクションを行うと、リンク アップ イベントがファブリック内の M*N 結合をもたらします。

CFS は、CFS レイヤでマージの複雑性に対処することで必要とされるマージ数を 1 つに減らすプロトコルをサポートしています。このプロトコルは、スコープ単位でアプリケーションごとに稼働します。プロトコルには、ファブリックのマージ マネージャとしてそのファブリック内から 1 つのスイッチを選択する作業が伴います。他のスイッチは、結合プロセスにおいて役割を担いません。

マージ時、2 つのファブリック内のマージ マネージャは相互にコンフィギュレーション データベースを交換します。一方のアプリケーションが情報をマージし、マージが正常に行われたかどうかを判断し、結合されたファブリック内のすべてのスイッチにマージ ステータスを通知します。

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

アプリケーションの CFS サポート

ここでは、アプリケーションをサポートする CFS 機能について説明します。

- CFS のアプリケーション要件（21-7 ページ）
- アプリケーションに対する CFS のイネーブル化（21-7 ページ）
- ネットワークのロック（21-8 ページ）
- 変更のコミット（21-9 ページ）
- 変更の廃棄（21-9 ページ）
- コンフィギュレーションの保存（21-9 ページ）
- ロック済みセッションのクリア（21-10 ページ）

CFS のアプリケーション要件

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

CFS には、次の要件があります。

- CFS の暗黙的な使用：CFS 対応アプリケーションの CFS 作業を初めて行う場合、設定変更プロセスが開始され、アプリケーションがネットワークをロックします。
- 保留データベース：保留データベースはコミットされていない情報を保持する一時的なバッファです。データベースが、ネットワーク内の他のスイッチのデータベースと確実に同期するために、コミットされていない変更はすぐには適用されません。変更をコミットすると、保留データベースはコンフィギュレーション データベース（別名、アクティブ データベースまたは有効データベース）を上書きします。
- アプリケーション単位でイネーブル化またはディセーブル化される CFS 配信：CFS 配信ステートのデフォルト（イネーブルまたはディセーブル）は、アプリケーション間で異なります。アプリケーションで CFS の配信がディセーブルにされている場合、そのアプリケーションは設定を配信せず、またネットワーク内の他のスイッチからの配信も受け入れません。
- 明示的な CFS コミット - 大半のアプリケーションでは、新しいデータベースをネットワークに配信したりネットワーク ロックを解除したりするために、一時的なバッファ内の変更をアプリケーション データベースにコピーする明示的なコミット操作が必要です。コミット操作を実行しないと、一時的バッファ内の変更は適用されません。

アプリケーションに対する CFS のイネーブル化

すべての CFS ベースのアプリケーションでは、配信機能をイネーブルまたはディセーブルにできます。

アプリケーションでは、配信はデフォルトでイネーブルにされています。

アプリケーションで配信が明示的にイネーブルにされていない場合は、CFS はそのアプリケーションの設定を配信しません。

アプリケーション登録スターテスの確認

show cfs application コマンドは、CFS に現在登録されているアプリケーションを表示します。最初のカラムには、アプリケーション名が表示されます。2 番めのカラムは、アプリケーションの配信がイネーブルであるかディセーブルであるかを示します（enabled または disabled）。最後のカラムは、アプリケーションの配信範囲を示します（論理、物理、またはその両方）。

（注）　**show cfs application** コマンドは、CFS に登録されているアプリケーションを表示するだけです。CFS を使用するコンディショナル サービスは、これらのサービスが稼働していなければ出力には示されません。

```
switch# show cfs application

----------------------------------------------
 Application    Enabled   Scope
----------------------------------------------
 ntp            No        Physical-all
 fscm           Yes       Physical-fc
```

```
 rscn           No        Logical
 fctimer        No        Physical-fc
 syslogd        No        Physical-all
 callhome       No        Physical-all
 fcdomain       Yes       Logical
 device-alias   Yes       Physical-fc

Total number of entries = 8
```

show cfs application name コマンドは、特定のアプリケーションの詳細を表示します。表示されるのは、イネーブル/ディセーブル ステート、CFS に登録されているタイムアウト、結合可能であるか（結合のサポートに対して CFS に登録されているか）、と配信範囲です。

```
switch# show cfs application name fscm

Enabled        : Yes
 Timeout        : 100s
 Merge Capable  : No
 Scope          : Physical-fc
```

ネットワークのロック

CFS インフラストラクチャを使用する機能（またはアプリケーション）を初めて設定する場合、この機能は CFS セッションを開始して、ネットワークをロックします。ネットワークがロックされた場合、この機能への設定変更は、スイッチ ソフトウェアにより、ロックを保持しているスイッチだけから行えます。別のスイッチから機能への設定変更を行う場合、ロックされているステータスを知らせるメッセージが、スイッチから発行されます。設定変更は、該当アプリケーションによって保留データベースに保持されます。

ネットワーク ロックを要求する CFS セッションを開始し、セッションを終了するのを忘れた場合は、管理者がそのセッションをクリアできます。ネットワークをロックしたユーザの名前は、再起動およびスイッチオーバーを行っても保持されます。（同じマシン上で）別のユーザが設定タスクを実行しようとしても、拒否されます。

CFS ロック ステータスの確認

show cfs lock コマンドを実行すると、アプリケーションによって現在取得されているすべてのロックが表示されます。このコマンドにより、アプリケーションごとにアプリケーション名とロックの取得範囲が表示されます。アプリケーション ロックが物理範囲で取得されている場合、このコマンドはスイッチ WWN、IP アドレス、ユーザ名、およびロック所有者のユーザ タイプを表示します。アプリケーションが論理範囲で取得されている場合、このコマンドはロックが取得された VSAN、ドメイン、IP アドレス、ユーザ名、およびロック所持者のユーザ タイプを表示します。

```
switch# show cfs lock

Application: ntp
Scope      : Physical
-------------------------------------------------------------------
 Switch WWN               IP Address       User Name    User Type
-------------------------------------------------------------------
 20:00:00:05:30:00:6b:9e  10.76.100.167    admin        CLI/SNMP v3
 Total number of entries = 1

Application: port-security
Scope      : Logical
-----------------------------------------------------------
```

```
 VSAN   Domain   IP Address       User Name    User Type
-----------------------------------------------------------
 1      238      10.76.100.167    admin        CLI/SNMP v3
 2      211      10.76.100.167    admin        CLI/SNMP v3
 Total number of entries = 2
```

show cfs lock name コマンドは、指定したアプリケーションで使用されているロックの詳細情報を表示します。

```
switch# show cfs lock name ntp
Scope      : Physical
-------------------------------------------------------------------
 Switch WWN               IP Address       User Name    User Type
-------------------------------------------------------------------
 20:00:00:05:30:00:6b:9e  10.76.100.167    admin        CLI/SNMP v3

 Total number of entries = 1
```

変更のコミット

コミット操作により、すべてのアプリケーション ピアの保留データベースを保存し、すべてのスイッチのロックを解除します。

一般に、コミット機能はセッションを開始しません。セッションを開始するのは、ロック機能だけです。ただし、設定変更がこれまでに行われていなければ、空のコミットが可能です。この場合、コミット操作の結果として、ロックを取得し、現在のデータベースを配信するセッションが行われます。

CFS インフラストラクチャを使用して機能への設定変更をコミットすると、次のいずれかの応答に関する通知が届きます。

- 1 つまたは複数の外部スイッチが正常なステータスを報告する場合 - アプリケーションは変更をローカルに適用し、ネットワーク ロックを解除します。
- どの外部スイッチも成功ステートを報告しない - アプリケーションはこのステートを失敗として認識し、ネットワーク内のどのスイッチにも変更を適用しません。ネットワーク ロックは解除されません。

commit コマンドを入力すると、指定した機能の変更をコミットできます。

変更の廃棄

設定変更を廃棄すると、アプリケーションは保留中のデータベースを一気に消去し、ネットワーク内のロックを解除します。中断およびコミット機能の両方を使用できるのは、ネットワーク ロックが取得されたスイッチだけです。

abort コマンドを入力すると、指定した機能の変更を廃棄できます。

コンフィギュレーションの保存

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

注意　変更内容は、コミットしなければ、実行コンフィギュレーションに保存されません。

CISCO-CFS-MIB には CFS 関連機能の SNMP 設定情報が含まれます。この MIB（管理情報ベース）の詳細については、『*Cisco Nexus 5000 シリーズ MIB Quick Reference*』を参照してください。

ロック済みセッションのクリア

ネットワーク内の任意のスイッチからアプリケーションが保持しているロックをクリアすると、ロックが取得されているにもかかわらず解除されていない状態から回復できます。この機能には、Admin 権限が必要になります。

注意　この機能を使用してネットワーク内のロックを解除する場合は、注意が必要です。ネットワーク内の任意のスイッチの保留中設定がフラッシュされ、内容が失われます。

CFS リージョン

ここでは、次の内容について説明します。

- CFS リージョンの概要（21-10 ページ）
- シナリオ例（21-10 ページ）
- CFS リージョンの管理（21-11 ページ）

CFS リージョンの概要

CFS リージョンは、物理配信範囲の所定の機能またはアプリケーションに対するスイッチのユーザ定義のサブセットです。ネットワークが広い範囲に及ぶ場合、物理的なプロキシミティに基づくスイッチ セット間での特定のプロファイルの配信を、（場合によって）ローカライズまたは制限する必要があります。CFS リージョンを使用すると、ネットワーク内で特定の CFS 機能またはアプリケーションに、配信の複数アイランドができます。CFS リージョンは、機能設定の配信をネットワーク内のスイッチの特定のセットまたはグループに制限するよう設計されています。

（注）　CFS リージョンの設定は、物理スイッチだけで行えます。CFS リージョンの設定は、VSAN では行えません。

シナリオ例

Call Home アプリケーションは、困難な状況、あるいは異常が発生した時にネットワーク管理者にアラートを送信します。ネットワークが広い地域に及び、複数のネットワーク管理者がネットワーク内のスイッチの各サブセットを担当している場合は、Call Home アプリケーションは、場所に関係なく、すべてのネットワーク管理者にアラートを送信します。Call Home アプリケーションでメッセージ アラートを、選択したネットワーク管理者に送信するには、CFS リージョンを実装してアプリケーションの物理範囲を微調整するか、絞り込む必要があります。

CFS リージョンは、0 ～ 200 の数字で識別されます。リージョン 0 はデフォルト リージョンとして予約されており、ネットワーク内のすべてのスイッチを含みます。1 ～ 200 のリージョンを設定できます。デフォルト リージョンでは下位互換性を維持しています。

機能が移動される、つまり、機能が新しいリージョンに割り当てられると、機能のスコープはそのリージョンに制限されます。他のすべてのリージョンは、配信やマージの対象から外されます。機能へのリージョンの割り当ては、配信において初期の物理スコープよりも優先されます。

複数の機能の設定を配信するように CFS リージョンを設定できます。ただし、特定のスイッチでは、一度に特定の機能設定を配信するように設定できる CFS リージョンは 1 つだけです。機能を CFS リージョンに割り当てた場合、この設定を別の CFS リージョン内に配信できません。

CFS リージョンの管理

ここでは、CFS リージョンの管理方法について説明します。次のタスクを実行するには、コマンド セットを使用します。

- CFS リージョンの作成（21-11 ページ）
- CFS リージョンへのアプリケーションの割り当て（21-11 ページ）
- 別の CFS リージョンへのアプリケーションの移動（21-12 ページ）
- リージョンからのアプリケーションの削除（21-12 ページ）
- CFS リージョンの削除（21-12 ページ）

CFS リージョンの作成

CFS リージョンを作成する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configure`** `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`cfs region`** *`region-id`*	リージョンを作成します。

CFS リージョンへのアプリケーションの割り当て

スイッチでリージョンにアプリケーションを割り当てる手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configure`** `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`cfs region`** *`region-id`*	リージョンを作成します。
ステップ 3	`switch(config-cfs-region)#` **`ntp`** `switch(config-cfs-region)#` **`callhome`**	アプリケーションを追加します。

別の CFS リージョンへのアプリケーションの移動

たとえば、NTP および Call Home アプリケーションが割り当てられているリージョン 1（元のリージョン）からリージョン 2（ターゲット リージョン）にアプリケーションを移動する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# cfs region region-id`	CFS リージョン サブモードを開始します。
ステップ 3	`switch(config-cfs-region)# ntp` `switch(config-cfs-region)# callhome`	元々リージョン 1 に属していたアプリケーションをリージョン 2 に移動するよう指定します。たとえば、ここでは、NTP および Call Home アプリケーションをリージョン 2 に移動します。

（注）　同じリージョンにアプリケーションを複数回追加しようとすると、「Application already present in the same region.」というエラー メッセージが表示されます。

リージョンからのアプリケーションの削除

リージョンからのアプリケーションの削除は、アプリケーションをデフォルト リージョンのリージョン 0 に戻す場合と同じです。したがって、ネットワーク全体がアプリケーションの配信の範囲になります。

リージョンからアプリケーションを削除する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# cfs region region-id`	CFS リージョン サブモードを開始します。
ステップ 3	`switch(config-cfs-region)# no ntp` `switch(config-cfs-region)# no callhome`	リージョンに属しているアプリケーションを削除します。

CFS リージョンの削除

リージョンの削除とは、リージョン定義を取り消すことです。リージョンを削除すると、リージョンによってバインドされているすべてのアプリケーションが解除されてデフォルト リージョンに戻ります。

たとえば、リージョン番号 4 というリージョンを削除する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# no cfs region region-id`	リージョンを削除します。

（注）　手順 2 のあとに、「All the applications in the region will be moved to the default region.」という警告が表示されます。

IP を介した CFS の設定

ここでは、IP を介した CFS の設定について説明します。

- IP を介した CFS のイネーブル化（21-13 ページ）
- IP を介した CFS 設定の確認（21-14 ページ）
- IP を介した CFS の IP マルチキャスト アドレスの設定（21-14 ページ）
- IP を介した CFS の IP マルチキャスト アドレス設定の確認（21-15 ページ）

IP を介した CFS のイネーブル化

（注）　CFS は同じスイッチから IPv4 と IPv6 の両方を介しては配信できません。

IPv4 を介した CFS をイネーブルまたはディセーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# cfs ipv4 distribute`	スイッチのすべてのアプリケーションに対して IPv4 を介した CFS をグローバルでイネーブルにします。
	`switch(config)# no cfs ipv4 distribute`	スイッチの IPv4 を介した CFS をディセーブルにします（デフォルト）。

IPv6 を介した CFS をイネーブルまたはディセーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# cfs ipv6 distribute`	スイッチのすべてのアプリケーションに対して IPv6 を介した CFS をグローバルでイネーブルにします。
	`switch(config)# no cfs ipv6 distribute`	スイッチの IPv6 を介した CFS をディセーブルにします（デフォルト）。

IP を介した CFS 設定の確認

IP を介した CFS 設定を確認するには、**show cfs status** コマンドを使用します。

```
switch# show cfs status
Distribution : Enabled
Distribution over IP : Enabled - mode IPv4
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4653
```

IP を介した CFS の IP マルチキャスト アドレスの設定

類似のマルチキャスト アドレスを持つ IP を介した CFS 対応スイッチのすべては、IP ネットワークを介した 1 つの CFS を形成します。ネットワーク トポロジ変更を検出するためのキープアライブ メカニズムのような CFS プロトコル特有の配信は、IP マルチキャスト アドレスを使用して情報を送受信します。

（注） アプリケーション データの CFS 配信はダイレクト ユニキャストを使用します。

IP を介した CFS の IPv4 または IPv6 どちらかのマルチキャスト アドレス値を設定できます。デフォルトの IPv4 マルチキャスト アドレスは 239.255.70.83 で、デフォルトの IPv6 マルチキャスト アドレスは ff13:7743:4653 です。

IPv4 を介した CFS の IP マルチキャスト アドレスを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure` `switch(config)#`	コンフィギュレーション モードに入ります。

ステップ 2	`switch(config)# cfs ipv4 mcast-address ipv4-address`
	`Distribution over this IP type will be affected`
	`Change multicast address for CFS-IP ?`
	`Are you sure? (y/n)  [n] y`
		IPv4 を介した CFS 配信の IPv4 マルチキャスト アドレスを設定します。有効な IPv4 アドレスの範囲は 239.255.0.0 ～ 239.255.255.255 および 239.192/16 ～ 239.251/16 です。

	`switch(config)# no cfs ipv4 mcast-address ipv4-address`
	`Distribution over this IP type will be affected`
	`Change multicast address for CFS-IP ?`
	`Are you sure? (y/n)  [n] y`
		IPv4 を介した CFS 配信の デフォルトの IPv4 マルチキャスト アドレスに戻します。CFS のデフォルトの IPv4 マルチキャスト アドレスは 239.255.70.83 です。

IPv6 を介した CFS の IP マルチキャスト アドレスを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure** switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **cfs ipv6 mcast-address** *ipv6-address* Distribution over this IP type will be affected Change multicast address for CFS-IP ? Are you sure? (y/n) [n] **y**	IPv6 を介した CFS 配信の IPv6 マルチキャスト アドレスを設定します。有効な IPv6 アドレスの範囲は ff15::/16（ff15::0000:0000 ～ ff15::ffff:ffff）および ff18::/16（ff18::0000:0000 ～ ff18::ffff:ffff）です。
	switch(config)# **no cfs ipv6 mcast-address** *ipv6-address* Distribution over this IP type will be affected Change multicast address for CFS-IP ? Are you sure? (y/n) [n] **y**	IPv6 を介した CFS 配信のデフォルトの IPv6 マルチキャスト アドレスに戻します。IP を介した CFS のデフォルトの IPv6 マルチキャスト アドレスは ff15::efff:4653 です。

IP を介した CFS の IP マルチキャスト アドレス設定の確認

IP を介した CFS の IP マルチキャスト アドレス設定を確認するには、**show cfs status** コマンドを使用します。

```
switch# show cfs status
Fabric distribution Enabled
IP distribution Enabled mode ipv4
IPv4 multicast address : 10.1.10.100
IPv6 multicast address : ff13::e244:4754
```

CFS 配信情報の表示

show cfs merge status name コマンドを実行すると、指定したアプリケーションの結合ステータスが表示されます。次に、論理範囲内のアプリケーション配信の出力例を示します。この例は、スイッチ上のすべての有効な VSAN におけるマージ ステータスを示しています。コマンドの出力は、結合ステータスを Success、Waiting、Failure、または In Progress のいずれかで示します。結合が正常に行われた場合は、ネットワーク内のすべてのスイッチがローカル ネットワークの下に表示されます。結合が失敗した場合、結合が進行中である場合は、結合に関わったローカル ネットワークとリモート ネットワークが別個に表示されます。各ネットワーク内の結合で主体となったアプリケーション サーバには、Merge Master の用語が表示されます。

```
switch# show cfs merge status name port-security

Logical [VSAN 1] Merge Status: Failed
Local Fabric
----------------------------------------------------------------
 Domain Switch WWN               IP Address
----------------------------------------------------------------
 238    20:00:00:05:30:00:6b:9e  10.76.100.167   [Merge Master]

Remote Fabric
----------------------------------------------------------------
 Domain Switch WWN               IP Address
----------------------------------------------------------------
 236    20:00:00:0e:d7:00:3c:9e  10.76.100.169    [Merge Master]
```

```
Logical [VSAN 2] Merge Status: Success
Local Fabric
----------------------------------------------------------------
 Domain Switch WWW               IP Address
----------------------------------------------------------------
 211    20:00:00:05:30:00:6b:9e  10.76.100.167    [Merge Master]
 1      20:00:00:0e:d7:00:3c:9e  10.76.100.169

Logical [VSAN 3] Merge Status: Success
Local Fabric
----------------------------------------------------------------
 Domain Switch WWW               IP Address
----------------------------------------------------------------
 221    20:00:00:05:30:00:6b:9e  10.76.100.167    [Merge Master]
 103    20:00:00:0e:d7:00:3c:9e  10.76.100.169
```

次の**show cfs merge status name** コマンドの出力例は、物理範囲において結合が失敗したアプリケーションを示します。このコマンドは、指定されたアプリケーション名を使用し、アプリケーション範囲に基づいた結合ステータスを表示します。

```
switch# show cfs merge status name ntp

Physical  Merge Status: Failed
Local Fabric
-------------------------------------------------------
 Switch WWW               IP Address
-------------------------------------------------------
 20:00:00:05:30:00:6b:9e  10.76.100.167    [Merge Master]

Remote Fabric
-------------------------------------------------------
 Switch WWW               IP Address
-------------------------------------------------------
 20:00:00:0e:d7:00:3c:9e  10.76.100.169    [Merge Master]
```

show cfs peers コマンドの出力例は、物理ネットワーク内のすべてのスイッチをスイッチ WWN および IP アドレスの観点から表示します。ローカル スイッチには Local が表示されます。

```
switch# show cfs peers

Physical Fabric
-------------------------------------------------
 Switch WWW               IP Address
-------------------------------------------------
 20:00:00:05:30:00:6b:9e  10.76.100.167   [Local]
 20:00:00:0e:d7:00:3c:9e  10.76.100.169

 Total number of entries = 2
```

show cfs peers name コマンドは、特定のアプリケーションが CFS に登録されているすべてのピアを表示します。コマンド出力には、アプリケーション範囲に応じて物理範囲のすべてのピア、またはスイッチ上の有効な各 VSAN のすべてのピアが表示されます。物理範囲では、すべてのピアのスイッチ WWW が表示されます。ローカル スイッチには Local が表示されます。

```
switch# show cfs peers name ntp

Scope      : Physical
-------------------------------------------------
Switch WWW               IP Address
-------------------------------------------------
20:00:00:44:22:00:4a:9e  172.22.92.27    [Local]
20:00:00:05:30:01:1b:c2  172.22.92.215
```

次の **show cfs peers name** コマンドの出力例は、すべてのアプリケーション ピアを表示します（アプリケーションが登録されているすべてのスイッチ）。ローカル スイッチには Local が表示されます。

```
switch# show cfs peers name port-security
Scope      : Logical [VSAN 1]
--------------------------------------------------------------
Domain   Switch WWN               IP Address
--------------------------------------------------------------
124      20:00:00:44:22:00:4a:9e  172.22.92.27    [Local]
98       20:00:00:05:30:01:1b:c2  172.22.92.215

Total number of entries = 2


Scope      : Logical [VSAN 3]
--------------------------------------------------------------
Domain   Switch WWN               IP Address
--------------------------------------------------------------
224      20:00:00:44:22:00:4a:9e  172.22.92.27    [Local]
151      20:00:00:05:30:01:1b:c2  172.22.92.215

Total number of entries = 2
```

デフォルト設定

表 21-1 に、CFS 設定のデフォルト設定値を示します。

表 21-1　デフォルトの CFS パラメータ

パラメータ	デフォルト
スイッチでの CFS 配信	イネーブル
データベース変更	最初の設定変更によって暗黙的にイネーブルにされる
アプリケーションの配信	アプリケーションごとに異なる
コミット	明示的な設定が必要
IP を介した CFS	ディセーブル
IPv4 マルチキャスト アドレス	239.255.70.83
IPv6 マルチキャスト アドレス	ff15::efff:4653

CHAPTER 22

ユーザ アカウントと RBAC の設定

この章では、Nexus 5000 シリーズ スイッチ上でユーザ アカウントおよびロールベース アクセス コントロール（RBAC）を設定する手順について説明します。

この章は、次の項で構成されています。

- ユーザ アカウントと RBAC の概要（22-1 ページ）
- 注意事項および制約事項（22-4 ページ）
- ユーザ アカウントの設定（22-4 ページ）
- RBAC の設定（22-5 ページ）
- ユーザ アカウントと RBAC の設定の確認（22-9 ページ）
- ユーザ アカウントと RBAC 設定の例（22-10 ページ）
- デフォルト設定（22-10 ページ）

ユーザ アカウントと RBAC の概要

ユーザ アカウントの作成および管理を行い、Nexus 5000 シリーズ スイッチ上で実行できる操作を制限するロールを割り当てることができます。RBAC は、ユーザが実行する必要のある管理操作の許可を制限するロールの割り当てのルールを定義することを可能にします。

この項では、次のトピックについて取り上げます。

- ユーザ アカウントについて（22-1 ページ）
- 強力なパスワードの特性（22-2 ページ）
- ユーザ ロールについて（22-2 ページ）
- 規則について（22-3 ページ）
- ユーザ ロール ポリシーについて（22-3 ページ）

ユーザ アカウントについて

ヒント bin、daemon、adm、lp、sync、shutdown、halt、mail、news、uucp、operator、games、gopher、ftp、nobody、nscd、mailnull、rpc、rpcuser、xfs、gdm、mtsuser、ftpuser、man、sys は予約語で、ユーザの設定には使用できません。

（注）　ユーザのパスワードは、設定ファイルでは表示されません。

注意　Nexus 5000 シリーズ スイッチは、TACACS+ または RADIUS によって作成されたか、ローカルに作成されたかに関係なく、すべて数字のユーザ名をサポートしていません。すべて数字の名前を持つローカル ユーザは作成できません。AAA サーバに数字だけのユーザ名が存在し、ログイン時にそのユーザ名を入力した場合、ログインできません。ユーザ名は英数字で始まる必要があり、次の特殊文字のみを使用できます:(+ = ._ \ -)。# 記号と！記号はサポートされていません。ユーザ名に許可されていない文字が含まれている場合、指定したユーザはログインできません。

強力なパスワードの特性

強力なパスワードは、次の特性を持ちます。

- 長さが 8 文字以上である
- 複数の連続する文字（"abcd" など）を含んでいない
- 複数の同じ文字の繰り返し（"aaabbb" など）を含んでいない
- 辞書に載っている単語を含んでいない
- 正しい名前を含んでいない
- 大文字および小文字の両方が含まれている
- 数字が含まれている

強力なパスワードの例を次に示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

（注）　クリア テキスト パスワードに含めることができる文字は、英数字だけです。ドル記号（$）やパーセント記号（%）などの特殊文字は使用できません。

ヒント　パスワードが簡単な場合（短く、解読されやすいパスワード）、Nexus 5000 シリーズ スイッチはパスワード設定を拒否します。サンプル設定のように、強力なパスワードを設定してください。パスワードは大文字と小文字が区別されます。

ユーザ ロールについて

ユーザ ロールには、そのロールを割り当てられたユーザが実行できる操作を定義するルールが含まれています。各ユーザ ロールに複数のルールを含めることができ、各ユーザが複数のロールを持つことができます。たとえば、ロール 1 では設定操作の実行だけが許可されており、ロール 2 ではデバッグ操作の実行だけが許可されている場合、ロール 1 とロール 2 の両方に属するユーザは、設定操作とデバッグ操作を実行できます。特定の VSAN、VLAN、およびインターフェイスへのアクセスを制限することもできます。

Nexus 5000 シリーズ スイッチは、次のデフォルトのユーザ ロールを提供します。

- network-admin（スーパーユーザ）：Nexus 5000 シリーズ スイッチ全体に対する読み取り/書き込みアクセスを実行できます。
- network-operator：Nexus 5000 シリーズ スイッチに対する読み取りアクセスを実行できます。

（注）　複数のロールに属するユーザは、そのロールで許可されるすべてのコマンドの組み合わせを実行できます。コマンドへのアクセス権は、コマンドへのアクセス拒否よりも優先されます。たとえば、ユーザが、コンフィギュレーション コマンドへのアクセスが拒否されたロール A を持っていたとします。また、コンフィギュレーション コマンドへのアクセスが許可されたロール B も持っていたとします。この場合、ユーザはコンフィギュレーション コマンドを使用できます。

規則について

ルールは、ロールの基本要素です。ルールは、そのロールがユーザにどの操作の実行を許可するかを定義します。ルールは次のパラメータで適用できます。

- Command：コマンドまたは正規表現で定義された一連のコマンド。
- 機能：Nexus 5000 シリーズ スイッチによって提供された機能に適用されるコマンド
  - **show role feature** コマンドを入力すれば、このパラメータに指定できる機能名が表示されます。
- Feature group：デフォルトまたはユーザ定義の機能グループ。
  - **show role feature-group** コマンドを入力すれば、このパラメータに指定できるデフォルトの機能グループが表示されます。

これらのパラメータは、階層状の関係を作成します。最も基本的な制御パラメータは command です。次の制御パラメータは feature です。これは、その機能にアソシエートされているすべてのコマンドを表します。最後の制御パラメータが、feature group です。feature group は、関連のある機能を結合して、既存の管理が簡単に行えるようにします。

ロールごとに最大 256 のルールを設定できます。ルールが適用される順序は、ユーザ指定のルール番号で決まります。ルールは降順で適用されます。たとえば、1 つのロールが 3 つのルールを持っている場合、ルール 3 がルール 2 よりも前に適用され、ルール 2 はルール 1 よりも前に適用されます。

ユーザ ロール ポリシーについて

ユーザがアクセスできるスイッチ リソースを制限するロール ポリシーを定義できます。インターフェイス、VLAN、および VSAN へのアクセスを制限するユーザ ロール ポリシーを定義できます。

ユーザ ロール ポリシーは、ロールに定義されている規則で制約されます。たとえば、特定のインターフェイスへのアクセスを許可するインターフェイス ポリシーを定義した場合、インターフェイス コマンドを許可するコマンド規則をロールに設定しないと、ユーザはインターフェイスにアクセスできません。ユーザ ロール インターフェイス ポリシーの変更（22-7 ページ）に、設定例があります。

コマンド ルールが特定のリソース（インターフェイス、VLAN、または VSAN）へのアクセスを許可した場合、リソースがユーザに関連付けられたユーザ ロール ポリシーに表示されていなくても、ユーザはこれらのリソースへのアクセスが許可されます。

注意事項および制約事項

ユーザ アカウントおよび RBAC には、次の注意事項および制限事項があります。

- ユーザ ロールには最大 256 個の規則を追加できます。
- 1 つのユーザ アカウントに最大 64 個のユーザ ロールを割り当てられます。

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

（注）　ユーザ アカウントは、少なくとも 1 つのユーザ ロールを持たなければなりません。

ユーザ アカウントの設定

Nexus 5000 シリーズ スイッチで最大 256 のユーザ アカウントを作成できます。ユーザ アカウントは、次の属性を持ちます。

- ユーザ名
- パスワード
- 失効日
- ユーザ ロール

ユーザ アカウントは、最大 64 個のユーザ ロールを持つことができます。ユーザ ロールの詳細については、「RBAC の設定」セクション（22-5 ページ）を参照してください。

（注）　ユーザ アカウントの属性に加えられた変更は、そのユーザがログインして新しいセッションを作成するまで有効になりません。

ユーザ アカウントを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch(config)# show role`	（任意）使用可能なユーザ ロールを表示します。必要に応じて、他のユーザ ロールを設定できます（「ユーザ ロールとルールの作成」セクション（22-5 ページ）を参照）。
ステップ 2	`switch# configure terminal` `switch(config)#`	グローバル コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	`switch(config)# username user-id [password password] [expire date] [role role-name]`	ユーザ アカウントを設定します。*user-id* 引数は、最大 28 文字の英数字で、大文字と小文字が区別されます。 デフォルト パスワードは定義されていません。 **（注）** パスワードを指定しないと、ユーザは Nexus 5000 シリーズ スイッチにログインできなくなる可能性があります。 **expire** *date* オプションの形式は、YYYY-MM-DD です。デフォルトでは、失効日はありません。
ステップ 4	`switch(config)# exit` `switch#`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	`switch# show user-account`	(任意) ロールの設定を表示します。
ステップ 6	`switch# copy running-config startup-config`	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、ユーザ アカウントを設定する例を示します。

```
switch# configure terminal
switch(config)# username NewUser password 4Ty18Rnt
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

RBAC の設定

この項では、次のトピックについて取り上げます。

- ユーザ ロールとルールの作成 (22-5 ページ)
- ユーザ ロール インターフェイス ポリシーの変更 (22-7 ページ)

ユーザ ロールとルールの作成

各ユーザ ロールが、最大 256 個のルールを持つことができます。1 つのユーザ ロールを複数のユーザ アカウントに割り当てることができます。

指定した規則番号が、規則の適用される順序を決定します。ルールは降順で適用されます。たとえば、1 つのロールが 3 つのルールを持っている場合、ルール 3 がルール 2 よりも前に適用され、ルール 2 はルール 1 よりも前に適用されます。

ユーザ ロールを作成してルールを指定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **role name** *role-name*	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。*role-name* 引数は、最大 16 文字の長さの英数字のストリングで、大文字小文字が区別されます。
ステップ 3	switch(config-role)# **rule** *number* {**deny** | **permit**} **command** *command-string*	コマンド規則を設定します。 *command-string* には、スペースおよび正規表現を含めることができます。たとえば、"interface ethernet *" は、すべてのイーサネット インターフェイスが含まれます。 必要な規則の数だけこのコマンドを繰り返します。
	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**}	すべての操作に対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。
	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name*	機能に対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。 **show role feature** コマンドを使用すれば、規則のリストが表示されます。 必要な規則の数だけこのコマンドを繰り返します。
	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name*	機能グループに対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。 **show role feature-group** コマンドを使用すれば、機能グループのリストが表示されます。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 4	switch(config-role)# **description** *text*	(任意) ロールの説明を設定します。説明にはスペースも含めることができます。
ステップ 5	switch(config-role)# **exit**	ロール コンフィギュレーション モードを終了します。
ステップ 6	switch(config)# **show role**	(任意) ユーザ ロールの設定を表示します。
ステップ 7	switch(config)# **copy running-config startup-config**	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、ユーザ ロールを作成して規則を指定する例を示します。

```
switch# configure terminal
switch(config)# role name UserA
switch(config-role)# rule deny command clear users
switch(config-role)# rule deny read-write
switch(config-role)# rule permit read feature router-bgp
switch(config-role)# rule deny read-write L3
switch(config-role)# description This role does not allow users to use clear commands
switch(config-role)# exit
switch(config)# show role
switch(config)# copy running-config startup-config
```

機能グループの作成

機能グループを作成する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# role feature-group group-name`	ユーザ ロール機能グループを指定して、ロール機能グループ コンフィギュレーション モードを開始します。 *group-name* 引数は、最大 32 文字の長さの英数字のストリングで、大文字小文字が区別されます。
ステップ 3	`switch(config-role-featuregrp)# exit`	ロール機能グループ コンフィギュレーション モードを終了します。
ステップ 4	`switch(config)# show role feature-group`	(任意)ロール機能グループの設定を表示します。
ステップ 5	`switch(config)# copy running-config startup-config`	(任意)実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

ユーザ ロール インターフェイス ポリシーの変更

ユーザ ロール インターフェイス ポリシーを変更することで、ユーザがアクセスできるインターフェイスを制限できます。ユーザ ロール インターフェイス ポリシーを変更する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# role name role-name`	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-role)# rule number permit command configure terminal ; interface *`	コマンド規則を設定して、すべてのインターフェイスへのアクセスを許可します。

	コマンド	目的
ステップ 4	switch(config-role)# **interface policy deny**	ロール インターフェイス ポリシー コンフィギュレーション モードを開始します。
ステップ 5	switch(config-role-interface)# **permit interface** *interface-list*	ロールがアクセスできるインターフェイスのリストを指定します。 必要なインターフェイスの数だけこのコマンドを繰り返します。 このコマンドの場合、イーサネット インターフェイス、ファイバ チャネル インターフェイス、および仮想ファイバ チャネル インターフェイスを指定できます。
ステップ 6	switch(config-role-interface)# **exit**	ロール インターフェイス ポリシー コンフィギュレーション モードを終了します。
ステップ 7	switch(config-role)# **show role**	(任意) ロールの設定を表示します。
ステップ 8	switch(config-role)# **copy running-config startup-config**	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

ロールがアクセスできるインターフェイスのリストを指定できます。これを必要なインターフェイスの数だけ指定できます。

```
switch(config-role-interface)# permit interface ethernet 2/1
switch(config-role-interface)# permit interface fc 3/1
switch(config-role-interface)# permit interface vfc 30/1
```

ユーザ ロール VLAN ポリシーの変更

ユーザ ロール VLAN ポリシーを変更することで、ユーザがアクセスできる VLAN を制限できます。ユーザ ロール VLAN ポリシーを変更する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **role name** *role-name*	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。
ステップ 3	switch(config-role)# **rule** *number* **permit command configure terminal ; vlan ***	コマンド規則を設定して、すべての VLAN へのアクセスを許可します。
ステップ 4	switch(config-role)# **vlan policy deny**	ロール VLAN ポリシー コンフィギュレーション モードを開始します。
ステップ 5	switch(config-role-vlan)# **permit vlan** *vlan-list*	ロールがアクセスできる VLAN の範囲を指定します。 必要な VLAN の数だけこのコマンドを繰り返します。
ステップ 6	switch(config-role-vlan)# **exit**	ロール VLAN ポリシー コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 7	switch(config-role)# **show role**	(任意)ロールの設定を表示します。
ステップ 8	switch(config-role)# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

ユーザ ロール VSAN ポリシーの変更

ユーザ ロール VSAN ポリシーを変更して、ユーザがアクセスできる VSAN を制限できます。

ユーザがアクセスできる VSAN を制限するユーザ ロール VSAN ポリシーを変更する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config-role)# **role name** *role-name*	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。
ステップ 3	switch(config-role)# **rule** *number* **permit command vsan database; vsan ***	すべての VSAN へのアクセスを許可するコマンド ルールを設定します。
ステップ 4	switch(config-role)# **vsan policy deny**	ロール VSAN ポリシー コンフィギュレーション モードを開始します。
ステップ 5	switch(config-role-vsan)# **permit vsan** *vsan-list*	ロールがアクセスできる VSAN 範囲を指定します。 必要な VSAN の数だけ、このコマンドを繰り返します。
ステップ 6	switch(config-role-vsan)# **exit**	ロール VSAN ポリシー コンフィギュレーション モードを終了します。
ステップ 7	switch(config-role)# **show role** **例:** switch(config-role)# show role	(任意)ロールの設定を表示します。
ステップ 8	switch(config-role)# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

ユーザ アカウントと RBAC の設定の確認

ユーザ アカウントおよび RBAC 設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show role	ユーザ ロールの設定を表示します。
show role feature	機能リストを表示します。

コマンド	目的
show role feature-group	機能グループの設定を表示します。
show startup-config security	スタートアップ コンフィギュレーションのユーザ アカウント設定を表示します。
show running-config security [all]	実行コンフィギュレーションのユーザ アカウント設定を表示します。**all** キーワードを指定すると、ユーザ アカウントのデフォルト値が表示されます。
show user-account	ユーザ アカウント情報を表示します。

ユーザ アカウントと RBAC 設定の例

次に、ユーザ ロールを設定する例を示します。

```
role name UserA
  rule 3 permit read feature l2nac
  rule 2 permit read feature dot1x
  rule 1 deny command clear *
```

次に、ユーザ ロール機能グループを設定する例を示します。

```
role feature-group name Security-features
  feature radius
  feature tacacs
  feature aaa
  feature acl
  feature access-list
```

デフォルト設定

表 22-1 に、ユーザ アカウントおよび RBAC パラメータのデフォルト設定値を示します。

表 22-1　デフォルトのユーザ アカウントと RBAC パラメータ

パラメータ	デフォルト
ユーザ アカウント パスワード	未定義
ユーザ アカウント失効日	なし
インターフェイス ポリシー	すべてのインターフェイスがアクセス可能
VLAN ポリシー	すべての VLAN がアクセス可能
VFC ポリシー	すべての VFC にアクセス可能
VETH ポリシー	すべての VETH にアクセス可能

CHAPTER 23

Session Manager の設定

この章では、Cisco NX-OS で Session Manager 機能を設定する方法について説明します。

この章は、次の項で構成されています。

- Session Manager の概要（23-1 ページ）
- 設定時の注意事項および制限事項（23-1 ページ）
- Session Manager の設定（23-2 ページ）
- Session Manager の設定確認（23-4 ページ）

Session Manager の概要

Session Manager を使用すると、設定変更をバッチ モードで実行できます。Session Manager は次のフェーズで機能します。

- コンフィギュレーション セッション：セッション マネージャ モードで実装するコマンドのリストを作成します。
- 検証：設定の基本的なセマンティック チェックを行います。Cisco NX-OS は、設定の一部でセマンティクス検査が失敗した場合にエラーを返します。
- 検証：既存のハードウェア設定、ソフトウェア設定、およびリソースに基づいて、設定全体を確認します。Cisco NX-OS は、設定がこの確認フェーズで合格しなかった場合にエラーを返します。
- コミット：Cisco NX-OS は全体の設定を確認して、デバイスに対する変更をアトミックに実行します。エラーが発生すると、Cisco NX-OS は元の設定に戻ります。
- 打ち切り：設定変更を実行しないで廃棄します。

任意で、変更をコミットしないでコンフィギュレーション セッションを終了できます。また、コンフィギュレーション セッションを保存することもできます。

設定時の注意事項および制限事項

Session Manager には、次の注意事項および制限事項があります。

- Session Manager がサポートするのは、ACL 機能だけです。
- 作成できるコンフィギュレーション セッションの最大数は 32 です。
- すべてのセッションで設定できるコマンドの最大数は 20,000 です。

Session Manager の設定

この項では、次のトピックについて取り上げます。

- セッションの作成（23-2 ページ）
- セッションでの ACL の設定（23-2 ページ）
- セッションの確認（23-3 ページ）
- セッションのコミット（23-3 ページ）
- セッションの保存（23-3 ページ）
- セッションの廃棄（23-3 ページ）
- Session Manager の設定例（23-3 ページ）

セッションの作成

作成できるコンフィギュレーション セッションの最大数は 32 です。

	コマンド	目的
ステップ 1	switch# **configure session** *name*	コンフィギュレーション セッションを作成し、セッション コンフィギュレーション モードを開始します。名前は任意の英数字ストリングです。
ステップ 2	switch(config-s)# **show configuration session** [*name*]	（任意）セッションの内容を表示します。
ステップ 3	switch(config-s)# **save** *location*	（任意）セッションをファイルに保存します。保存場所には、bootflash または volatile を指定できます。

セッションでの ACL の設定

コンフィギュレーション セッションで ACL を設定できます。

	コマンド	目的
ステップ 1	switch# **configure session** *name*	コンフィギュレーション セッションを作成し、セッション コンフィギュレーション モードを開始します。名前は任意の英数字ストリングです。
ステップ 2	switch(config-s)# **ip access-list** *name*	ACL を作成します。
ステップ 3	switch(config-s-acl)# **permit** *protocol source destination*	（任意）ACL に許可文を追加します。
ステップ 4	switch(config-s-acl)# **interface** *interface-type number*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	switch(config-s-if)# **ip port access-group** *name* **in**	インターフェイスにポート アクセス グループを追加します。
ステップ 6	switch# **show configuration session** [*name*]	（任意）セッションの内容を表示します。

セッションの確認

セッションを確認するには、セッション モードで次のコマンドを使用します。

コマンド	目的
`switch(config-s)# verify [verbose]`	コンフィギュレーション セッションのコマンドを確認します。

セッションのコミット

セッションをコミットするには、セッション モードで次のコマンドを使用します。

コマンド	目的
`switch(config-s)# commit [verbose]`	コンフィギュレーション セッションのコマンドをコミットします。

セッションの保存

セッションを保存するには、セッション モードで次のコマンドを使用します。

コマンド	目的
`switch(config-s)# save location`	(任意)セッションをファイルに保存します。保存場所には、bootflash または volatile を指定できます。

セッションの廃棄

セッションを廃棄するには、セッション モードで次のコマンドを使用します。

コマンド	目的
`switch(config-s)# abort`	コマンドを適用しないで、コンフィギュレーション セッションを廃棄します。

Session Manager の設定例

この例では、ACL のコンフィギュレーション セッションを作成します。

```
switch# configure session name test2
switch(config-s)# ip access-list acl2
switch(config-s-acl)# permit tcp any any
switch(config-s-acl)# exit
switch(config-s)# interface Ethernet 1/4
switch(config-s-ip)# ip port access-group acl2 in
switch(config-s-ip)# exit
```

```
switch(config-s)# verify
switch(config-s)# exit
switch# show configuration session test2
```

Session Manager の設定確認

Session Manager の設定情報を確認するには、次のコマンドを使用します。

コマンド	目的
show configuration session [*name*]	コンフィギュレーション ファイルの内容を表示します。
show configuration session status [*name*]	コンフィギュレーション セッションのステータスを表示します。
show configuration session summary	すべてのコンフィギュレーション セッションについて、要約を表示します。

CHAPTER 24

オンライン診断の設定

この章では、汎用オンライン診断（GOLD）機能を設定する方法について説明します。

この章は、次の項で構成されています。

- オンライン診断について（24-1 ページ）
- オンライン診断の設定（24-4 ページ）
- オンライン診断設定の確認（24-4 ページ）
- デフォルト設定値（24-4 ページ）

オンライン診断について

オンライン診断では、スイッチの起動時またはリセット時にハードウェア コンポーネントを確認し、通常の動作時にはハードウェアの状態を監視します。

この項では、次のトピックについて取り上げます。

- オンライン診断の概要（24-1 ページ）
- 起動時診断（24-1 ページ）
- ヘルス モニタリング診断（24-2 ページ）
- 拡張モジュール診断（24-3 ページ）

オンライン診断の概要

Cisco Nexus 5000 シリーズ スイッチは、起動時診断および実行時診断をサポートします。起動時診断には、システム起動時とリセット時に実行する、中断を伴うテストおよび非中断テストが含まれます。

実行時診断（ヘルス モニタリング診断）には、スイッチの通常の動作時にバックグラウンドで実行する非中断テストが含まれます。

起動時診断

起動時診断は、スイッチをオンラインにする前にハードウェアの障害を検出します。起動診断では、スーパーバイザと ASIC の間のデータ パスと制御パスの接続も確認します。表 24-1 に、スイッチの起動時またはリセット時にだけ実行される診断を示します。

表 24-1　起動時診断

診断	説明
USB フラッシュ	USB フラッシュ デバイスの整合性を確認します。
PCIe	PCI express（PCIe）アクセスをテストします。
OBFL	オンボード障害ロギング フラッシュの整合性を確認します。
NVRAM	NVRAM（不揮発性 RAM）の整合性を確認します。
Voltage	電圧レベルが適切な範囲内であることを確認します。
GPIO	General Purpose I/O（GPIO）コンポーネントをテストします。
インバンド ポート	インバンド ポートとスーパーバイザの接続をテストします。
管理ポート	管理ポートをテストします。
メモリ	DRAM の整合性を確認します。

起動時診断には、ヘルス モニタリング診断と共通するテスト セットも含まれます。表 24-3 に、起動時診断およびヘルス モニタリング診断を示します。

起動時診断では、オンボード障害ロギング（OBFL）システムに障害を記録します。また、障害により LED が表示され、診断テストのステート（on、off、pass、または fail）を示します。

起動時診断をバイパスするか、完全な起動時診断セットを実行するよう Cisco Nexus 5000 シリーズ スイッチを設定できます。「オンライン診断の設定」セクション（24-4 ページ）を参照してください。

ヘルス モニタリング診断

ヘルス モニタリング診断では、スイッチの状態に関する情報を提供します。実行時のハードウェア エラー、メモリ エラー、ソフトウェア障害、およびリソースの不足を検出します。

ヘルス モニタリング診断は中断されずにバックグラウンドで実行され、ライブ ネットワーク トラフィックを処理するスイッチの状態を確認します。

表 24-2 に、スイッチのヘルス モニタリング診断を示します。

表 24-2　ヘルス モニタリング診断テスト

診断	説明
LED	ポートおよびシステムのステータス LED を監視します。
電源モジュール	電源装置のヘルス ステータスを監視します。
温度センサー	温度センサーの読み取り値を監視します。
テスト ファン	ファンの速度およびファンの制御を監視します。

表 24-3 に、システム起動時とリセット時にも実行されるヘルス モニタリング診断を示します。

表 24-3　ヘルス モニタリングおよび起動時診断テスト

診断	説明
SPROM	バックプレーンとスーパーバイザ SPROM の整合性を確認します。
ファブリック エンジン	スイッチ ファブリック ASIC をテストします。
ファブリック ポート	スイッチ ファブリック ASIC 上のポートをテストします。
転送エンジン	転送エンジン ASIC をテストします。
転送エンジン ポート	転送エンジン ASIC 上のポートをテストします。
前面ポート	前面ポート上のコンポーネント（PHY および MAC など）をテストします。

拡張モジュール診断

スイッチの起動時またはリセット時の起動時診断には、スイッチのインサービス（IS）拡張モジュールのテストが含まれます。

稼働中のスイッチに拡張モジュールを挿入すると、診断テスト セットが実行されます。表 24-4 に、拡張モジュールの起動時診断を示します。起動時診断が失敗した場合、拡張モジュールはサービス状態になりません。

表 24-4　拡張モジュールの起動時診断およびヘルス モニタリング診断

診断	説明
SPROM	バックプレーンとスーパーバイザ SPROM の整合性を確認します。
ファブリック エンジン	スイッチ ファブリック ASIC をテストします。
ファブリック ポート	スイッチ ファブリック ASIC 上のポートをテストします。
転送エンジン	転送エンジン ASIC をテストします。
転送エンジン ポート	転送エンジン ASIC 上のポートをテストします。
前面ポート	前面ポート上のコンポーネント（PHY および MAC など）をテストします。

ヘルス モニタリング診断は、IS 拡張モジュールで実行されます。表 24-4 に、起動時診断と共通するテストを示します。表 24-5 に、拡張モジュールのヘルス モニタリング診断に固有の追加テストを示します。

表 24-5　拡張モジュールのヘルス モニタリング診断

診断	説明
LED	ポートおよびシステムのステータス LED を監視します。
温度センサー	温度センサーの読み取り値を監視します。

オンライン診断の設定

完全なテスト セットを実行するよう起動時診断を設定できます。もしくは、高速モジュール起動時のすべての起動時診断テストをバイパスできます。

（注）　起動時オンライン診断レベルを **complete** に設定することを推奨します。起動時オンライン診断をバイパスすることは推奨しません。

起動時オンライン診断レベルを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# diagnostic bootup level [complete | bypass]`	デバイスの起動時に診断を実行するよう起動時診断レベルを次のように設定します。 • complete：すべての起動時診断を実行します。これはデフォルト値です。 • bypass：起動時診断を実行しません。
ステップ 3	`switch# show diagnostic bootup level`	（任意）現在、スイッチで実行されている起動時診断レベル（bypass または complete）を表示します。

次に、完全な診断を実行するよう起動時診断レベルを設定する例を示します。

```
switch# configure terminal
switch(config)# diagnostic bootup level complete
```

オンライン診断設定の確認

オンライン診断設定情報を表示するには、次の作業を行います。

コマンド	目的
show diagnostic bootup level	起動時診断レベルを表示します。
show diagnostic result module *slot*	診断テストの結果を表示します。

デフォルト設定値

表 24-6 に、オンライン診断パラメータのデフォルト設定値を示します。

表 24-6　デフォルトのオンライン診断パラメータ

パラメータ	デフォルト
起動時診断レベル	complete

CHAPTER 25

システム メッセージ ロギングの設定

この章では、スイッチにシステム メッセージ ロギングを設定する方法について説明します。

この章は、次の項で構成されています。

- システム メッセージ ロギングの概要（25-1 ページ）
- システム メッセージ ロギングの設定（25-2 ページ）
- システム メッセージ ロギングの設定の確認（25-9 ページ）
- システム メッセージ ロギングの設定例（25-9 ページ）
- デフォルト設定（25-10 ページ）

システム メッセージ ロギングの概要

システム メッセージ ロギングを使用して宛先を制御し、システム プロセスが生成するメッセージの重大度をフィルタリングできます。端末セッション、ログ ファイル、およびリモート システム上の Syslog サーバへのロギングを設定できます。

デフォルトでは、スイッチはメッセージをターミナル セッションへ出力します。ターミナル セッションへのロギングの設定については、「ターミナル セッションへのシステム メッセージ ロギングの設定」セクション（25-3 ページ）を参照してください。

デフォルトでは、スイッチはシステム メッセージをログ ファイルに記録します。ファイルへのロギングの設定については、「ファイルへのシステム メッセージ ロギングの設定」セクション（25-4 ページ）を参照してください。

表 25-1 に、システム メッセージで使用する重大度を示します。重大度を設定する場合、システムはそのレベル以下のメッセージを出力します。

表 25-1　システム メッセージの重大度

レベル	説明
0：緊急	システムが使用不可
1：アラート	即時処理が必要
2：クリティカル	クリティカル状態
3：エラー	エラー状態
4：警告	警告状態
5：通知	正常だが注意を要する状態

表 25-1　　システム メッセージの重大度（続き）

レベル	説明
6:情報	単なる情報メッセージ
7:デバッグ	デバッグ実行時にのみ表示

重大度 0、1、または 2 の最新のメッセージを 100 個まで不揮発性 RAM（NVRAM）ログに記録します。NVRAM へのロギングは設定できません。

メッセージを生成したファシリティと重大度に基づいて記録するシステム メッセージを設定できます。モジュールおよびファシリティごとの重大度の設定については、「記録されたモジュールおよびファシリティ メッセージの設定」セクション（25-4 ページ）を参照してください。

Syslog サーバ

Syslog サーバは、Syslog プロトコルに基づいてシステム メッセージを記録するよう設定されたリモート システムで稼働します。最大で 3 台の Syslog サーバを設定できます。Syslog サーバの設定については、「Syslog サーバの設定」セクション（25-5 ページ）を参照してください。

ファブリック内のすべてのスイッチで Syslog サーバの同じ設定をサポートするために、Cisco Fabric Services（CFS）を使用して Syslog サーバ設定を配布できます。Syslog サーバ設定の配布については、「Syslog サーバ設定の配布の設定」セクション（25-7 ページ）を参照してください。

（注）　スイッチを最初に初期化する場合、ネットワークが初期化されてからメッセージが Syslog サーバに送信されます。

システム メッセージ ロギングの設定

この項では、次のトピックについて取り上げます。

- ターミナル セッションへのシステム メッセージ ロギングの設定（25-3 ページ）
- ファイルへのシステム メッセージ ロギングの設定（25-4 ページ）
- 記録されたモジュールおよびファシリティ メッセージの設定（25-4 ページ）
- Syslog サーバの設定（25-5 ページ）
- Syslog サーバ設定の配布の設定（25-7 ページ）
- ログ ファイルの表示およびクリア（25-8 ページ）

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

ターミナル セッションへのシステム メッセージ ロギングの設定

コンソール、Telnet、および SSH セッションに対する重大度によって、メッセージを記録するようスイッチを設定できます。

デフォルトでは、ターミナル セッションでロギングはイネーブルです。メッセージを記録するようスイッチを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# logging console [severity-level]`	指定された重大度またはそれ以上の重大度に基づいて、スイッチはメッセージをコンソール セッションへ記録できます。重大度は 0 ～ 7 で、表 25-1 に示します。重大度が指定されていない場合、デフォルトの 2 が使用されます。
	`switch(config)# no logging console [severity-level]`	コンソールへメッセージを記録するスイッチの機能をディセーブルにします。
ステップ 3	`switch(config)# show logging console`	(任意)コンソール ロギング設定を表示します。
ステップ 4	`switch(config)# logging monitor [severity-level]`	指定された重大度またはそれ以上の重大度に基づいて、スイッチはメッセージをモニタへ記録できます。設定は Telnet および SSH セッションに適用されます。重大度は 0 ～ 7 で、表 25-1 に示します。重大度が指定されていない場合、デフォルトの 2 が使用されます。
	`switch(config)# no logging monitor [severity-level]`	Telnet および SSH セッションへのメッセージのロギングをディセーブルにします。
ステップ 5	`switch(config)# show logging monitor`	(任意)モニタ ロギング設定を表示します。
ステップ 6	`switch(config)# copy running-config startup-config`	(任意)実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、メッセージを記録するようスイッチを設定する例を示します。

```
switch# configure terminal
switch(config)# logging console 3
switch(config)# no logging console
switch(config)# show logging console
switch(config)# logging monitor 3
switch(config)# no logging monitor
switch(config)# show logging monitor
switch(config)# copy running-config startup-config
```

ファイルへのシステム メッセージ ロギングの設定

システム メッセージをファイルに記録するようスイッチを設定できます。デフォルトでは、システム メッセージはファイル log:messages に記録されます。

ログ ファイルの表示およびクリアについては、「ログ ファイルの表示およびクリア」セクション（25-8 ページ）を参照してください。

システム メッセージをファイルに記録するようスイッチを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **logging logfile** *logfile-name severity-level* [**size** *bytes*]	システム メッセージを保存するのに使用するログ ファイルの名前と、記録する最小重大度を設定します。任意で最大ファイル サイズを指定できます。デフォルトの重大度は 5 です。ファイル サイズは 10485760 です。表 25-1 に、重大度を示します。ファイル サイズは 4096 ～ 10485760 バイトです。
	switch(config)# **no logging logfile** [*logfile-name severity-level* [**size** *bytes*]]	ログ ファイルへのロギングをディセーブルにします。
ステップ 3	switch(config)# **show logging info**	（任意）ロギング設定を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意）実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、システム メッセージをファイルに記録するようスイッチを設定する例を示します。

```
switch# configure terminal
switch(config)# logging logfile my_log size 6
switch(config)# no logging logfile
switch(config)# show logging info
switch(config)# copy running-config startup-config
```

記録されたモジュールおよびファシリティ メッセージの設定

モジュールおよびファシリティによって記録されたメッセージの重大度とタイムスタンプ単位を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **logging module** [*severity-level*]	指定された重大度またはそれ以上の重大度であるモジュール ログ メッセージをイネーブルにします。重大度は 0 ～ 7 で、表 25-1 に示します。重大度が指定されていない場合、デフォルトの 5 が使用されます。
	switch(config)# **no logging module** [*severity-level*]	モジュール ログ メッセージをディセーブルにします。

	コマンド	目的
ステップ 3	switch(config)# **show logging module**	(任意)モジュール ロギング設定を表示します。
ステップ 4	switch(config)# **logging level** *facility severity-level*	指定された重大度またはそれ以上の重大度である指定のファシリティからのロギング メッセージをイネーブルにします。重大度は 0 ～ 7 で、表 25-1 に示します。同じ重大度をすべてのファシリティに適用するには、**all** ファシリティを使用します。デフォルト値については、**show logging level** コマンドを参照してください。
	switch(config)# **no logging level** [*facility severity-level*]	指定されたファシリティのロギング重大度をデフォルト レベルにリセットします。ファシリティおよび重大度を指定しないと、スイッチはすべてのファシリティをデフォルト レベルにリセットします。
ステップ 5	switch(config)# **show logging level** [*facility*]	(任意)ファシリティごとに、ロギング レベル設定およびシステムのデフォルト レベルを表示します。ファシリティを指定しないと、スイッチはすべてのファシリティのレベルを表示します。
ステップ 6	switch(config)# **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	ロギング タイムスタンプ単位を設定します。デフォルトでは、単位は秒です。
	switch(config)# **no logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	ロギング タイムスタンプ単位をデフォルトの秒にリセットします。
ステップ 7	switch(config)# **show logging timestamp**	(任意)設定されたロギング タイムスタンプ単位を表示します。
ステップ 8	switch(config)# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、メッセージの重大度とタイムスタンプ単位を設定する例を示します。

```
switch# configure terminal
switch(config)# logging module 3
switch(config)# show logging module
switch(config)# logging level aaa 2
switch(config)# logging timestamp milliseconds
switch(config)# show logging timestamp
switch(config)# copy running-config startup-config
```

Syslog サーバの設定

システム メッセージを記録するリモート システムを参照する Syslog サーバを最大で 3 台設定できます。

ファブリックでの Syslog 設定の配布については、「Syslog サーバ設定の配布の設定」セクション(25-7 ページ)を参照してください。

/etc/syslog.conf ファイルに次の行を追加して、UNIX または Linux システム上に Syslog サーバを設定できます。

```
facility.level <five tab characters> action
```

表 25-2 に、設定可能な Syslog フィールドを示します。

表 25-2　syslog.conf の Syslog フィールド

フィールド	説明
Facility	メッセージの作成者。auth、authpriv、cron、daemon、kern、lpr、mail、mark、news、syslog、user、local0 ～ local7 です。アスタリスク (*) を使用するとすべてを指定します。これらのファシリティ指定により、発信元に基づいてメッセージの宛先を制御できます。 **(注)**　ローカル ファシリティを使用する前に設定をチェックします。
Level	メッセージを記録する最小重大度。debug、info、notice、warning、err、crit、alert、emerg です。アスタリスク (*) を使用するとすべてを指定します。none を使用するとファシリティをディセーブルにできます。
Action	メッセージの宛先。ファイル名、前にアット マーク (@) が付いたホスト名、カンマで区切られたユーザ リストです。アスタリスク (*) を使用するとすべてのログイン ユーザを指定します。

UNIX または Linux システムに Syslog サーバを設定するには、次の作業を行います。

ステップ 1　/etc/syslog.conf ファイルに次の行を追加して、ファイル /var/log/myfile.log に local7 ファシリティのデバッグ メッセージを記録します。

```
debug.local7              /var/log/myfile.log
```

ステップ 2　シェル プロンプトで次のコマンドを入力して、ログ ファイルを作成します。

```
$ touch /var/log/myfile.log
$ chmod 666 /var/log/myfile.log
```

ステップ 3　次のコマンドを入力して、システム メッセージ ロギング デーモンが myfile.log をチェックして、新しい変更を取得するようにします。

```
$ kill -HUP ~cat /etc/syslog.pid~
```

Syslog サーバを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# logging server host [severity-level [facility]]`	指定されたホスト名、あるいは IPv4 または IPv6 アドレスで Syslog サーバを設定します。特定のファシリティの、最小重大度であるメッセージのロギングを制限できます。重大度は 0 ～ 7 で、表 25-1に示します。デフォルトの発信ファシリティは local7 です。
	`switch(config)# no logging server host`	指定されたホストのロギング サーバを削除します。
ステップ 3	最大 3 台の Syslog サーバに対して、ステップ 2 を繰り返します。	

	コマンド	目的
ステップ 4	`switch(config)# show logging server`	(任意)Syslog サーバ設定を表示します。
ステップ 5	`switch(config)# copy running-config startup-config`	(任意)実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

次に、Syslog サーバを設定する例を示します。

```
switch# configure terminal
switch(config)# logging server 172.28.254.254 5 local3
switch(config)# show logging server
switch(config)# copy running-config startup-config
```

Syslog サーバ設定の配布の設定

Cisco Fabric Services(CFS)インフラストラクチャを使用して、ネットワーク内の他のスイッチへ Syslog サーバ設定を配布できます。

CFS の詳細については、「CFS について」セクション(21-1 ページ)を参照してください。

Syslog サーバ設定の配布をイネーブルにすると、配布設定をコミットする前に Syslog サーバ設定を変更し、保留中の変更を表示できます。配布がイネーブルである限り、スイッチは Syslog サーバ設定に対する保留中の変更を維持します。

(注)　スイッチを再起動すると、不揮発性メモリに保存されている Syslog サーバ設定の変更は失われます。

Syslog サーバ設定の配布を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# logging distribute`	CFS インフラストラクチャを使用して、ネットワーク スイッチへの Syslog サーバ設定の配布をイネーブルにできます。デフォルトでは、配布はディセーブルです。
	`switch(config)# no logging distribute`	CFS インフラストラクチャを使用して、ネットワーク スイッチへの Syslog サーバ設定の配布をディセーブルにできます。設定変更が保留中の場合は、配布をディセーブルにできません。**logging commit** および **logging abort** コマンドを参照してください。デフォルトでは、配布はディセーブルです。
ステップ 3	Syslog サーバ コンフィギュレーション コマンドを入力します。	「Syslog サーバの設定」セクション(25-5 ページ)を参照してください。
ステップ 4	`switch(config)# show logging pending`	(任意)Syslog サーバ設定に対する保留中の変更を表示します。

	コマンド	目的
ステップ 5	switch(config)# **show logging pending-diff**	(任意)Syslog サーバ設定の保留中の変更に対して、現在の Syslog サーバ設定との違いを表示します。
ステップ 6	switch(config)# **logging commit**	ファブリック内のスイッチへ配布するための Syslog サーバ設定に対する保留中の変更をコミットします。
	switch(config)# **logging abort**	Syslog サーバ設定に対する保留中の変更をキャンセルします。
ステップ 7	switch(config)# **show logging internal info**	(任意)Syslog サーバ配布の現在の状態と最後に実行したアクションに関する情報を表示します。
ステップ 8	switch(config)# **copy running-config startup-config**	(任意)実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

ログ ファイルの表示およびクリア

ログ ファイルおよび NVRAM 内のメッセージを表示およびクリアするには、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **show logging last** *number-lines*	ロギング ファイルの最終行番号を表示します。最終行番号には 1 ～ 9999 を指定できます。
ステップ 2	switch# **show logging logfile** [**start-time** *yyyy mmm dd hh:mm:ss*] [**end-time** *yyyy mmm dd hh:mm:ss*]	入力されたスパン内にタイム スタンプがあるログ ファイルのメッセージを表示します。終了時間を入力しないと、現在の時間が使用されます。month time フィールドには 3 文字を、year フィールドと day time フィールドには数値を入力します。
ステップ 3	switch# **show logging nvram** [**last** *number-lines*]	NVRAM のメッセージを表示します。表示される行数を制限するには、表示する最終行番号を入力できます。最終行番号には 1 ～ 100 を指定できます。
ステップ 4	switch# **clear logging logfile**	ログ ファイルの内容をクリアします。
ステップ 5	switch# **clear logging nvram**	NVRAM の記録されたメッセージをクリアします。

次に、ログ ファイルのメッセージを表示またはクリアする例を示します。

```
switch# show logging last 40
switch# show logging logfile start-time 2007 nov 1 15:10:0
switch# show logging nvram last 10
switch# clear logging logfile
switch# clear logging nvram
```

システム メッセージ ロギングの設定の確認

システム メッセージ ロギングの設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show logging console	コンソール ロギング設定を表示します。
show logging info	ロギング設定を表示します。
show logging internal info	Syslog 配布情報を表示します。
show logging last *number-lines*	ログ ファイルの末尾から指定行数を表示します。
show logging level [*facility*]	ファシリティ ロギング重大度設定を表示します。
show logging logfile [**start-time** *yyyy mmm dd hh:mm:ss*] [**end-time** *yyyy mmm dd hh:mm:ss*]	ログ ファイルのメッセージを表示します。
show logging module	モジュール ロギング設定を表示します。
show logging monitor	モニタ ロギング設定を表示します。
show logging nvram [**last** *number-lines*]	NVRAM ログのメッセージを表示します。
show logging pending	Syslog サーバの保留中の配布設定を表示します。
show logging pending-diff	Syslog サーバの保留中の配布設定の違いを表示します。
show logging server	Syslog サーバ設定を表示します。
show logging session	ロギング セッションのステータスを表示します。
show logging status	ロギング ステータスを表示します。
show logging timestamp	ロギング タイムスタンプ単位設定を表示します。

システム メッセージ ロギングの設定例

次に、システム メッセージ ロギングを設定する例を示します。

```
configure terminal
  logging console 3
  logging monitor 3
  logging logfile my_log 6
  logging module 3
  logging level aaa 2
  logging timestamp milliseconds
  logging distribute
  logging server 172.28.254.253
  logging server 172.28.254.254 5 local3
  logging commit
  copy running-config startup-config
```

デフォルト設定

表 25-3 に、システム メッセージ ロギング パラメータのデフォルト設定を示します。

表 25-3　デフォルトのシステム メッセージ ロギング パラメータ

パラメータ	デフォルト
コンソール ロギング	重大度 2 でイネーブル
モニタ ロギング	重大度 2 でイネーブル
ログ ファイル ロギング	重大度 5 で log:messages をイネーブル
モジュール ロギング	重大度 5 でイネーブル
ファシリティ ロギング	イネーブル
タイムスタンプ単位	秒
Syslog サーバ ロギング	ディセーブル
Syslog サーバ設定の配布	ディセーブル

CHAPTER 26

Smart Call Home の設定

この章では、Smart Call Home 機能を設定する方法について説明します。この章は、次の項で構成されています。

- Call Home について（26-1 ページ）
- Call Home の前提条件（26-7 ページ）
- 設定時の注意事項および制限事項（26-7 ページ）
- Call Home の設定（26-7 ページ）
- Call Home の設定の確認（26-15 ページ）
- Call Home の設定例（26-16 ページ）
- デフォルト設定（26-16 ページ）
- その他の関連資料（26-17 ページ）

Call Home について

Call Home は、重要なシステム イベントを E メールで通知します。Nexus 5000 シリーズ スイッチは、幅広いメッセージ フォーマットを提供し、ポケットベル サービス、標準 E メール、または XML ベースの自動解析アプリケーションと最適な互換性を保てます。この機能を使用して、ネットワーク サポート エンジニアや Network Operations Center を呼び出せます。また、Cisco Smart Call Home サービスを使用して、TAC でケースを自動的に生成することもできます。

この項では、次のトピックについて取り上げます。

- Call Home の概要（26-1 ページ）
- 宛先プロファイル（26-2 ページ）
- Call Home アラート グループ（26-3 ページ）
- Call Home のメッセージ レベル（26-5 ページ）
- Smart Call Home の取得（26-6 ページ）

Call Home の概要

Call Home を使用すると、重要なイベントがデバイスで発生した場合に外部エンティティに通知できます。コール ホームは、*宛先プロファイル*に設定された複数の受信者にアラートを配信します（「宛先プロファイル」セクション（26-2 ページ）*を参照*）。

Call Home には、スイッチで事前に定義された一連のアラートが含まれます。これらのアラートはアラート グループにグループ化され、アラート グループ内でアラートが発生したときに実行するため CLI コマンドが割り当てられます。スイッチには、転送された Call Home メッセージのコマンド出力が含まれます。アラートのリストと、アラートが発生したときに送信される定義済みの CLI コマンドについては、「Call Home アラート グループ」セクション（26-3 ページ）を参照してください。

Call Home 機能には、次の利点があります。

- 関連する CLI コマンド出力の実行および添付が自動化されます。
- 次のような、複数のメッセージ フォーマット オプションがあります。
  - ショート テキスト：ポケットベルまたは印刷形式のレポートに最適。
  - フル テキスト：人間が判読しやすいように完全にフォーマットされたメッセージ情報です。
  - XML：Extensible Markup Language（XML）および Adaptive Messaging Language（AML）XML スキーマ定義（XSD）を使用した、判読可能なフォーマットです。AML XSD は、Cisco.com の Web サイト（http://www.cisco.com/）で公開されています。XML フォーマットでは、シスコの TAC との通信が可能になります。
- 複数のメッセージ宛先への同時配信が可能。各宛先プロファイルには最大 50 件の電子メール宛先アドレスを設定できます。

宛先プロファイル

宛先プロファイルには、次の情報が含まれます。

- 1 つまたは複数のアラート グループ：アラートの発生時に、特定の Call Home メッセージを送信するアラートのグループ。
- 1 つまたは複数の E メール宛先：この宛先プロファイルに割り当てられたアラート グループによって生成された Call Home メッセージの受信者リスト。
- メッセージ フォーマット：Call Home メッセージのフォーマット（ショート テキスト、フル テキスト、または XML）。
- メッセージ重大度：スイッチが宛先プロファイル内のすべての E メール アドレスに対して Call Home メッセージを生成する前に、アラートが満たす必要がある Call Home 重大度。Call Home 重大度の詳細については、「Call Home のメッセージ レベル」セクション（26-5 ページ）を参照してください。アラートの Call Home 重大度が、宛先プロファイルに設定されたメッセージ重大度よりも低い場合、Nexus 5000 シリーズ スイッチはアラートを生成しません。

定期メッセージを日別、週別、月別で送信するコンポーネント アラート グループを使用して、定期的なコンポーネント アップデート メッセージを許可するよう宛先プロファイルを設定することもできます。

Nexus 5000 シリーズ スイッチは、次の定義済み宛先プロファイルをサポートします。

- CiscoTAC-1：XML メッセージ フォーマットの Cisco-TAC アラート グループをサポートします。
- full-text-destination：フル テキスト メッセージ フォーマットをサポートします。
- short-text-destination：ショート テキスト メッセージ フォーマットをサポートします。

メッセージ フォーマットの詳細については、「メッセージ フォーマット」セクション（26-17 ページ）を参照してください。

Call Home アラート グループ

アラート グループは、すべての Nexus 5000 シリーズ スイッチでサポートされる Call Home アラートの定義済みサブセットです。アラート グループ機能を使用すると、定義済みまたはカスタム宛先プロファイルに送信する一連の Call Home アラートを選択できます。コール ホーム アラートが宛先プロファイルにアソシエートされたいずれかのアラート グループに属する場合、およびアラートで、Call Home メッセージ重大度が宛先プロファイルに設定されているメッセージ重大度と同じか、それ以上である場合のみ、Call Home アラートは宛先プロファイルの E メールの宛先に送信されます（「Call Home のメッセージ レベル」セクション（26-5 ページ）を参照）。

表 26-1 に、サポートされるアラート グループと、アラート グループ用に生成された Call Home メッセージに含まれるデフォルトの CLI コマンド出力を示します。

表 26-1　アラート グループおよび実行されるコマンド

アラート グループ	説明	実行されるコマンド
Cisco-TAC	Smart Call Home 宛ての、他のアラート グループからのすべてのクリティカル アラート。	アラートを発信するアラート グループに基づいてコマンドを実行します。
設定（Configuration）	設定に関連した定期的なイベント。	**show module** **show module fex** **show running-config all** **show startup-config** **show version**
診断	診断によって生成されたイベント。	**show diagnostic result fex all** **show diagnostic result module all** **show diagnostic result module** ***number*** **show logging last** ***number*** **show module** **show module fex** **show prom all** **show tech-support platform** **show tech-support platform callhome** **show tech-support platform callhome fex** **show version**
組み込みイベント マネージャ（EEM）	EEM によって生成されるイベント	**show diagnostic result module all** **show diagnostic result module** ***number*** **show module** **show tech-support platform**

表 26-1　アラート グループおよび実行されるコマンド（続き）

アラート グループ	説明	実行されるコマンド
Environmental	電源、ファン、および温度アラームなどの環境検知要素に関連するイベント。	**show environment** **show environment fan** **show environment fex all** **show environment power** **show environment temperature** **show logging last 1000** **show module** **show tech-support platform callhome** **show version**
インベントリ	装置がコールド ブートした場合、または FRU の取り付けまたは取り外しを行った場合に示されるコンポーネント ステータス。このアラートは重要でないイベントであり、情報はステータスおよび使用権に使用されます。	**show inventory** **show inventory fex all** **show license** **show license usage** **show module** **show sprom all** **show system uptime** **show version**
ライセンス	ライセンスおよびライセンス違反に関連するイベント	**show license** **show license usage** **show logging last *number***
ラインカード ハードウェア	標準またはインテリジェント スイッチング モジュールに関連するイベント。	**show diagnostic result module all** **show diagnostic result module *number*** **show module** **show prom all** **show tech-support ethpm** **show tech-support platform** **show tech-support platform callhome** **show version**
スーパーバイザ ハードウェア	スーパーバイザ モジュールに関連するイベント。	**show diagnostic result module all** **show diagnostic result module *number*** **show module** **show prom all** **show tech-support ethpm** **show tech-support platform** **show tech-support platform callhome** **show version**

表 26-1　アラート グループおよび実行されるコマンド（続き）

アラート グループ	説明	実行されるコマンド
システム	装置の動作に必要なソフトウェア システムの障害によって生成されたイベント。	**show diagnostic result module all** **show diagnostic result module *number*** **show logging last number** **show module** **show prom all** **show system reset-reason** **show system resources** **show system uptime** **show tech-support** **show tech-support ethpm** **show tech-support platform**

Call Home は、Syslog の重大度を、Syslog ポート グループ メッセージの対応する Call Home の重大度に対応させます（「Call Home のメッセージ レベル」セクション（26-5 ページ）を参照）。

特定のイベントが発生し、Call Home メッセージを含む **show** 出力を送信した場合に、追加の CLI **show** コマンドを実行するために、定義済みのアラート グループをカスタマイズできます。

show コマンドは、フル テキストおよび XML 宛先プロファイルにのみ追加できます。ショート テキスト宛先プロファイルは、128 バイトのテキストに制限されているため、追加の **show** コマンドをサポートしていません。

Call Home のメッセージ レベル

Call Home を使用すると、緊急度に基づいてメッセージをフィルタリングできます。各宛先プロファイル（定義済みおよびユーザ定義）を、Call Home メッセージ レベルしきい値にアソシエートすることができます。宛先プロファイルのこのしきい値よりも小さな値を持つ Call Home メッセージは、生成されません。Call Home メッセージの緊急度の範囲は 0（緊急度が最小）～ 9（緊急度が最大）です。デフォルトは 0 です（Nexus 5000 シリーズはすべてのメッセージを送信します）。

Syslog アラート グループに送信される Call Home メッセージでは、Syslog の重大度が Call Home メッセージ レベルにマッピングされます。

（注） Call Home は、メッセージ テキストで Syslog メッセージ レベルを変更しません。

表 26-2 に、各 Call Home メッセージ レベルのキーワードと、Syslog ポート アラート グループの対応する Syslog レベルを示します。

表 26-2　重大度と Syslog レベルの対応

Call Home レベル	キーワード	Syslog レベル	説明
9	**Catastrophic**	該当なし	ネットワーク全体に壊滅的な障害が発生しています。
8	**Disaster**	該当なし	ネットワークに重大な影響が及びます。
7	**Fatal**	緊急（0）	システムが使用不可能な状態。

表 26-2　重大度と Syslog レベルの対応（続き）

Call Home レベル	キーワード	Syslog レベル	説明
6	**Critical**	アラート（1）	クリティカルな状況で、すぐに対応する必要があります。
5	**Major**	重要（2）	重大な状態。
4	**Minor**	エラー（3）	軽微な状態。
3	**Warning**	警告（4）	警告状態。
2	**Notification**	通知（5）	基本的な通知および情報メッセージです。他と関係しない、重要性の低い障害です。
1	**Normal**	情報（6）	標準状態に戻ることを示す標準イベントです。
0	**Debugging**	デバッグ（7）	デバッグ メッセージ。

Smart Call Home の取得

シスコと直接サービス契約を結んでいる場合は、Smart Call Home サービス用にデバイスを登録できます。Smart Call Home では、お使いのデバイスから送信された Call Home メッセージを分析し、背景説明と推奨事項を提供することによって、システムの問題をすばやく解決できます。既知と特定できる問題、特に GOLD 診断エラーについては、シスコ TAC によって自動サービス リクエストが生成されます。

Smart Call Home には、次の機能があります。

- 継続的なデバイス ヘルス モニタリングとリアルタイムの診断アラート。
- 問題解決を迅速に行うための詳細な診断情報を含む、適切な TAC チームに転送された、お使いのデバイスからの Call Home メッセージの分析および自動サービス リクエストの生成（該当する場合）。
- セキュアなメッセージ転送が、ご使用のデバイスから直接、またはダウンロード可能な Transport Gateway（TG）集約ポイントを経由して行われます。複数のデバイスでサポートを必要としている場合、またはセキュリティ要件の関係でご使用のデバイスをインターネットに直接接続できない場合は、TG 集約ポイントを使用できます。
- Call Home メッセージと推奨事項、すべての Call Home デバイスのコンポーネントと設定情報への Web アクセス。関連するフィールド通知、セキュリティ勧告、およびサポート終了日情報にアクセスできます。

次の項目を登録する必要があります。

- ご使用のスイッチの SMARTnet 契約番号
- 電子メール アドレス
- Cisco.com ID

Smart Call Home の詳細については、次の URL の Smart Call Home のページを参照してください。

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

Call Home の前提条件

Call Home には次の前提条件があります。

- E メール サーバを設定する必要があります。
- Call Home をイネーブルにするには、まず担当者名（SNMP サーバ担当者）、電話番号、および住所情報を設定する必要があります。この手順は、受信メッセージの送信元を判別するために必要です。
- スイッチは、E メール サーバに IP 接続する必要があります。
- Smart Call Home サービスを使用する場合、設定中のデバイスに対応している現在のサービス契約が必要です。

設定時の注意事項および制限事項

Call Home には、次の注意事項および制限事項があります。

- IP 接続がない場合、またはプロファイル宛先に対する VPN ルーティングおよび転送（VRF）のインターフェイスがダウン状態である場合、スイッチは Call Home メッセージを送信できません。
- すべてのシンプル メール転送プロトコル（SMTP）サーバと連動します。

Call Home の設定

この項では、次のトピックについて取り上げます。

- Call Home 設定のガイドライン（26-8 ページ）
- 担当者情報の設定（26-8 ページ）
- 宛先プロファイルの作成（26-9 ページ）
- 宛先プロファイルの変更（26-10 ページ）
- アラート グループと宛先プロファイルのアソシエーション（26-11 ページ）
- アラート グループへの show コマンドの追加（26-12 ページ）
- E メールの設定（26-13 ページ）
- 定期的なインベントリ通知の設定（26-13 ページ）
- 重複メッセージの抑制のディセーブル化（26-14 ページ）
- Call Home のイネーブル化またはディセーブル化（26-14 ページ）
- Call Home の通信のテスト（26-15 ページ）

Call Home 設定のガイドライン

Call Home を設定するには、次の作業を行います。

ステップ 1　連絡先情報を割り当てます。

ステップ 2　宛先プロファイルを設定します。

ステップ 3　各プロファイルに 1 つまたは複数のアラート グループを関連付けます。

ステップ 4　(任意)追加の **show** コマンドをアラート グループに追加します。

ステップ 5　トランスポート オプションを設定します。

ステップ 6　Call Home をイネーブルにします。

ステップ 7　(任意)Call Home メッセージをテストします。

担当者情報の設定

Call Home には、E メール、電話番号、住所の各情報を指定する必要があります。契約 ID、カスタマー ID、サイト ID、およびスイッチ プライオリティ情報を任意で指定できます。

担当者情報を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configuration terminal`**	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`snmp-server contact`** *`sys-contact`*	SNMP sysContact を設定します。
ステップ 3	`switch(config)#` **`callhome`**	Call Home コンフィギュレーション モードを開始します。
ステップ 4	`switch(config-callhome)#` **`email-contact`** *`email-address`*	デバイスの担当者の E メール アドレスを設定します。最大 255 文字の英数字を E メール アドレス フォーマットで指定できます。 **(注)**　任意の有効な E メール アドレスを使用できます。スペースは使用できません。
ステップ 5	`switch(config-callhome)#` **`phone-contact`** *`international-phone-number`*	デバイスの担当者の電話番号を国際電話フォーマットで設定します。最大 17 文字の英数字を国際フォーマットで指定できます。 **(注)**　スペースは使用できません。数字の前に、必ず **+** プレフィックスを使用してください。
ステップ 6	`switch(config-callhome)#` **`streetaddress`** *`address`*	デバイスの担当者の住所を、スペースを含めて英数字で設定します。スペースを含めて最大 255 文字の英数字を指定できます。
ステップ 7	`switch(config-callhome)#` **`contract-id`** *`contract-number`*	(任意)サービス契約からこのデバイスの契約番号を設定します。契約番号は、最大 255 文字の英数字を自由なフォーマットで指定できます。

	コマンド	目的
ステップ 8	switch(config-callhome)# **customer-id** *customer-number*	(任意)サービス契約からこのデバイスのカスタマー番号を設定します。カスタマー番号は、最大 255 文字の英数字を自由なフォーマットで指定できます。
ステップ 9	switch(config-callhome)# **site-id** *site-number*	(任意)このデバイスのサイト番号を設定します。サイト番号は、最大 255 文字の英数字を自由なフォーマットで指定できます。
ステップ 10	switch(config-callhome)# **switch-priority** *number*	(任意)このデバイスのスイッチ プライオリティを設定します。指定できる範囲は 0 ～ 7 です。0 は最高のプライオリティを、7 は最低のプライオリティを示します。デフォルト値は 7 です。 **(注)** スイッチのプライオリティは、運用要員または TAC サポート要員によって、最初に対処すべき Call Home メッセージを決定するために使用されます。各スイッチから送信される重大度が同じ Call Home アラートに優先順位を設定できます。
ステップ 11	switch(config-callhome)# **show callhome**	(任意)Call Home 設定の概要を示します。
ステップ 12	switch(config)# **copy running-config startup-config**	(任意)この設定の変更を保存します。

次に、Call Home に関する契約情報を設定する例を示します。

```
switch# configuration terminal
switch(config)# snmp-server contact personname@companyname.com
switch(config)# callhome
switch(config-callhome)# email-contact admin@Mycompany.com
switch(config-callhome)# phone-contact +1-800-123-4567
switch(config-callhome)# street-address 123 Anystreet st. Anytown,AnyWhere
```

宛先プロファイルの作成

ユーザ定義の宛先プロファイルを作成し、新しい宛先プロファイルにメッセージ フォーマットを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **callhome**	Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome)# **destination-profile** *name* **format** {**XML** | **full-txt** | **short-txt**}	新しい宛先プロファイルを作成し、そのプロファイルのメッセージ フォーマットを設定します。名前は、最大 31 文字の英数字で指定できます。

	コマンド	目的
ステップ 4	`switch(config-callhome)# show callhome destination-profile [profile name]`	(任意)1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	`switch(config)# copy running-config startup-config`	(任意)この設定の変更を保存します。

次に、Call Home の宛先プロファイルを作成する例を示します。

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# destination-profile Noc101 format full-text
```

宛先プロファイルの変更

定義済みまたはユーザ定義の宛先プロファイルの次の属性を変更できます。

- 宛先アドレス:アラートの送信先となる実際のアドレス(トランスポート メカニズムに関係します)。
- メッセージ フォーマット:アラート送信に使用されるメッセージ フォーマット(フル テキスト、ショート テキスト、または XML)。
- メッセージ レベル:この宛先プロファイルの Call Home メッセージの重大度
- メッセージ サイズ:この宛先プロファイルの E メール アドレスに送信された Call Home メッセージの長さ

宛先プロファイルのアラート グループの設定の詳細については、「アラート グループと宛先プロファイルのアソシエーション」セクション(26-11 ページ)を参照してください。

(注) CiscoTAC-1 宛先プロファイルは変更または削除できません。

宛先プロファイルの属性を変更する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# callhome`	Call Home コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-callhome)# destination-profile { name | full-txt-destination | short-txt-destination} email-addr address`	ユーザ定義または定義済みの宛先プロファイルに E メール アドレスを設定します。 **ヒント**　宛先プロファイルには、最大 50 個の E メール アドレスを設定できます。

	コマンド	目的
ステップ 4	**destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **message-level** *number* 例: destination-profile full-txt-destination message-level 5	この宛先プロファイルの Call Home メッセージの重大度を設定します。Call Home 重大度が一致する、またはそれ以上であるアラートのみが、このプロファイルの宛先に送信されます。指定できる範囲は 0 ～ 9 です。9 は最大の重大度を示します。
ステップ 5	switch(config-callhome)# **destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **message-size** *number*	この宛先プロファイルの最大メッセージ サイズを設定します。値の範囲は 0 ～ 5000000 です。デフォルトのサイズは 2500000 です。ただし、メッセージのサイズが 5000000 を超えている場合、そのメッセージは自動的に削除されます。
ステップ 6	switch(config-callhome)# **show callhome destination-profile** [**profile** *name*]	(任意) 1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 7	switch(config)# **copy running-config startup-config**	(任意) この設定の変更を保存します。

次に、Call Home の宛先プロファイルを変更する例を示します。

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# destination-profile full-text-destination email-addr
person@place.com
switch(config-callhome)# destination-profile full-text-destination message-level 5
switch(config-callhome)# destination-profile full-text-destination message-size 10000
```

アラート グループと宛先プロファイルのアソシエーション

1 つまたは複数のアラート グループを 1 つの宛先プロファイルに関連付けるには、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **callhome**	Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome)# **destination-profile** *name* **alert-group** {**All** | **Configuration** |**Diagnostic** | **EEM** | **Cisco-TAC** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Crash** | **Test**}	アラート グループをこの宛先プロファイルにアソシエートします。キーワード **All** を使用して、すべてのアラート グループをこの宛先プロファイルにアソシエートします。

	コマンド	目的
ステップ 4	switch(config-callhome)# **show callhome destination-profile** [**profile** *name*]	(任意)1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	(任意)この設定の変更を保存します。

次に、すべてのアラート グループを宛先プロファイル Noc101 に関連付ける例を示します。

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# destination-profile Noc101 alert-group All
```

アラート グループへの show コマンドの追加

アラート グループに最大 5 つのユーザ定義 CLI **show** コマンドを割り当てる手順は、次のとおりです。

（注） CiscoTAC-1 宛先プロファイルには、ユーザ定義の CLI **show** コマンドを追加できません。

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **callhome**	Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome)# **alert-group** {**Configuration** | **Diagnostic** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test**} **user-def-cmd** *show-cmd*	**show** コマンド出力を、このアラート グループに送信された Call Home メッセージに追加します。**show** コマンドは二重引用符で囲む必要があります。有効な **show** コマンドだけが受け入れられます。
ステップ 4	switch(config-callhome)# **show callhome user-def-cmds**	(任意)アラート グループに追加されたすべてのユーザ定義 **show** コマンドに関する情報を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	(任意)この設定の変更を保存します。

次に、**show ip routing** コマンドを Cisco-TAC アラート グループに追加する例を示します。

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# alert-group Configuration user-def-cmd “show ip routing”
```

E メールの設定

Call Home 機能が動作するよう SMTP サーバ アドレスを設定します。送信元および返信先 E メール アドレスも設定できます。

E メールを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# callhome`	Call Home コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-callhome)# transport email smtp-server ip-address [port number] [use-vrf vrf-name]`	SMTP サーバを、ドメイン ネーム サーバ（DNS）名、IPv4 アドレス、または IPv6 アドレスのいずれかとして設定します。任意でポート番号を設定します。ポート範囲は 1 ～ 65535 です。デフォルトのポート番号は 25 です。 また、この SMTP サーバと通信する際に使用するよう任意で VRF を設定します。
ステップ 4	`switch(config-callhome)# transport email from email-address`	（任意）Call Home メッセージの送信元 E メール フィールドを設定します。
ステップ 5	`switch(config-callhome)# transport email reply-to email-address`	（任意）Call Home メッセージの返信先 E メール フィールドを設定します。
ステップ 6	`switch(config-callhome)# show callhome transport-email`	（任意）Call Home の E メール設定に関する情報を表示します。
ステップ 7	`switch(config)# copy running-config startup-config`	（任意）この設定の変更を保存します。

次に、Call Home メッセージの E メール オプションを設定する例を示します。

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# transport email smtp-server 192.0.2.10 use-vrf Red
switch(config-callhome)# transport email from person@company.com
switch(config-callhome)# transport email reply-to person@company.com
```

定期的なインベントリ通知の設定

ハードウェアのインベントリ情報に加えて、デバイス上でイネーブルになっているすべてのソフトウェア サービスおよび実行中のソフトウェア サービスのインベントリに関するメッセージを定期的に送信するようにスイッチを設定できます。スイッチは 2 つの Call Home 通知（定期的な設定メッセージと定期的なインベントリ メッセージ）を生成します。

定期的なインベントリ通知情報を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **callhome** **E**	Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome)# **periodic-inventory notification** [**interval** *days*][**timeofday** *time*]	定期的なインベントリ メッセージを設定します。インターバル範囲は 1 ～ 30 日です。デフォルト値は 7 です。timeofday 値は HH:MM 形式です。
ステップ 4	switch(config-callhome)# **show callhome**	(任意)Call Home に関する情報を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	(任意)この設定の変更を保存します。

次に、定期的なインベントリ メッセージを 20 日ごとに生成するよう設定する例を示します。

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# periodic-inventory notification interval 20
```

重複メッセージの抑制のディセーブル化

同じイベントについて受信する重複メッセージの数を制限できます。デフォルトでは、スイッチは同じイベントについて受信する重複メッセージの数を制限します。2 時間の時間枠内で送信された重複メッセージの数が 30 メッセージを超えると、同じアラート タイプの以降のメッセージは廃棄されます。

Call Home コンフィギュレーション モードで重複メッセージ抑制をディセーブルにする手順は、次のとおりです。

コマンド	目的
switch(config-callhome)# **no duplicate-message throttle**	Call Home の重複メッセージ抑制をディセーブルにします。デフォルトでは、イネーブルです。

Call Home のイネーブル化またはディセーブル化

担当者情報を設定した場合、Call Home 機能をイネーブルにできます。

Call Home コンフィギュレーション モードで Call Home をイネーブルにする手順は、次のとおりです。

コマンド	目的
switch(config-callhome)# **enable**	Call Home をイネーブルにします。デフォルトでは、ディセーブルです。

Call Home コンフィギュレーション モードで Call Home をディセーブルにする手順は、次のとおりです。

コマンド	目的
`switch(config-callhome)# no enable`	Call Home をディセーブルにします。デフォルトでディセーブル

Call Home の通信のテスト

テスト メッセージを生成して Call Home 通信をテストできます。

テスト Call Home メッセージを生成する手順は、次のとおりです。

コマンド	目的
`switch# callhome send diagnostic`	設定されたすべての宛先に指定の Call Home テスト メッセージを送信します。
`switch# callhome test`	設定されたすべての宛先にテスト メッセージを送信します。 **callhome test** および **callhome test inventory** コマンドがサポートされます。
`switch# callhome test inventory`	(任意)。

Call Home の設定の確認

Call Home 設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
`show callhome`	Call Home のステータスを表示します。
`show callhome destination-profile name`	1 つまたは複数の Call Home 宛先プロファイルを表示します。
`show callhome diagnostic signature`	Call Home の診断署名ファイルの属性と統計情報を表示します。
`show callhome smart-licensing`	Call Home のスマート ライセンス情報を表示します。
`show callhome transport-email`	Call Home の E メール設定を表示します。
`show callhome user-def-cmds`	任意のアラート グループに追加された CLI コマンドを表示します。
`show running-config [callhome | callhome-all]` `show startup-config callhome`	Call Home の実行コンフィギュレーションを表示します。

コマンド	目的
show startup-config callhome	Call Home のスタートアップ コンフィギュレーションを表示します。
show tech-support callhome	Call Home のテクニカル サポート出力を表示します。

Call Home の設定例

次の例では、CFS を使用して、宛先プロファイル Noc101 を作成し、Cisco-TAC アラート グループをそのプロファイルに関連付けて、連絡先と E メール情報をすべての CFS 対応デバイスに設定します。

```
configure terminal
 snmp-server contact person@company.com
 callhome
  email-contact admin@Mycompany.com
  phone-contact +1-800-123-4567
  street-address 123 Anystreet st. Anytown,AnyWhere
  destination-profile Noc101 full-text
  destination-profile full-text-destination email-addr person@company.com
  destination-profile full-text-destination message-level 5
  destination-profile Noc101 alert-group Configuration
  alert-group Configuration user-def-cmd “show ip routing”
  transport email smtp-server 192.0.2.10 use-vrf Red
 enable
  commit
```

デフォルト設定

表 26-3 に、Call Home パラメータのデフォルト設定を示します。

表 26-3　デフォルトの Call Home パラメータ

パラメータ	デフォルト
フル テキスト形式で送信されるメッセージの宛先メッセージ サイズ。	4000000
XML 形式で送信されるメッセージの宛先メッセージ サイズ。	4000000
ショート テキスト形式で送信されるメッセージの宛先メッセージ サイズ。	4000
ポートが指定されていない場合の SMTP サーバ ポート番号	25
プロファイルとのアラート グループの関連付け	フル テキスト宛先プロファイルおよびショート テキスト宛先プロファイルの場合はすべて。CiscoTAC-1 宛先プロファイルの場合は cisco-tac アラート グループ
形式タイプ	XML
Call Home メッセージ レベル。	0（ゼロ）

その他の関連資料

Call Home の実装に関連した情報については、次を参照してください。

- メッセージ フォーマット（26-17 ページ）
- フル テキスト形式での Syslog アラート通知の例（26-21 ページ）
- XML 形式での Syslog アラート通知の例（26-21 ページ）

メッセージ フォーマット

Call Home では、次のメッセージ フォーマットがサポートされます。

- ショート テキスト メッセージ フォーマット
- すべてのフル テキストと XML メッセージに共通のフィールド
- 対処的または予防的イベント メッセージに挿入されるフィールド
- インベントリ イベント メッセージの挿入フィールド
- ユーザが作成したテスト メッセージの挿入フィールド

表 26-4 に、すべてのメッセージ タイプのショート テキスト形式のオプションを示します。

表 26-4　ショート テキスト メッセージ フォーマット

データ項目	説明
デバイス ID	設定されたデバイス名
日時スタンプ	起動イベントのタイム スタンプ
エラー判別メッセージ	起動イベントの簡単な説明（英語）
アラームの緊急度	エラー レベル（システム メッセージに適用されるエラー レベルなど）

表 26-5 に、フル テキストまたは XML の共通するイベント メッセージ フォーマットを示します。

表 26-5　すべてのフル テキストと XML メッセージに共通のフィールド

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
Time stamp	ISO 時刻通知でのイベントの日付/タイム スタンプ *YYYY-MM-DD HH:MM:SS GMT+HH:MM*.	/aml/header/time
メッセージ名	メッセージの名前。具体的なイベント名のリストは表 26-4に示されています。	/aml/header/name
メッセージ タイプ	リアクティブまたはプロアクティブなどのメッセージ タイプの名前	/aml/header/type
メッセージ グループ	Syslog などのアラート グループの名前	/aml/header/group
重大度	メッセージの重大度（「Call Home のメッセージ レベル」セクション（26-5 ページ）を参照）。	/aml/header/level

表 26-5　すべてのフル テキストと XML メッセージに共通のフィールド（続き）

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
送信元 ID	ルーティングのための製品タイプ。具体的に Catalyst 6500。	/aml/header/source
デバイス ID	メッセージを生成したエンド デバイスの Unique Device Identifier（UDI）。メッセージがデバイスに対して固有でない場合は、このフィールドを空にする必要があります。形式は、*type@Sid@serial*。 • *type* は、バックプレーン IDPROM からの製品の型番。 • @ は区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：WS-C6509@C@12345678	/aml/ header/deviceId
Customer ID	サポート サービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド。	/aml/ header/customerID
契約 ID	サポート サービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド。	/aml/ header /contractId
サイト ID	シスコが提供したサイト ID または別のサポート サービスにとって意味のあるその他のデータに使用されるオプションのユーザ設定可能なフィールド。	/aml/ header/siteId
サーバ ID	デバイスからメッセージが生成された場合、これはデバイスの Unique Device Identifier（UDI）フォーマットです。 形式は、*type@Sid@serial*。 • *type* は、バックプレーン IDPROM からの製品の型番。 • @ は区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：WS-C6509@C@12345678	/aml/header/serverId
メッセージの説明	エラーを説明するショート テキスト	/aml/body/msgDesc
デバイス名	イベントが発生したノード（デバイスのホスト名）	/aml/body/sysName
担当者名	イベントが発生したノード関連の問題について問い合わせる担当者名	/aml/body/sysContact
連絡先 E メール	この装置の担当者の E メール アドレス	/aml/body/sysContactEmail
Contact phone number	このユニットの連絡先である人物の電話番号。	/aml/body/sysContactPhone Number
住所	この装置関連の返品許可（RMA）部品の送付先住所を保存するオプション フィールド	/aml/body/sysStreetAddress

表 26-5　すべてのフル テキストと XML メッセージに共通のフィールド（続き）

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
モデル名	デバイスのモデル名（製品ファミリ名に含まれる具体的なモデル）	/aml/body/chassis/name
Serial number	ユニットのシャーシのシリアル番号。	/aml/body/chassis/serialNo
シャーシの部品番号	シャーシの最上アセンブリ番号。	/aml/body/chassis/partNo

特定のアラート グループ メッセージの固有のフィールドは、ここに挿入されます。

このアラート グループに対して複数の CLI コマンドが実行されると、次のフィールドが繰り返される場合があります。		
コマンド出力名	実行された CLI コマンドの正確な名前	/aml/attachments/attachment/name
添付タイプ	特定のコマンド出力	/aml/attachments/attachment/type
MIME タイプ	プレーン テキストまたは符号化タイプ	/aml/attachments/attachment/mime
コマンド出力テキスト	自動的に実行されたコマンドの出力（「Call Home アラート グループ」セクション（26-3 ページ）を参照）。	/aml/attachments/attachment/atdata

表 26-6 に、フル テキストまたは XML のリアクティブ イベント メッセージを示します。

表 26-6　対処的または予防的イベント メッセージに挿入されるフィールド

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
シャーシのハードウェア バージョン	シャーシのハードウェア バージョン。	/aml/body/chassis/hwVersion
スーパーバイザ モジュール ソフトウェア バージョン	最上レベルのソフトウェア バージョン。	/aml/body/chassis/swVersion
影響のある FRU の名前	イベント メッセージを生成する関連 FRU の名前	/aml/body/fru/name
影響のある FRU のシリアル番号	関連 FRU のシリアル番号	/aml/body/fru/serialNo
影響のある FRU の製品番号	関連 FRU の部品番号	/aml/body/fru/partNo
FRU スロット	イベント メッセージを生成する FRU のスロット番号	/aml/body/fru/slot

表 26-6　対処的または予防的イベント メッセージに挿入されるフィールド（続き）

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
FRU ハードウェア バージョン	関連 FRU のハードウェア バージョン	/aml/body/fru/hwVersion
FRU ソフトウェア バージョン	関連 FRU で稼働しているソフトウェア バージョン	/aml/body/fru/swVersion

表 26-7 に、フル テキストまたは XML のインベントリ イベント メッセージを示します。

表 26-7　インベントリ イベント メッセージの挿入フィールド

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
シャーシのハードウェア バージョン	シャーシのハードウェア バージョン	/aml/body/chassis/hwVersion
スーパーバイザ モジュール ソフトウェア バージョン	最上レベルのソフトウェア バージョン。	/aml/body/chassis/swVersion
FRU name	イベント メッセージを生成する関連 FRU の名前	/aml/body/fru/name
FRU s/n	FRU のシリアル番号	/aml/body/fru/serialNo
FRU 製品番号	FRU の部品番号	/aml/body/fru/partNo
FRU スロット	FRU のスロット番号	/aml/body/fru/slot
FRU ハードウェア バージョン	FRU のハードウェア バージョン	/aml/body/fru/hwVersion
FRU ソフトウェア バージョン	FRU で稼働しているソフトウェア バージョン	/aml/body/fru/swVersion

表 26-8 に、フル テキストまたは XML のユーザ生成のテスト メッセージを示します。

表 26-8　ユーザが作成したテスト メッセージの挿入フィールド

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
プロセス ID	固有のプロセス ID。	/aml/body/process/id
Process state	プロセスの状態（実行中、中止など）。	/aml/body/process/processState
Process exception	原因コードの例外。	/aml/body/process/exception

フル テキスト形式での Syslog アラート通知の例

次の例では、Syslog ポート アラート グループ通知のフル テキスト形式を示します。

```
source:MDS9000
Switch Priority:7
Device Id:WS-C6509@C@FG@07120011
Customer Id:Example.com
Contract Id:123
Site Id:San Jose
Server Id:WS-C6509@C@FG@07120011
Time of Event:2004-10-08T11:10:44
Message Name:SYSLOG_ALERT
Message Type:Syslog
Severity Level:2
System Name:10.76.100.177
Contact Name:User Name
Contact Email:admin@yourcompany.com
Contact Phone:+1 408 555-1212
Street Address:#1234 Picaboo Street, Any city, Any state, 12345
Event Description:2006 Oct  8 11:10:44 10.76.100.177 %PORT-5-IF_TRUNK_UP: %$VLAN 1%$
Interface e2/5, vlan 1 is up

syslog_facility:PORT
start chassis information:
Affected Chassis:WS-C6509
Affected Chassis Serial Number:FG@07120011
Affected Chassis Hardware Version:0.104
Affected Chassis Software Version:3.1(1)
Affected Chassis Part No:73-8607-01
end chassis information:
```

XML 形式での Syslog アラート通知の例

次の例では、Syslog ポート アラート グループ通知の XML を示します。

```
From: example
Sent: Wednesday, April 25, 2007 7:20 AM
To: User (user)
Subject: System Notification From Router - syslog - 2007-04-25 14:19:55
GMT+00:00

<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.example.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.example.com/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.example.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.example.com/appliance/uri</aml-session:From>
<aml-session:MessageId>M2:69000101:C9D9E20B</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.example.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.example.com/2005/05/callhome/syslog</aml-block:Type>
```

```
<aml-block:CreationDate>2007/04/25 14:19:55 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>Cat6500</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G3:69000101:C9F9E20C</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>2</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:Call Home xmlns:ch="http://www.example.com/2005/05/callhome" version="1.0">
<ch:EventTime>2007/04/25 14:19:55 GMT+00:00</ch:EventTime>
<ch:MessageDescription>03:29:29: %CLEAR-5-COUNTERS: Clear counter on all interfaces by
console</ch:MessageDescription>
<ch:Event>
<ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>Catalyst 6500 Series Switches</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>user@example.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId>12345</ch:CustomerId>
<ch:SiteId>building 1</ch:SiteId>
<ch:ContractId>abcdefg12345</ch:ContractId>
<ch:DeviceId>WS-C6509@C@69000101</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>Router</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>user@example.com</ch:ContactEmail>
<ch:ContactPhoneNumber>+1 408 555-1212</ch:ContactPhoneNumber>
<ch:StreetAddress>270 E. Tasman Drive, San Jose, CA</ch:StreetAddress>
</ch:SystemInfo>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.example.com/rme/4.0">
<rme:Model>WS-C6509</rme:Model>
<rme:HardwareVersion>1.0</rme:HardwareVersion>
<rme:SerialNumber>69000101</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="73-3438-03 01" />
<rme:AD name="SoftwareVersion" value="4.0(20080421:012711)" />
</rme:AdditionalInformation>
</rme:Chassis>
</ch:Device>
</ch:Call Home>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 53 messages logged, xml disabled,
```

```
                    filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                    filtering disabled
    Buffer logging: level debugging, 53 messages logged, xml disabled,
                   filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 72 message lines logged

Log Buffer (8192 bytes):

00:00:54: curr is 0x20000

00:00:54: RP: Currently running ROMMON from F2 region
0:01:05: %SYS-5-CONFIG_I: Configured from memory by console
00:01:09: %SYS-5-RESTART: System restarted --
Cisco IOS Software, s72033_rp Software (s72033_rp-ADVENTERPRISEK9_DBG-VM), Experimental
Version 12.2(20070421:012711)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 15:54 by xxx

Firmware compiled 11-Apr-07 03:34 by integ Build [100]


00:01:01: %PFREDUN-6-ACTIVE: Initializing as ACTIVE processor for this switch

00:01:01: %SYS-3-LOGGER_FLUSHED: System was paused for 00:00:00 to ensure console
debugging output.

00:03:00: SP: SP: Currently running ROMMON from F1 region
00:03:07: %C6K_PLATFORM-SP-4-CONFREG_BREAK_ENABLED: The default factory setting for config
register is 0x2102.It is advisable to retain 1 in 0x2102 as it prevents returning to
ROMMON when break is issued.

00:03:18: %SYS-SP-5-RESTART: System restarted --
Cisco IOS Software, s72033_sp Software (s72033_sp-ADVENTERPRISEK9_DBG-VM), Experimental
Version 12.2(20070421:012711)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 18:00 by xxx
00:03:18: %SYS-SP-6-BOOTTIME: Time taken to reboot after reload =  339 seconds
00:03:18: %OIR-SP-6-INSPS: Power supply inserted in slot 1
00:03:18: %C6KPWR-SP-4-PSOK: power supply 1 turned on.
00:03:18: %OIR-SP-6-INSPS: Power supply inserted in slot 2
00:01:09: %SSH-5-ENABLED: SSH 1.99 has been enabled
00:03:18: %C6KPWR-SP-4-PSOK: power supply 2 turned on.
00:03:18: %C6KPWR-SP-4-PSREDUNDANTMISMATCH: power supplies rated outputs do not match.
00:03:18: %C6KPWR-SP-4-PSREDUNDANTBOTHSUPPLY: in power-redundancy mode, system is
operating on both power supplies.
00:01:10: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:01:10: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:03:20: %C6KENV-SP-4-FANHIOUTPUT: Version 2 high-output fan-tray is in effect
00:03:22: %C6KPWR-SP-4-PSNOREDUNDANCY: Power supplies are not in full redundancy, power
usage exceeds lower capacity supply
00:03:26: %FABRIC-SP-5-FABRIC_MODULE_ACTIVE: The Switch Fabric Module in slot 6 became
active.
00:03:28: %DIAG-SP-6-RUN_MINIMUM: Module 6: Running Minimal Diagnostics...
00:03:50: %DIAG-SP-6-DIAG_OK: Module 6: Passed Online Diagnostics
00:03:50: %OIR-SP-6-INSCARD: Card inserted in slot 6, interfaces are now online
0:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 3: Running Minimal Diagnostics...
0:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 7: Running Minimal Diagnostics...
0:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 9: Running Minimal Diagnostics...
00:01:51: %MFIB_CONST_RP-6-REPLICATION_MODE_CHANGE: Replication Mode Change
Detected.Current system replication mode is Ingress
0:04:01: %DIAG-SP-6-DIAG_OK: Module 3: Passed Online Diagnostics
```

```
00:04:01: %OIR-SP-6-DOWNGRADE: Fabric capable module 3 not at an appropriate hardware
revision level, and can only run in flowthrough mode
0:04:02: %OIR-SP-6-INSCARD: Card inserted in slot 3, interfaces are now online
0:04:11: %DIAG-SP-6-DIAG_OK: Module 7: Passed Online Diagnostics
0:04:14: %OIR-SP-6-INSCARD: Card inserted in slot 7, interfaces are now online
0:04:35: %DIAG-SP-6-DIAG_OK: Module 9: Passed Online Diagnostics
0:04:37: %OIR-SP-6-INSCARD: Card inserted in slot 9, interfaces are now online
00:00:09: DaughterBoard (Distributed Forwarding Card 3)

Firmware compiled 11-Apr-07 03:34 by integ Build [100]


00:00:22: %SYS-DFC4-5-RESTART: System restarted --
Cisco DCOS Software, c6lc2 Software (c6lc2-SPDBG-VM), Experimental Version
4.0(20080421:012711)
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 26-Apr-08 17:20 by xxx
00:00:23: DFC4: Currently running ROMMON from F2 region
00:00:25: %SYS-DFC2-5-RESTART: System restarted --
Cisco IOS Software, c6slc Software (c6slc-SPDBG-VM), Experimental Version
12.2(20070421:012711)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-08 16:40 by username1
00:00:26: DFC2: Currently running ROMMON from F2 region
0:04:56: %DIAG-SP-6-RUN_MINIMUM: Module 4: Running Minimal Diagnostics...
00:00:09: DaughterBoard (Distributed Forwarding Card 3)

Firmware compiled 11-Apr-08 03:34 by integ Build [100]

slot_id is 8

00:00:31: %FLASHFS_HES-DFC8-3-BADCARD: /bootflash:: The flash card seems to be corrupted
00:00:31: %SYS-DFC8-5-RESTART: System restarted --
Cisco DCOS Software, c6lc2 Software (c6lc2-SPDBG-VM), Experimental Version
4.0(20080421:012711)
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 26-Apr-08 17:20 by username1
00:00:31: DFC8: Currently running ROMMON from S (Gold) region
0:04:59: %DIAG-SP-6-RUN_MINIMUM: Module 2: Running Minimal Diagnostics...
0:05:12: %DIAG-SP-6-RUN_MINIMUM: Module 8: Running Minimal Diagnostics...
0:05:13: %DIAG-SP-6-RUN_MINIMUM: Module 1: Running Minimal Diagnostics...
00:00:24: %SYS-DFC1-5-RESTART: System restarted --
Cisco DCOS Software, c6slc Software (c6slc-SPDBG-VM), Experimental Version
4.0(20080421:012711)
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 26-Apr-08 16:40 by username1
00:00:25: DFC1: Currently running ROMMON from F2 region
0:05:30: %DIAG-SP-6-DIAG_OK: Module 4: Passed Online Diagnostics
00:05:31: %SPAN-SP-6-SPAN_EGRESS_REPLICATION_MODE_CHANGE: Span Egress HW Replication Mode
Change Detected.Current replication mode for unused asic session 0 is Centralized
00:05:31: %SPAN-SP-6-SPAN_EGRESS_REPLICATION_MODE_CHANGE: Span Egress HW Replication Mode
Change Detected.Current replication mode for unused asic session 1 is Centralized
0:05:31: %OIR-SP-6-INSCARD: Card inserted in slot 4, interfaces are now online
0:06:02: %DIAG-SP-6-DIAG_OK: Module 1: Passed Online Diagnostics
0:06:03: %OIR-SP-6-INSCARD: Card inserted in slot 1, interfaces are now online
0:06:31: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
0:06:33: %OIR-SP-6-INSCARD: Card inserted in slot 2, interfaces are now online
00:04:30: %XDR-6-XDRIPCNOTIFY: Message not sent to slot 4/0 (4) because of IPC error
timeout.Disabling linecard.(Expected during linecard OIR)
0:06:59: %DIAG-SP-6-DIAG_OK: Module 8: Passed Online Diagnostics
00:06:59: %OIR-SP-6-DOWNGRADE_EARL: Module 8 DFC installed is not identical to system PFC
and will perform at current system operating mode.
0:07:06: %OIR-SP-6-INSCARD: Card inserted in slot 8, interfaces are now online
```

```
Router#]]></aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```

その他の関連資料

CHAPTER 27

SNMP の設定

この章では、Cisco Nexus 5000 シリーズ のスイッチに SNMP 機能を設定する方法について説明します。

この章は、次の項で構成されています。

- SNMP について（27-1 ページ）
- 設定時の注意事項および制限事項（27-5 ページ）
- SNMP の設定（27-5 ページ）
- SNMP の設定の確認（27-12 ページ）
- SNMP の設定例（27-12 ページ）
- デフォルト設定値（27-13 ページ）

SNMP について

簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェント間の通信用メッセージ フォーマットを提供する、アプリケーションレイヤ プロトコルです。SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。

この項では、次のトピックについて取り上げます。

- SNMP 機能の概要（27-1 ページ）
- SNMP 通知（27-2 ページ）
- SNMPv3（27-2 ページ）

SNMP 機能の概要

SNMP フレームワークは 3 つの部分で構成されます。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスのアクティビティを制御し、モニタリングするシステム
- SNMP エージェント：デバイスのデータを維持し、必要に応じてこれらのデータを管理システムに報告する、管理対象デバイス内のソフトウェア コンポーネント。Cisco Nexus 5000 シリーズ スイッチはエージェントおよび MIB をサポートします。SNMP エージェントをイネーブルにするには、マネージャとエージェントの関係を定義する必要があります。
- 管理情報ベース（Management Information Base）：SNMP エージェントの管理対象オブジェクトのコレクション

SNMP は、RFC 3411 ～ 34180 で定義されています。

（注）　Cisco NX-OS は、イーサネット MIB の SNMP セットをサポートしません。

Cisco Nexus 5000 シリーズ スイッチは、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。SNMPv1 と SNMPv2c は、ともにコミュニティベース形式のセキュリティを使用します。

SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。これらの通知では、要求を SNMP マネージャから送信する必要はありません。通知は、不正なユーザ認証、再起動、接続の切断、隣接ルータとの接続の切断、その他の重要なイベントを表示します。

Cisco Nexus 5000 シリーズ スイッチは、トラップまたはインフォームとして SNMP 通知を生成します。トラップの信頼性はインフォームより低くなります。SNMP マネージャはトラップを受信しても確認応答（ACK）を送信しないからです。Cisco Nexus 5000 シリーズ スイッチでは、トラップを受信したかどうかを判断できません。インフォーム要求を受信する SNMP マネージャは、SNMP 応答プロトコル データ ユニット（PDU）でメッセージの受信を確認応答します。Cisco Nexus 5000 シリーズ スイッチが応答を受信しない場合、インフォーム要求を再度送信できます。

複数のホスト レシーバに通知を送信するよう Cisco Nexus 5000 シリーズ スイッチを設定できます。ホスト レシーバーの詳細については、「SNMP 通知レシーバーの設定」セクション（27-7 ページ）を参照してください。

SNMPv3

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュア アクセスを実現します。SNMPv3 が提供するセキュリティ機能は次のとおりです。

- メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- 認証：メッセージのソースが有効かどうかを判別します。
- 暗号化：許可されていないソースにより判読されないように、パケットの内容のスクランブルを行います。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

ここでは、次の内容について説明します。

- SNMPv1、SNMPv2、SNMPv3 のセキュリティ モデルおよびセキュリティ レベル（27-3 ページ）
- ユーザベースのセキュリティ モデル（27-3 ページ）
- コマンドライン インターフェイス（CLI）および SNMP ユーザの同期（27-4 ページ）
- グループベースの SNMP アクセス（27-5 ページ）

SNMPv1、SNMPv2、SNMPv3 のセキュリティ モデルおよびセキュリティ レベル

セキュリティ レベルは、SNMP メッセージを開示から保護する必要があるかどうか、およびメッセージを認証するかどうか判断します。セキュリティ モデル内のさまざまなセキュリティ レベルは、次のとおりです。

- noAuthNoPriv：認証または暗号化を実行しないセキュリティ レベル。
- authNoPriv：認証は実行するが、暗号化を実行しないセキュリティ レベル。
- authPriv：認証と暗号化両方を実行するセキュリティ レベル。

SNMPv1、SNMPv2c、および SNMPv3 の 3 つのセキュリティ モデルを使用できます。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP メッセージの処理中に適用されるセキュリティ メカニズムが決まります。

表 27-1 に、セキュリティ モデルとセキュリティ レベルの組み合わせの意味を示します。

ユーザベースのセキュリティ モデル

表 27-1　SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v3	noAuthNoPriv	Username	No	ユーザ名の照合を使用して認証します。
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	No	Hash-Based Message Authentication Code（HMAC）メッセージ ダイジェスト 5（MD5）アルゴリズムまたは HMAC Secure Hash Algorithm（SHA）アルゴリズムに基づいて認証します。
v3	authPriv	HMAC-MD5 または HMAC-SHA	DES	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格（DES）の 56 ビット暗号化、および暗号ブロック連鎖（CBC）DES（DES-56）標準に基づいた認証を提供します。

SNMPv3 ユーザベース セキュリティ モデル（USM）は SNMP メッセージレベル セキュリティを参照し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されていないことを保証します。また、データ シーケンスが、通常発生するものよりも高い頻度で変更されていないことを保証します。
- メッセージ発信元の認証：受信データを発信したユーザのアイデンティティが確認されたことを保証します。
- メッセージの機密性：情報が使用不可であること、または不正なユーザ、エンティティ、またはプロセスに開示されないことを保証します。

SNMPv3 は、設定済みユーザによる管理動作のみを許可し、SNMP メッセージを暗号化します。

Cisco Nexus 5000 シリーズは、次の 2 つの SNMPv3 認証プロトコルを使用します。

- HMAC-MD5-96 認証プロトコル
- HMAC-SHA-96 認証プロトコル

Cisco Nexus 5000 シリーズ は、SNMPv3 メッセージ暗号化用プライバシー プロトコルの 1 つとして、Advanced Encryption Standard（AES）を使用し、RFC 3826 に準拠します。

priv オプションで、SNMP セキュリティ暗号化方式として、DES または 128 ビット AES を選択できます。**priv** オプションを **aes-128** トークンと併用すると、プライバシー パスワードは 128 ビット AES キーの生成に使用されます。AES のプライバシー パスワードは最小で 8 文字です。パスフレーズをクリア テキストで指定する場合、最大 64 文字を指定できます。ローカライズド キーを使用する場合は、最大 130 文字を指定できます。

（注） 外部の AAA サーバを使用して SNMPv3 を使う場合、外部 AAA サーバのユーザ設定でプライバシー プロトコルに AES を指定する必要があります。

コマンドライン インターフェイス（CLI）および SNMP ユーザの同期

SNMPv3 ユーザ管理は、Access Authentication and Accounting（AAA）サーバ レベルで集中化できます。この中央集中型ユーザ管理により、Cisco Nexus 5000 シリーズの SNMP エージェントは AAA サーバのユーザ認証サービスを利用できます。ユーザ認証が検証されると、SNMP PDU の処理が進行します。AAA サーバはユーザ グループ名の格納にも使用されます。SNMP はグループ名を使用して、スイッチでローカルに使用できるアクセス ポリシーまたはロール ポリシーを適用します。

ユーザ グループ、ロール、またはパスワードの設定が変更されると、SNMP と AAA の両方のデータベースが同期化されます。

Cisco Nexus 5000 シリーズは、次のようにユーザ設定を同期化します。

- **snmp-server user** コマンドで指定された **auth** パスフレーズは、CLI ユーザのパスワードになります。
- **username** コマンドで指定されたパスワードは、SNMP ユーザの **auth** および **priv** パスフレーズになります。
- SNMP または CLI のいずれかを使用してユーザを削除すると、SNMP と CLI の両方の該当ユーザが削除されます。
- ユーザとロールの対応関係の変更は、SNMP と CLI で同期化されます。

（注） パスフレーズ/パスワードをローカライズド キー/暗号化形式で設定すると、Cisco Nexus 5000 シリーズはパスワードを同期化しません。

グループベースの SNMP アクセス

（注）　グループが業界全体で使用されている標準 SNMP 用語なので、この SNMP の項では、ロールのことをグループと言います。

SNMP アクセス権は、グループ別に編成されます。SNMP 内の各グループは、CLI を使用する場合のロールに似ています。各グループは 3 つのアクセス権により定義されます。つまり、読み取りアクセス、書き込みアクセス、および通知アクセスです。それぞれのアクセスを、各グループでイネーブルまたはディセーブルに設定できます。

ユーザ名が作成され、ユーザのロールが管理者によって設定され、ユーザがそのロールに追加されていれば、そのユーザはエージェントとの通信を開始できます。

設定時の注意事項および制限事項

SNMP には、次の注意事項および制限事項があります。

- Cisco NX-OS は、イーサネット MIB への読み取り専用アクセスをサポートします。

SNMP の設定

この項では、次のトピックについて取り上げます。

- SNMP ユーザの設定（27-6 ページ）
- SNMP メッセージ暗号化の適用（27-6 ページ）
- SNMPv3 ユーザに対する複数のロールの割り当て（27-7 ページ）
- SNMP コミュニティの作成（27-7 ページ）
- SNMP 通知レシーバーの設定（27-7 ページ）
- 通知ターゲット ユーザの設定（27-8 ページ）
- SNMP 通知のイネーブル化（27-9 ページ）
- linkUp/linkDown 通知の設定（27-10 ページ）
- インターフェイスでの Up/Down 通知のディセーブル化（27-11 ページ）
- TCP での SNMP に対するワンタイム認証のイネーブル化（27-11 ページ）
- SNMP スイッチの連絡先および場所の情報の割り当て（27-11 ページ）

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

SNMP ユーザの設定

SNMP のユーザを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **snmp-server user** *name* [**auth** {md5 | sha} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*][**localizedkey**]]	認証およびプライバシー パラメータのある SNMP ユーザを設定します。
ステップ 3	switch(config-callhome)# **show snmp user**	(任意)1 人または複数の SNMP ユーザに関する情報を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	(任意)この設定の変更を保存します。

SNMP メッセージ暗号化の適用

着信要求に認証または暗号化が必要となるよう SNMP を設定できます。デフォルトでは、SNMP エージェントは、認証と暗号化なしで SNMPv3 メッセージを受け入れます。プライバシーを適用する場合、Cisco Nexus 5000 シリーズは、noAuthNoPriv または uthNoPriv のどちらかの securityLevel パラメータを使用しているすべての SNMPv3 PDU 要求に対して、authorization Error で応答します。

グローバル コンフィギュレーション モードで 1 人のユーザに SNMP メッセージ暗号化を適用する手順は、次のとおりです。

コマンド	目的
switch(config)# **snmp-server user** *name* **enforcePriv**	このユーザに対して SNMP メッセージ暗号化を適用します。

グローバル コンフィギュレーション モードですべてのユーザに SNMP メッセージ暗号化を適用する手順は、次のとおりです。

コマンド	目的
switch(config)# **snmp-server globalEnforcePriv**	すべてのユーザに対して SNMP メッセージ暗号化を適用します。

SNMPv3 ユーザに対する複数のロールの割り当て

SNMP ユーザを作成した後で、そのユーザに複数のロールを割り当てることができます。

（注）　他のユーザにロールを割り当てることができるのは、network-admin ロールに属するユーザだけです。

グローバル コンフィギュレーション モードで 1 人の SNMP ユーザにロールを割り当てる手順は、次のとおりです。

コマンド	目的
switch(config)# **snmp-server user** *name group*	この SNMP ユーザと設定されたユーザ ロールをアソシエートします。

SNMP コミュニティの作成

SNMPv1 または SNMPv2c の SNMP コミュニティを作成できます。

グローバル コンフィギュレーション モードで SNMP コミュニティ文字列を作成する手順は、次のとおりです。

コマンド	目的
switch(config)# **snmp-server community** *name group* {**ro** | **rw**}	SNMP コミュニティ ストリングを作成します。

SNMP 通知レシーバーの設定

複数のホスト レシーバーに対して SNMP 通知を生成するよう Cisco Nexus 5000 シリーズを設定できます。

グローバル コンフィギュレーション モードで SNMPv1 トラップのホスト レシーバを設定する手順は、次のとおりです。

コマンド	目的
switch(config)# **snmp-server host** *ip-address* **traps** {**version 1**} *community* [**udp_port** *number*]	SNMPv1 トラップのホスト レシーバを設定します。コミュニティは、最大 255 文字の英数字で指定できます。UDP ポート番号の範囲は 0 ～ 65535 です。

グローバル コンフィギュレーション モードで SNMPv2c トラップまたはインフォームのホスト レシーバを設定する手順は、次のとおりです。

コマンド	目的
switch(config)# **snmp-server host** *ip-address* {**traps** | **informs**} **version 2c** *community* [**udp_port** *number*]	SNMPv2c トラップまたはインフォームのホスト レシーバを設定します。コミュニティは、最大 255 文字の英数字で指定できます。UDP ポート番号の範囲は 0 ～ 65535 です。

グローバル コンフィギュレーション モードで SNMPv3 トラップまたはインフォームのホスト レシーバを設定する手順は、次のとおりです。

コマンド	目的
switch(config)# **snmp-server host** *ip-address* {**traps** | **informs**} **version 3** {**auth** | **noauth** | **priv** } *username* [**udp_port** *number*]	SNMPv2c トラップまたはインフォームのホスト レシーバを設定します。ユーザ名は、最大 255 文字の英数字で指定できます。UDP ポート番号の範囲は 0 ～ 65535 です。

次に、SNMPv3 インフォームのホスト レシーバを設定する例を示します。

```
switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS
```

（注）　SNMP マネージャは、SNMPv3 メッセージを認証し暗号解除するため、Cisco Nexus 5000 シリーズ デバイスの SNMP engineID に基づくユーザ クレデンシャル（authKey/PrivKey）を認識していなければなりません。

通知ターゲット ユーザの設定

SNMPv3 インフォーム通知を通知ホスト レシーバに送信するには、デバイスに通知ターゲット ユーザを設定する必要があります。

Cisco Nexus 5000 シリーズ スイッチは、通知ターゲット ユーザのクレデンシャルを使用して、設定した通知ホスト レシーバへの SNMPv3 インフォーム通知メッセージを暗号化します。

（注）　受信した INFORM PDU を認証し暗号解除するためには、通知ホスト レシーバが、インフォームを認証し暗号解除する Cisco Nexus 5000 シリーズ スイッチ内に設定されたクレデンシャルと同じユーザ クレデンシャルを保持している必要があります。

通知ターゲット ユーザを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
switch(config)# **snmp-server user** *name* [**auth** {md5 | sha} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*]	通知ホスト レシーバに対応した、指定した engineID を持つ通知ターゲット ユーザを設定します。engineID フォーマットは、コロンで区切られた 12 桁の 16 進数です。

次に、通知ターゲット ユーザを設定する例を示します。

```
switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh enginID
00:00:00:63:00:01:00:a1:ac:15:10:03
```

SNMP 通知のイネーブル化

通知をイネーブルまたはディセーブルにできます。通知名を指定しないと、Cisco Nexus 5000 シリーズは通知をすべてイネーブルにします。

表 27-2 に、Cisco Nexus 5000 シリーズ MIB の通知をイネーブルにする CLI コマンドを示します。

（注）　**snmp-server enable traps** CLI コマンドを使用すると、設定通知ホスト レシーバーによっては、トラップとインフォームの両方をイネーブルにできます。

表 27-2　SNMP 通知のイネーブル化

MIB	関連コマンド
すべての通知	**snmp-server enable traps**
CISCO-AAA-SERVER-MIB	**snmp-server enable traps aaa**
ENITY-MIB、 CISCO-ENTITY-FRU-CONTROL-MIB、 CISCO-ENTITY-SENSOR-MIB	**snmp-server enable traps entity** **snmp-server enable traps entity fru**
CISCO-LICENSE-MGR-MIB	**snmp-server enable traps license**
IF-MIB	**snmp-server enable traps link**
CISCO-PSM-MIB	**snmp-server enable traps port-security**
SNMPv2-MIB	**snmp-server enable traps snmp** **snmp-server enable traps snmp authentication**
CISCO-FCC-MIB	**snmp-server enable traps fcc**
CISCO-DM-MIB	**snmp-server enable traps fcdomain**
CISCO-NS-MIB	**snmp-server enable traps fcns**
CISCO-FCS-MIB	**snmp-server enable traps fcs discovery-complete** **snmp-server enable traps fcs request-reject**
CISCO-FDMI-MIB	**snmp-server enable traps fdmi**
CISCO-FSPF-MIB	**snmp-server enable traps fspf**
CISCO-PSM-MIB	**snmp-server enable traps port-security**
CISCO-RSCN-MIB	**snmp-server enable traps rscn** **snmp-server enable traps rscn els** **snmp-server enable traps rscn ils**
CISCO-ZS-MIB	**snmp-server enable traps zone** **snmp-server enable traps zone default-zone-behavior-change** **snmp-server enable traps zone merge-failure** **snmp-server enable traps zone merge-success** **snmp-server enable traps zone request-reject** **snmp-server enable traps zone unsupp-mem**

（注）　ライセンス通知は、デフォルトではイネーブルです。他の通知はすべて、デフォルトではディセーブルです。

グローバル コンフィギュレーション モードで指定の通知をイネーブルにするには、次の作業を行います。

コマンド	目的
switch(config)# **snmp-server enable traps**	すべての SNMP 通知をイネーブルにします。
switch(config)# **snmp-server enable traps aaa** [**server-state-change**]	AAA SNMP 通知をイネーブルにします。
switch(config)# **snmp-server enable traps entity** [**fru**]	ENTITY-MIB SNMP 通知をイネーブルにします。
switch(config)# **snmp-server enable traps license**	ライセンス SNMP 通知をイネーブルにします。
switch(config)# **snmp-server enable traps port-security**	ポート セキュリティ SNMP 通知をイネーブルにします。
switch(config)# **snmp-server enable traps snmp** [**authentication**]	SNMP エージェント通知をイネーブルにします。

linkUp/linkDown 通知の設定

デバイスに対して、イネーブルにする linkUp/linkDown 通知を設定できます。次のタイプの linkUp/linkDown 通知をイネーブルにできます。

- Cisco：Cisco Nexus 5000 シリーズ は、インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルの場合は、シスコ定義の通知（CISCO-IF-EXTENSION-MIB.my の cieLinkUp、cieLinkDown）だけを送信します。
- IETF：Cisco Nexus 5000 シリーズ は、インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルの場合は、定義されている変数バインドだけを IETF 定義の通知（IF-MIB の linkUp、linkDown）と一緒に送信します。
- IEFT extended：Cisco Nexus 5000 シリーズ は、インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルの場合は、IETF 定義の通知（IF-MIB の linkUp、linkDown）だけを送信します。Cisco Nexus 5000 シリーズ は、IF-MIB に定義されている変数バインドに加え、シスコに固有の変数バインドも送信します。これがデフォルト設定です。
- IEFT Cisco：Cisco Nexus 5000 シリーズ は、インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルの場合は、IF-MIB に定義された通知（linkUp、linkDown）および CISCO-IF-EXTENSION-MIB.my に定義された通知（cieLinkUp、cieLinkDown）を送信します。Cisco Nexus 5000 シリーズ は、linkUp および linkDown 通知に定義された変数バインドだけを送信します。
- IEFT extended Cisco：Cisco Nexus 5000 シリーズ は、インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルの場合は、IF-MIB に定義された通知（linkUp、linkDown）および CISCO-IF-EXTENSION-MIB.my に定義された通知（cieLinkUp、cieLinkDown）を送信します。Cisco Nexus 5000 シリーズ は、linkUp および linkDown 通知の IF-MIB に定義されている変数バインドに加え、シスコに固有の変数バインドも送信します。

グローバル コンフィギュレーション モードで linkUp/linkDown 通知のタイプを設定する手順は、次のとおりです。

コマンド	目的
switch(config)# **snmp-server enable traps link** [**cisco**] [**ietf** | **ietf-extended**]	リンク SNMP 通知をイネーブルにします。

インターフェイスでの Up/Down 通知のディセーブル化

個別のインターフェイスで linkUp および linkDown 通知をディセーブルにできます。フラッピング インターフェイス（Up と Down の間を頻繁に切り替わるインターフェイス）で、この制限通知を使用できます。

インターフェイス コンフィギュレーション モードでインターフェイスの linkUp/linkDown 通知をディセーブルにする手順は、次のとおりです。

コマンド	目的
switch(config-if)# **no snmp trap link-status**	インターフェイスの SNMP リンクステート トラップをディセーブルにします。デフォルトでは、イネーブルです。

TCP での SNMP に対するワンタイム認証のイネーブル化

TCP セッション上で SNMP に対するワンタイム認証をイネーブルにできます。

グローバル コンフィギュレーション モードで、TCP セッション上の SNMP に対するワンタイム認証をイネーブルにする手順は、次のとおりです。

コマンド	目的
switch(config)# **snmp-server tcp-session [auth]**	TCP セッション上で SNMP に対するワンタイム認証をイネーブルにします。デフォルトは無効です。

SNMP スイッチの連絡先および場所の情報の割り当て

32 文字までの長さで（スペースを含まない）のスイッチ コンタクト情報を指定できます。さらに、スイッチ ロケーションを指定できます。情報を割り当てる手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **snmp-server contact** *name*	sysContact（SNMP 担当者名）を設定します。

	コマンド	目的
ステップ 3	switch(config)# **snmp-server location** *name*	sysLocation（SNMP ロケーション）を設定します。
ステップ 4	switch(config-callhome)# **show snmp**	（任意）1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意）この設定の変更を保存します。

SNMP の設定の確認

SNMP 設定情報を表示するには、次の作業を行います。

コマンド	目的
show snmp	SNMP ステータスを表示します。
show snmp community	SNMP コミュニティ ストリングを表示します。
show snmp engineID	SNMP engineID を表示します。
show snmp group	SNMP ロールを表示します。
show snmp sessions	SNMP セッションを表示します。
show snmp trap	イネーブルまたはディセーブルである SNMP 通知を表示します。
show snmp user	SNMPv3 ユーザを表示します。

SNMP の設定例

次の例では、Cisco linkUp/linkDown 通知を 1 つの通知ホスト レシーバに送信するよう Cisco Nexus 5000 シリーズ を設定し、2 人の SNMP ユーザ（Admin および NMS）を定義します。

```
configuration terminal
 snmp-server contact Admin@company.com
 snmp-server user Admin auth sha abcd1234 priv abcdefgh
 snmp-server user NMS auth sha abcd1234 priv abcdefgh enginID
00:00:00:63:00:01:00:a1:ac:15:10:03
 snmp-server host 192.0.2.1 informs version 3 auth NMS
 snmp-server host 192.0.2.1
 snmp-server enable traps link cisco
```

デフォルト設定値

表 27-3 に、SNMP パラメータのデフォルト設定を示します。

表 27-3　デフォルトの SNMP パラメータ

パラメータ	デフォルト
ライセンス通知	enabled
linkUp/Down 通知タイプ	ietf-extended

CHAPTER 28

RMON の設定

この章では、RMON 機能を設定する方法について説明します。

この章は、次の項で構成されています。

- RMON について（28-1 ページ）
- 設定時の注意事項および制限事項（28-3 ページ）
- RMON の設定（28-3 ページ）
- RMON の設定の確認（28-5 ページ）
- RMON の設定例（28-5 ページ）
- 関連項目（28-5 ページ）
- デフォルト設定（28-6 ページ）

RMON について

RMON は、各種のネットワーク エージェントおよびコンソール システムがネットワーク モニタリング データを交換できるようにするための、Internet Engineering Task Force（IETF）標準モニタリング仕様です。Cisco NX-OS は、Cisco Nexus 5000 シリーズ スイッチを監視するための RMON アラーム、イベント、およびログをサポートします。

RMON アラームは、指定された期間、特定の管理情報ベース（MIB）オブジェクトをモニタリングし、指定されたしきい値でアラームを発生させ、別のしきい値でアラームをリセットします。アラームと RMON イベントを組み合わせて使用し、RMON アラームが発生したときにログ エントリまたは SNMP 通知を生成できます。

Cisco Nexus 5000 シリーズでは RMON はデフォルトでディセーブルに設定されており、イベントまたはアラームは設定されていません。RMON のアラームおよびイベントを設定するには、CLI または SNMP 準拠のネットワーク管理ステーションを使用します。

ここでは、次の内容について説明します。

- RMON アラーム（28-2 ページ）
- RMON イベント（28-2 ページ）

RMON アラーム

SNMP INTEGER タイプの解決を行う任意の MIB オブジェクトにアラームを設定できます。指定するオブジェクトは、標準のドット付き表記で表した既存の SNMP MIB オブジェクトでなければなりません（たとえば、1.3.6.1.2.1.2.2.1.14 は ifInOctets.14 を表します）。

アラームを作成する場合、次のパラメータを指定します。

- モニタリングする MIB オブジェクト
- サンプリング間隔：MIB オブジェクトのサンプル値を収集するのに Cisco Nexus 5000 シリーズ スイッチが使用する間隔
- サンプル タイプ：絶対サンプルは MIB オブジェクト値の現在のスナップショットを使用します。デルタ サンプルは連続した 2 つのサンプルを使用し、これらの差を計算します。
- 上限しきい値：Cisco Nexus 5000 シリーズ スイッチが上限アラームを発生させる、または下限アラームをリセットする場合の値
- 下限しきい値：Cisco Nexus 5000 シリーズ スイッチが下限アラームを発生させる、または上限アラームをリセットする場合の値
- イベント：アラーム（上限または下限）の発生時に Cisco Nexus 5000 シリーズ スイッチが実行するアクション

（注）　hcalarms オプションを使用して、アラームを 64 ビットの整数の MIB オブジェクトに設定します。

たとえば、エラー カウンタ MIB オブジェクトにデルタ タイプ上限アラームを設定できます。エラー カウンタ デルタがこの値を超えた場合、SNMP 通知を送信し、上限アラーム イベントを記録するイベントを発生させることができます。この上限アラームは、エラー カウンタのデルタ サンプルが下限しきい値を下回るまで再度発生しません。

（注）　下限しきい値には、上限しきい値よりも小さな値を指定してください。

RMON イベント

特定のイベントを各 RMON アラームにアソシエートさせることができます。RMON は次のイベント タイプをサポートします。

- SNMP 通知：関連したアラームが発生したときに、SNMP risingAlarm または fallingAlarm 通知を送信します。
- ログ：関連したアラームが発生した場合、RMON ログ テーブルにエントリを追加します。
- 両方：関連したアラームが発生した場合、SNMP 通知を送信し、RMON ログ テーブルにエントリを追加します。

下限アラームおよび上限アラームに異なるイベントを指定できます。

設定時の注意事項および制限事項

RMON には、次の注意事項および制限事項があります。

- SNMP 通知イベント タイプを使用するよう、SNMP ユーザを通知レシーバに設定する必要があります。
- 整数になる MIB オブジェクトに、RMON アラームのみを設定できます。

RMON の設定

この項では、次のトピックについて取り上げます。

- RMON アラームの設定（28-3 ページ）
- RMON イベントの設定（28-4 ページ）

（注）　Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

RMON アラームの設定

任意の整数の SNMP MIB オブジェクトに RMON アラームを設定できます。次の 2 つのタイプの SNMP アラームを設定できます。

- 32 ビット RMON アラーム
- 64 ビット大容量 RMON アラーム

32 ビット RMON アラームを設定するには、**rmon alarm** コマンドを使用します。64 ビット大容量 RMON アラームを設定するには、**rmon hcalarm** コマンドを使用します。

次のパラメータを任意で指定することもできます。

- 32 ビットおよび 64 ビット RMON アラームのイベント番号。上昇または下限しきい値が指定された制限を超えた場合、このイベント番号がアラームをトリガーします。*rising-event* または *falling-event* パラメータを使用して、イベント番号の値を指定します。範囲は 0 ～ 65535 です。値を指定しないと、イベント 0 がデフォルトになります。
- 32 ビット RMON アラームの上昇および下限しきい値。**rising-threshold** *value* コマンドまたは **falling-threshold** *value* コマンドを使用します。範囲は – 2147483647 ～ 214748364 です。
- 64 ビット RMON アラームの上昇しきい値。**rising-threshold-high** *value* コマンドを使用して、64 ビット上昇しきい値の上位 32 ビットを設定します。**rising-threshold-low** *value* コマンドを使用して、64 ビット上昇しきい値の下位 32 ビットを設定します。範囲は 0 ～ 4294967295 です。
- 64 ビット RMON アラームの下限しきい値。**falling-threshold-high** *value* コマンドを使用して、64 ビット下限しきい値の上位 32 ビットを設定します。**falling-threshold-low** *value* コマンドを使用して、64 ビット下限しきい値の下位 32 ビットを設定します。範囲は 0 ～ 4294967295 です。
- アラームのオーナー

SNMP ユーザが設定され、SNMP 通知がイネーブルであることを確認します（「SNMP の設定」セクション（27-5 ページ）を参照）。

RMON アラームを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **rmon alarm** *index mib-object sample-interval* {**absolute** | **delta**} **rising-threshold** *value* [*event-index*] **falling-threshold** *value* [*event-index*] [**owner** *name*]	32 ビット RMON アラームを作成します。値の範囲は、– 2147483647 ～ 2147483647 です。オーナー名は任意の英数字ストリングです。
	switch(config)# **rmon hcalarm** *index mib-object sample-interval* {**absolute** | **delta**} **rising-threshold-high** *value* **rising-threshold-low** *value* [*event-index*] **falling-threshold-high** *value* **falling-threshold-low** *value* [*event-index*] [**owner** *name*] [**storagetype** type]	64 ビット大容量 RMON アラームを作成します。値の範囲は、– 2147483647 ～ 2147483647 です。オーナー名は任意の英数字ストリングです。 ストレージ タイプの範囲は 1 ～ 5 です。
ステップ 3	switch(config)# **show rmon** {**alarms** | **hcalarms**}	(任意)RMON アラームまたは大容量アラームに関する情報を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	(任意)この設定の変更を保存します。

次に、RMON アラームを設定する例を示します。

```
switch# configure terminal
switch(config)# rmon alarm 20 1.3.6.1.2.1.2.2.1.14 2900 delta rising-threshold 1500 1
falling-threshold 0 owner test
switch(config)# rmon alarm 20 1.3.6.1.2.1.2.2.1.14.16777216 2900 delta
rising-threshold-high 15 rising-threshold-low 151 falling-threshold-high 0
falling-threshold-low 0 owner test
switch(config)# show rmon alarms
switch(config)# copy running-config startup-config
```

RMON イベントの設定

RMON アラームとアソシエートするよう RMON イベントを設定できます。複数の RMON アラームで同じイベントを再利用できます。

SNMP ユーザが設定され、SNMP 通知がイネーブルであることを確認します(「SNMP の設定」セクション(27-5 ページ)を参照)。

RMON イベントを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **rmon event** *index* [**description** *string*] [**log**] [**trap**] [**owner** *name*]	RMON イベントを設定します。説明のストリングおよびオーナー名は、任意の英数字ストリングです。
ステップ 3	switch(config)# **show rmon** {**alarms** | **hcalarms**}	(任意)RMON アラームまたは高容量アラームに関する情報を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	(任意)この設定の変更を保存します。

RMON の設定の確認

RMON 設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show rmon alarms	RMON アラームに関する情報を表示します。
show rmon events	RMON イベントに関する情報を表示します。
show rmon hcalarms	RMON 高容量アラームに関する情報を表示します。
show rmon logs	RMON ログに関する情報を表示します。

RMON の設定例

ifInOctets.14 にデルタ上限アラームを作成し、このアラームに通知イベントを関連付ける例を示します。

```
configure terminal
 rmon alarm 20 1.3.6.1.2.1.2.2.1.14 2900 delta rising-threshold 1500 1 falling-threshold 0
owner test
 rmon event 1 trap
```

関連項目

次の関連項目を参照してください。

- SNMP の設定(27-5 ページ)。

デフォルト設定

表 28-1 に、RMON パラメータのデフォルト設定を示します。

表 28-1　デフォルトの RMON パラメータ

パラメータ	デフォルト
Alarms	未設定
events	未設定

CHAPTER 29

FCoE の設定

Fibre Channel over Ethernet（FCoE）は、物理イーサネット接続上でファイバ チャネル トラフィックを転送する方式を提供します。FCoE では、基礎となるイーサネットを全二重にして、ファイバ チャネル トラフィックのロスレス動作を提供する必要があります。

この章では、FCoE 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。

- Fibre Channel over Ethernet（FCoE）について（29-1 ページ）
- FCoE の設定（29-5 ページ）
- LLDP の設定（29-7 ページ）
- FCoE 設定の確認（29-8 ページ）

Fibre Channel over Ethernet（FCoE）について

Cisco Nexus 5000 シリーズ スイッチでは、すべての10ギガビット イーサネット インターフェイスにより FCoE がサポートされています。

FCoE を使用するには、スイッチはサーバに直接接続され、サーバ ポートは統合ネットワーク アダプタでイーサネットを終端する必要があります。

この項では、次のトピックについて取り上げます。

- ライセンス要件（29-1 ページ）
- 統合ネットワーク アダプタ（29-2 ページ）
- DCBX 機能（29-2 ページ）
- DCBX プロトコル（29-3 ページ）
- DCBX 機能のネゴシエーション（29-3 ページ）
- イーサネット フレーム フォーマット（29-4 ページ）

ライセンス要件

Cisco Nexus 5000 シリーズ スイッチでは、FCoE 機能は Storage Protocol Services ライセンスに含まれます。

FCoE 機能を使用する前に、次の点を確認します。

- 正しいライセンス（N5010SS または N5020SS）がインストールされていること。
- コンフィギュレーション モードで **feature fcoe** コマンドを入力し、FCoE がアクティブであること。

統合ネットワーク アダプタ

次の統合ネットワーク アダプタ（CNA）が使用できます。

- ハードウェア アダプタ
  - サーバ内の既存の FC HBA ドライバと LAN NIC ドライバと連動します。
  - ネットワークのサーバ オペレーティング システム表示は変更されません。CNA はオペレーティング システムに SAN インターフェイスおよび LAN インターフェイスを提供します。
- FCoE ソフトウェア スタック
  - 既存の 10 ギガビット イーサネット アダプタで動作します。

FCoE は、多数のオプション機能を提供します。使用可能な機能と設定可能な値は、スイッチとアダプタの間でネゴシエーションが行われます。これを実行するには、アダプタとスイッチは Data Center Bridging Exchange（DCBX）プロトコルを使用して情報を交換します。

設定エラーを抑制し、管理を容易にするため、すべてのアダプタに設定データを配布するようにスイッチを設定することができます。

DCBX 機能

Cisco Nexus 5000 シリーズ スイッチによってサポートされる DCBX 機能については、次で説明します。

- FCoE（29-2 ページ）
- プライオリティ フロー制御（29-2 ページ）
- 論理リンクのアップ/ダウン（29-3 ページ）

FCoE

デフォルトでは、各イーサネット インターフェイスは FCoE 機能をアダプタにアドバタイズすることで、FCoE 機能をイネーブルにしようとします。

FCoE ネゴシエーションが失敗した場合、FCoE をディセーブルにする、またはこのインターフェイスの FCoE を強制的にイネーブルにするようスイッチを設定できます。

プライオリティ フロー制御

プライオリティ フロー制御（PFC）機能により、ポーズ機能を特定のトラフィック クラスに適用できます。PFC は、IEEE 802.1p の CoS 値に基づき、ポーズを適用するかどうかを判断します。スイッチが PFC をイネーブルにすると、特定の CoS 値を持つパケットにポーズ機能を適用するよう接続済みアダプタを設定します。

デフォルトでは、スイッチは PFC 機能をイネーブルにするためのネゴシエーションを行います。ネゴシエーションに成功すると、PFC がイネーブルにされますが、リンクレベル フロー制御は（設定値に関係なく）ディセーブルのままです。

PFC ネゴシエーションに失敗した場合は、PFC をインターフェイスで強制的にイネーブルにするか、IEEE 802.x リンクレベル フロー制御をイネーブルにできます。

PFC がイネーブルでない場合にかぎり、インターフェイスでリンクレベルのフロー制御をイネーブルにできます。リンクレベルのフロー制御に関する詳細については、「リンクレベル フロー制御」セクション（31-3 ページ）を参照してください。

論理リンクのアップ/ダウン

ネイティブ ファイバ チャネル リンクでは、一部の設定アクション（VSAN の変更など）で、インターフェイス ステータスをリセットする必要があります。スイッチは、インターフェイスをディセーブルにしてから直ちにそれを再度イネーブルにすることで、リセットを実行します。

イーサネット リンクが FCoE サービスを提供している場合、物理リンクをリセットしないでください。リセットすると、リンク上のすべてのトラフィックが中断されます。

論理リンク アップ/ダウン機能を使用すると、個別の仮想リンクをリセットできます。スイッチは DCBX メッセージを送信して、仮想ファイバ チャネル インターフェイスだけをリセットするようアダプタに要求します。

（注） アダプタが論理リンク レベル アップ/ダウン機能をサポートしていない場合、アダプタは物理リンクをリセットします。この場合、イーサネット インターフェイスのすべてのトラフィックが中断されます。

DCBX プロトコル

DCBX プロトコルは、リンク層検出プロトコル（LLDP）を拡張したプロトコルです。DCBX エンド ポイントは、要求および確認応答（ACK）メッセージを交換します。柔軟性については、パラメータは TLV フォーマットで符号化されます。

DCBX は、Cisco Nexus 5000 シリーズ スイッチとサーバの統合ネットワーク アダプタの間の物理イーサネット リンク上で動作します。デフォルトでは、DCBX はイーサネット インターフェイスでイネーブルです。イーサネット インターフェイスがアップすると、スイッチはアダプタとの通信を自動的に開始します。

スイッチとアダプタの間の FCoE の通常の動作時には、DCBX プロトコルはリンクエラーを検出します。

また DCBX は、スイッチとアダプタの間で機能についてネゴシエーションを行い、アダプタに設定値を送信する場合にも使用します。

Cisco Nexus 5000 シリーズ スイッチに接続されたアダプタは、スイッチが送信する設定値を受け入れるようプログラミングされます。スイッチは設定値をすべての接続されたアダプタに配信できます。この機能により、設定エラーの可能性を減らし、アダプタの管理を簡素化します。

スイッチは、DCBX を使用してネゴシエーションが行われた各パラメータに対する、手動による設定の上書きを提供しています。アダプタが DCBX をサポートしていない場合、またはアダプタがスイッチの要求する特定の機能をサポートしていない場合、この上書きが有効になります。

DCBX 機能のネゴシエーション

スイッチとアダプタは機能情報および設定値を交換します。Cisco Nexus 5000 シリーズ スイッチは次の機能をサポートします。

- FCoE

  アダプタが FCoE 機能をサポートする場合、スイッチは FCoE パケットで使用する IEEE 802.1p CoS 値を送信します。

- PFC

  アダプタが PFC をサポートする場合、スイッチは PFC でイネーブルにする IEEE 802.1p CoS 値を送信します。
- イーサネット論理リンク アップおよびダウン信号
- FCoE 論理リンク アップおよびダウン信号

次のルールによって、ネゴシエーションの後に機能がイネーブルになるかどうか決定されます。

- 機能と設定値がスイッチとアダプタの間で一致する場合、その機能はイネーブルになります。
- 機能は一致するが、設定値が一致しない場合:
  - スイッチの設定値を受け入れるようアダプタが設定されている場合、スイッチの値を使用して機能がイネーブルになります。
  - スイッチの設定値を受け入れるようアダプタが設定されていない場合、機能はディセーブルのままです。
- アダプタが DCBX 機能をサポートしていない場合、機能はディセーブルのままです。
- アダプタが DCBX を実装していない場合、すべての機能はディセーブルのままです。

（注）　Cisco Nexus 5000 シリーズ スイッチは、アダプタとのネゴシエーションの結果を手動で上書きする CLI コマンドを提供します。インターフェイス単位で、機能を強制的にイネーブルまたはディセーブルにできます。詳細は、「FCoE の設定」セクション（29-5 ページ）を参照してください。

イーサネット フレーム フォーマット

スイッチによってアダプタに送信されるイーサネット フレームには、IEEE 802.1Q タグが含まれます。このタグには、PFC が使用するサービス クラス（CoS）のフィールドが含まれます。IEEE 802.1Q タグには、Cisco Nexus 5000 シリーズ スイッチが現在使用していない VLAN（仮想 LAN）フィールドも含まれます。

スイッチは、アダプタからのタグ付きフレームまたはタグなしフレームを必ず受信します。

FCoE 機能がスイッチとアダプタの間でイネーブルである場合、次のようになります。

- アダプタに送信されるすべてのイーサネット フレームには、IEEE 802.1Q タグが含まれます。
  - VLAN ID フィールドは常に 0 に設定されます。
  - CoS フィールドは、関連付けられたシステム クラスの CoS 値に設定されます。詳細は、「システム クラス」セクション（31-2 ページ）を参照してください。
- スイッチは、アダプタからのタグ付きフレームまたはタグなしフレームを受信します。

FCoE 機能がスイッチとアダプタの間でディセーブルである場合、次のようになります。

- アダプタに送信されるイーサネット フレームには、IEEE 802.1Q タグが含まれません。
- スイッチは、アダプタからのタグ付きフレームまたはタグなしフレームを受信します。

FCoE の設定

ここでは、次の内容について説明します。

- FCoE のイネーブル化（29-5 ページ）
- イーサネット インターフェイスでの FCoE のイネーブル化（29-5 ページ）
- プライオリティ フロー制御の設定（29-6 ページ）
- IEEE 802.3x リンクレベル フロー制御の設定（29-7 ページ）

FCoE のイネーブル化

FC_FEATURES_PKG がインストールされたら、FCoE 機能をイネーブルにする必要があります。FCoE をイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# feature fcoe`	FCoE 機能をイネーブルにします。

次の例は、スイッチで FCoE をイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# feature fcoe
FC license checked out successfully
```

イーサネット インターフェイスでの FCoE のイネーブル化

デフォルトでは、10 ギガビット イーサネット インターフェイスはアダプタと FCoE 機能についてネゴシエーションを行います。FCoE 機能を強制的にイネーブルにすることで、ネゴシエーション結果を上書きできます。FCoE 機能を強制的にイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface type slot/port`	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# fcoe mode {auto | on}`	FCoE パラメータを **auto** に設定すると、インターフェイスは接続されたアダプタと設定についてネゴシエーションを行います。アダプタが FCoE をサポートしていない場合、FCoE はインターフェイスでイネーブルになりません。 モードが **on** に設定されている場合、ネゴシエーション結果は無視され、FCoE はインターフェイスで enabled に設定されます。

次に、イーサネット インターフェイスの FCoE を強制的にイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# fcoe mode on
```

FCoE 機能を強制的にディセーブルにする手順は、次のとおりです。

コマンド	目的
switch(config-if)# **no fcoe mode** [**auto** | **on**]	このインターフェイスの FCoE 機能をディセーブルにします。

次に、イーサネット インターフェイスの FCoE をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# no fcoe mode auto
```

fcoe コマンドは、物理イーサネット インターフェイスにだけ適用できます。

プライオリティ フロー制御の設定

デフォルトでは、イーサネット インターフェイスはアダプタと PFC 機能についてネゴシエーションを行います。PFC 機能を強制的にイネーブルにすることで、ネゴシエーション結果を上書きできます。PFC 機能を強制的にイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** *type slot/port*	変更するインターフェイスを指定します。
ステップ 3	switch(config-if)# **priority-flow-control mode** {**auto** | **on** }	選択したインターフェイスの PFC モードを設定します。 PFC 機能についてネゴシエーションを行うには、**auto** を指定します。 PFC を強制的にイネーブルにするには、**on** を指定します。

次に、インターフェイスで PFC を強制的にイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# priority-flow-control mode on
```

このインターフェイスの PFC 機能をディセーブルにする手順は、次のとおりです。

コマンド	目的
switch(config-if)# **no priority-flow-control mode** [**auto** | **on**]	このインターフェイスの PFC 機能をディセーブルにします。

IEEE 802.3x リンクレベル フロー制御の設定

デフォルトでは、イーサネット インターフェイス上のリンクレベル フロー制御機能はディセーブルです。PFC がインターフェイスでディセーブルの場合、リンクレベル フロー制御機能だけをイネーブルにします。

リンクレベル フロー制御を設定するには、「IEEE 802.3x リンクレベル フロー制御の設定」セクション（31-9 ページ）を参照してください。

LLDP の設定

ここでは、LLDP をグローバルに設定する方法と個々のインターフェイスに設定する方法について説明します。この項では、次のトピックについて取り上げます。

- グローバル LLDP コマンドの設定（29-7 ページ）
- インターフェイス LLDP コマンドの設定（29-8 ページ）

グローバル LLDP コマンドの設定

グローバルな LLDP 設定値を設定できます。これらの設定値には、ピアから受信した LLDP 情報を廃棄するまでの時間、任意のインターフェイスで LLDP 初期化を実行するまで待機する時間、および LLDP パケットを送信するレートが含まれます。

LLDP 設定値を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# lldp {holdtime seconds | reinit seconds | timer seconds}`	LLDP オプションを設定します。 **holdtime** オプションを使用して、デバイスが受信した LLDP 情報を廃棄するまでの保存時間を設定します（10 ～ 255 秒、デフォルトは 120 秒）。 **reinit** オプションを使用して、任意のインターフェイスで LLDP 初期化を実行するまでの待機時間を設定します（1 ～ 10 秒、デフォルトは 2 秒）。 **timer** オプションを使用して、LLDP パケットを送信するレートを設定します（5 ～ 254 秒、デフォルトは 30 秒）。

次に、LLDP タイマー オプションを 15 秒に設定する例を示します。

```
switch# configure terminal
switch(config)# lldp timer 15
```

LLDP 設定値をリセットする手順は、次のとおりです。

コマンド	目的
`switch(config)# no lldp {holdtime | reinit | timer}`	LLDP 値をデフォルトにリセットします。

インターフェイス LLDP コマンドの設定

物理イーサネット インターフェイスの LLDP 機能を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** *type slot/port*	変更するインターフェイスを選択します。
ステップ 3	switch(config-if)# [**no**] **lldp** {**receive** | **transmit**}	選択したインターフェイスを受信または送信に設定します。 このコマンドの **no** 形式を使用すると、LLDP の送信または受信をディセーブルにします。

次に、LLDP パケットを送信するようインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# lldp transmit
```

次に、LLDP をディセーブルにするようインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no lldp transmit
switch(config-if)# no lldp receive
```

このコマンドを使用できるのは、物理イーサネット インターフェイスに対してだけです。

FCoE 設定の確認

FCoE の設定情報を確認するには、次のうちいずれかの作業を行います。

コマンド	目的
switch# **show fcoe**	FCoE がスイッチでイネーブルになっているかどうかを表示します。
switch# **show lldp**	LLDP の設定を表示します。

次に、FCoE 機能がイネーブルになっているか確認する例を示します。

```
switch# show fcoe
FCoE/FC feature is desired.
```

次に、LLDP インターフェイス情報を表示する例を示します。

```
switch# show lldp interface ethernet 1/2
tx_enabled: TRUE
rx_enabled: TRUE
dcbx_enabled: TRUE
```

```
Port MAC address:  00:0d:ec:a3:5f:48

Remote Peers Information

No remote peers exist
```

次に、LLDP ネイバー情報を表示する例を示します。

```
switch# show lldp neighbors
```

次に、LLDP タイマー情報を表示する例を示します。

```
switch# show lldp timers
LLDP Timers

holdtime 120 seconds
reinit 2 seconds
msg_tx_interval 30 seconds
```

次に、LLDP カウンタを表示する例を示します。

```
switch# show lldp traffic
```

CHAPTER 30

仮想インターフェイスの設定

ここでは、Cisco Nexus 5000 シリーズ スイッチの仮想インターフェイスの設定について説明します。内容は次のとおりです。

- 仮想インターフェイスについて（30-1 ページ）
- 注意事項および制約事項（30-1 ページ）
- 仮想インターフェイスの設定（30-2 ページ）
- 仮想インターフェイス情報の確認（30-4 ページ）

仮想インターフェイスについて

Cisco Nexus 5000 シリーズ スイッチでは、Fibre Channel over Ethernet（FCoE）がサポートされています。これにより、スイッチとサーバの間の同じ物理イーサネット接続上でファイバ チャネルおよびイーサネット トラフィックを伝送できます。FCoE の詳細については、第 29 章「FCoE の設定」を参照してください。

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

（注） 仮想インターフェイスは、管理状態がダウンに設定された状態で作成されます。仮想インターフェイスを動作状態にするよう管理状態を明示的に設定する必要があります。

注意事項および制約事項

仮想インターフェイスを設定する場合、次の注意事項および制限事項に注意してください。

- 各仮想ファイバ チャネル インターフェイスは、FCoE 対応のイーサネット インターフェイスにバインドされている必要があります。FCoE は、10 ギガビット イーサネット インターフェイスでサポートされます。
- 各仮想ファイバ チャネル インターフェイスは、ただ 1 つの VSAN に関連付けられます。
- 仮想ファイバ チャネル インターフェイスに関連付けられた VSAN は、専用の FCoE 対応の VLAN にマッピングする必要があります。
- プライベート VLAN では、FCoE はサポートされません。

仮想インターフェイスの設定

ここでは、仮想インターフェイス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。

- 仮想ファイバ チャネル インターフェイスの作成（30-2 ページ）
- VLAN への VSAN のマッピング（30-2 ページ）
- 仮想ファイバ チャネル インターフェイスの削除（30-3 ページ）

仮想ファイバ チャネル インターフェイスの作成

仮想ファイバ チャネル インターフェイスをバインドするイーサネット インターフェイスは、次のように設定する必要があります。

- このインターフェイスは、トランク ポートである必要があります（**switchport mode trunk** コマンドを使用）。
- 仮想ファイバ チャネルの VSAN に対応する FCoE VLAN は、許可 VLAN リストに含まれている必要があります。
- FCoE VLAN をトランク ポートのネイティブ VLAN として設定しないでください。
- イーサネット インターフェイスは、PortFast として設定する必要があります（**spanning-tree port type edge trunk** コマンドを使用）。

上記の設定に関する注意事項を遵守することで、T11 Fibre Channel Initialization Protocol（FIP）をベースにした、将来の FCoE リリース に確実にアップグレードできます。

仮想ファイバ チャネル インターフェイスを作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface vfc vfc-id`	仮想ファイバ チャネル インターフェイスがまだ存在していない場合、それを作成し、インターフェイス コンフィギュレーション モードを開始します。 仮想ファイバ チャネル インターフェイス ID の範囲は、1 ～ 8192 です。
ステップ 3	`switch(config-if)# bind interface ethernet slot/port`	仮想ファイバ チャネル インターフェイスを指定された物理イーサネット インターフェイスにバインドします。

VLAN への VSAN のマッピング

VSAN とそれに関連付けられた VLAN とのマッピングを作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# vlan vlan-id`	VLAN コンフィギュレーション モードを開始します。VLAN 番号の範囲は、1 ～ 4096 です。

	コマンド	目的
ステップ 3	switch(config-vlan)# **fcoe** [**vsan** *vsan-id*]	指定された VLAN で FCoE をイネーブルにします。デフォルトでは、この VLAN から同じ番号の VSAN へのマッピングが作成されます。 (任意)この VLAN から指定した VSAN へのマッピングを設定します。
ステップ 4	switch(config-vlan)# **exit**	VLAN コンフィギュレーション モードを終了します。
ステップ 5	switch(config)# **vsan database**	VSAN コンフィギュレーション モードを開始します。
ステップ 6	switch(config-vsan)# **vsan** *vsan-id* **interface vfc** *vfc-id*	VSAN と仮想ファイバ チャネル インターフェイスの関連付けを設定します。 VSAN 番号は、仮想ファイバ チャネル インターフェイスにバインドされた物理イーサネット インターフェイスの上の VLAN にマッピングする必要があります。

次の例では、物理イーサネット アドレスに VLAN を設定し、仮想ファイバ チャネル インターフェイス 4 を作成して、vfc 4 を物理イーサネット インターフェイスにバインドする方法を示します。また、関連付けられた VLAN 200 をイネーブルにし、VLAN 200 を VSAN 2 にマッピングします。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1,200
switch(config)# interface vfc 4
switch(config-if)# bind interface ethernet 1/2
switch(config-if)# exit
switch(config)# vlan 200
switch(config-vlan)# fcoe vsan 2
switch(config-vlan)# exit
switch(config)# vsan database
switch(config-vsan)# vsan 2 interface vfc 4
```

仮想ファイバ チャネル インターフェイスの削除

仮想ファイバ チャネル インターフェイスを削除するには、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **no interface vfc** *vfc-id*	仮想ファイバ チャネル インターフェイスを削除します。

次の例では、仮想ファイバ チャネル インターフェイスを削除します。

```
switch# configure terminal
switch(config)# no interface vfc 4
switch(config-if)# exit
```

仮想インターフェイス情報の確認

仮想インターフェイスに関する設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
switch# **show interface vfc** *vfc-id*	指定されたファイバ チャネル インターフェイスの詳細な設定を表示します。
switch# **show interface brief**	すべてのインターフェイスのステータスが表示されます。

次の例では、仮想ファイバ チャネル インターフェイスに関する情報を表示します。

```
switch# show interface vfc 3
vfc3 is down
Bound interface is Ethernet3/2
    Hardware is GigabitEthernet
    Port WWN is 20:01:00:0d:ec:6d:81:3f
    Admin port mode is F
    snmp link state traps are enabled
    Port vsan is 1
    Beacon is turned unknown
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      0 frames input, 0 bytes
        0 discards, 0 errors
      0 frames output, 0 bytes
        0 discards, 0 errors
```

次の例では、スイッチ上のすべてのインターフェイスのステータスを示します（簡略化のため、一部の出力は削除）。

```
switch# show interface brief

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                          Mode  Speed  Channel
                         Mode                                (Gbps)
--------------------------------------------------------------------------------
fc3/1      1      auto   on      trunking         swl    TE      2    --
fc3/2      1      auto   on      sfpAbsent        --     --           --
...
fc3/8      1      auto   on      sfpAbsent        --     --           --

--------------------------------------------------------------------------------
Interface                Status     IP Address        Speed    MTU   Port
                                                                     チャネル
--------------------------------------------------------------------------------
Ethernet1/1              hwFailure  --                --       1500  --
Ethernet1/2              hwFailure  --                --       1500  --
Ethernet1/3              up         --                10000    1500  --
...
Ethernet1/39             sfpIsAbsen --                --       1500  --
Ethernet1/40             sfpIsAbsen --                --       1500  --
```

```
--------------------------------------------------------------------------------
Interface                Status     IP Address        Speed    MTU
--------------------------------------------------------------------------------
mgmt0                    up         172.16.24.41      100      1500

--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                          Mode  Speed  Channel
                         Mode                                 (Gbps)
--------------------------------------------------------------------------------
vfc 1        1      F      --      down             --     --           --
```

CHAPTER 31

QoS の設定

ここでは、Cisco Nexus 5000 シリーズ スイッチで Quality of Service（QoS）機能を設定する方法について説明します。

この章は、次の項で構成されています。

- QoS の概要（31-1 ページ）
- 設定時の注意事項および制限事項（31-7 ページ）
- PFC および LLC の設定（31-8 ページ）
- システム クラスの設定（31-10 ページ）
- インターフェイスでの QoS の設定（31-14 ページ）

QoS の概要

Cisco Nexus 5000 シリーズ スイッチはトラフィックの優先順位付けおよび出力帯域幅割り当てなどの QoS 機能を提供します。

スイッチ上のデフォルトの QoS 設定により、ファイバ チャネルおよび Fibre Channel Over Ethernet（FCoE）トラフィックのロスレス サービスと、ファイバ チャネルのベストエフォート型サービスを提供します。イーサネット トラフィックのサービス クラス（CoS）を追加するよう QoS を設定できます。Cisco Nexus 5000 シリーズQoS 機能は、Cisco モジュラ QoS コマンドライン インターフェイス（MQC）を使用して設定されます。

この項では、次のトピックについて取り上げます。

- MQC（31-2 ページ）
- システム クラス（31-2 ページ）
- デフォルトのシステム クラス（31-3 ページ）
- リンクレベル フロー制御（31-3 ページ）
- プライオリティ フロー制御（31-4 ページ）
- MTU（31-4 ページ）
- 信頼境界（31-4 ページ）
- 入力ポリシー（31-5 ページ）
- 出力ポリシー（31-5 ページ）

- マルチキャスト トラフィックの QoS（31-6 ページ）
- ファイバ チャネル インターフェイスのポリシー（31-7 ページ）
- CPU 方向のトラフィックの QoS（31-7 ページ）

MQC

Cisco MQC は、QoS を設定するための標準コマンド セットを提供します。

MQC を使用して、追加のトラフィック クラスを定義し、システム全体および個々のイーサネット インターフェイスで QoS ポリシーを設定できます。MQC で QoS ポリシーを設定するには、次の手順を実行します。

1. **class-map** コマンドを使用して、トラフィック クラスを定義します。

   クラス マップは、IEEE 802.1p CoS 値などの一致基準に基づいて、着信または発信パケットを分類します。ユニキャスト パケットおよびマルチキャスト パケットが分類されます。

2. **policy-map** コマンドを使用して、各トラフィック クラスにポリシーまたはアクションを関連付けます。

   ポリシー マップは、帯域幅の制限やパケットのドロップなど、アソシエートされたトラフィック クラスで実行するアクション セットを定義します。

3. **service-policy** コマンドを使用して、MQC ターゲットにポリシーを適用します。

   MQC ターゲットは、パケットのフローを表すエンティティ（イーサネット インターフェイスなど）です。サービス ポリシーはポリシー マップを MQC ターゲットにアソシエートし、着信または発信パケットでポリシーを適用するかどうか指定します。これにより、ポリシングおよび帯域割り当てなど、インターフェイス固有の QoS ポリシーの設定をイネーブルにします。

システム クラス

システム クラスは新しいタイプの MQC ターゲットです。サービス ポリシーは、ポリシー マップをシステム クラスに関連付けることができます。これにより、スイッチ全体で QoS ポリシーのアプリケーションをイネーブルにします。

特定のトラフィック クラスのパケットがネットワーク上で転送された場合、一貫した処理を受けられるようにするため、システム クラスのパラメータをスイッチとネットワーク全体で一貫して設定する必要があります。

QoS の一貫性を確保するため（および設定しやすくするため）に、スイッチはDCBX プロトコルを使用して接続されたネットワーク アダプタのすべてにシステム クラス パラメータ値を配布します。スイッチとアダプタ間の通信についての詳細は、「DCBX プロトコル」セクション（29-3 ページ）を参照してください。

サービス ポリシーがインターフェイス レベルで設定されている場合、インターフェイス レベルのポリシーは常にシステム クラス設定またはデフォルト値よりも優先されます。

システム クラスには、次の QoS パラメータを指定できます。

- ドロップ

  No drop は、システム クラスのロスレス サービスを指定します。drop は、このシステム クラスのキューが満杯である場合にテール ドロップを使用することを指定します。

- MTU

  システム クラス MTU は、システム クラスに分類されたパケットの最大パケット サイズを定義します。システム クラスごとにデフォルトの MTU があります。システム クラス MTU は設定可能です。

- Match CoS 値

  match CoS 値は、このシステム クラスに関連付ける IEEE 802.1p CoS 値を指定します。

- 帯域幅とプライオリティ

  このシステム クラスの帯域幅およびプライオリティ設定値を設定します。システム クラス値は、すべてのインターフェイスでデフォルト値として使用されます。

デフォルトのシステム クラス

Cisco Nexus 5000 シリーズ スイッチは次のデフォルトのシステム クラスを提供します。

- FCoE システム クラス

  すべてのファイバ チャネルおよび FCoE 制御トラフィックおよびデータ トラフィックは、自動的に FCoE システム クラスに分類されます。これにより、no-drop サービスを提供します。

  このクラスは、システムの起動時に自動的に作成されます（クラス名は CLI で **class-fcoe** です）。このクラスは削除できません。このクラスに関連付ける IEEE 802.1p CoS 値の変更だけ可能です。

  スイッチは、次のようにパケットを FCoE システム クラスに分類します。

  - FCoE トラフィックは EtherType に基づいて分類されます。
  - ネイティブ ファイバ チャネル トラフィックは、物理インターフェイス タイプに基づいて分類されます。

- ドロップ システム クラス

  デフォルトでは、すべてのユニキャストおよびマルチキャスト イーサネット トラフィックは、デフォルトのドロップ システム クラスに分類されます。

  システムの起動時にこのクラスは自動的に作成されます（クラス名は CLI で **class-default** です）。このクラスは削除できません。このデフォルト クラスに関連付けられた CoS 値も変更できません。

システムの内部用に 2 つのシステム クラスが予約されています。

リンクレベル フロー制御

IEEE 802.3x リンクレベル フロー制御機能により、輻輳レシーバは遠端と通信して、短時間の間データの転送を停止できます。リンクレベル フロー制御機能は、リンク上のすべてのトラフィックに適用されます。

送受信方向は個別に設定できます。デフォルトでは、リンクレベル フロー制御は両方向でディセーブルです。

Cisco Nexus 5000 シリーズ スイッチでは、イーサネット インターフェイスはリンクレベル フロー制御機能を自動検出しません。イーサネット インターフェイスでこの機能を明示的に設定する必要があります。

各イーサネット インターフェイスで、スイッチはプライオリティ フロー制御またはリンクレベル フロー制御のいずれか（両方は不可）をイネーブルにできます。

プライオリティ フロー制御

PFC 機能により、ポーズ機能をリンク上のすべてのトラフィックではなく、リンク上の特定のトラフィック クラスに適用できます。PFC は、IEEE 802.1p CoS 値に基づいて、ポーズ機能を適用します。スイッチが PFC をイネーブルにすると、ポーズ機能を適用する CoS 値をアダプタに伝えます。

イーサネット インターフェイスは PFC を使用して、ロスレス サービスを no-drop システム クラスに提供します。PFC はクラス単位でポーズ フレームを実装し、IEEE 802.1p CoS 値を使用してロスレス サービスを必要とするクラスを特定します。

スイッチでは、各システム クラスにはアソシエートされた IEEE 802.1p CoS 値があります（デフォルトで割り当てられるか、システム クラスで設定されます）。PFC がイネーブルである場合、スイッチは no-drop CoS 値をアダプタに送信し、PFC をこれらの CoS 値に適用します。

FCoE システム クラスのデフォルトの CoS 値は 3 です。この値は設定可能です。デフォルト ドロップ システム クラスのデフォルトの CoS 値は 0 です。この値は設定可能です。

PFC がインターフェイスでイネーブルでない場合、IEEE 802.3X リンクレベル ポーズをイネーブルにできます。デフォルトでは、リンクレベル ポーズはディセーブルです。

MTU

Cisco Nexus 5000 シリーズ スイッチはレイヤ 2 スイッチで、パケット フラグメンテーションをサポートしません。入力インターフェイスと出力インターフェイスの間で MTU の設定不一致が発生すると、パケットが切り捨てられることがあります。

MTU を設定する場合は、次の注意事項に従ってください。

- MTU はシステム クラス単位で指定されます。インターフェイスでは MTU を設定できません。
- ファイバ チャネルおよび FCoE ペイロード MTU は、スイッチで 2112 バイトです。その結果、ファイバ チャネル インターフェイスの rxbufsize は 2112 バイトに固定されます。Cisco Nexus 5000 シリーズ スイッチが 2112 バイトではない rxbufsize をピアから受信すると、ELP ネゴシエーションに失敗し、リンクはアップ状態になりません。
- **system jumbomtu** コマンドを実行すると、システム内の MTU の上限が定義されます。システム ジャンボ MTU のデフォルト値は 9216 バイトです。最小 MTU は 2240 バイトで、最大 MTU は 9216 バイトです。
- システム クラス MTU はクラス内のすべてのパケットの MTU を設定します。システム クラス MTU を、グローバル ジャンボ MTU よりも大きく設定できません。
- FCoE システム クラス（ファイバ チャネルおよび FCoE トラフィックの場合）のデフォルト MTU は 2240 バイトです。この値は変更できません。
- デフォルトのドロップ システム クラスのデフォルト MTU は 1500 バイトです。この値は設定できます。
- スイッチは MTU 設定を、DCBXP をサポートするネットワーク アダプタに送信します。

信頼境界

信頼境界は、次のように着信インターフェイスによって実行されます。

- すべてのファイバ チャネルおよび仮想ファイバ チャネル インターフェイスは、FCoE システム クラスに自動的に分類されます。

- デフォルトでは、すべてのイーサネット インターフェイスは信頼できるインターフェイスです。802.1p CoS 値でタグ付けされたパケットは、パケット内の値を使用して、システム クラスに分類されます。
- 802.1p CoS 値でタグ付けされていないパケットは、デフォルトのドロップ システム クラスに分類されます。タグなしパケットがトランク上で送信される場合、このパケットにはデフォルトのタグなし CoS 値 0 がタグ付けされます。
- イーサネット インターフェイスまたはポート チャネルのデフォルトのタグなし Cos 値は上書きできます。

システムがタグなし CoS 値を適用しても、QoS は、CoS 値がタグ付けされたシステムに入るパケットと同様に機能します。

入力ポリシー

入力ポリシー マップをイーサネット インターフェイスに関連付けて、指定されたトラフィック クラスの帯域幅を確保したり、プライオリティ キューを指定したりできます。

アダプタの入力ポリシーは、指定された Cos 値と一致するすべての発信トラフィックに適用されます。

インターフェイスの入力ポリシーを設定すると、スイッチはアダプタに設定データを送信します。アダプタが DCBX プロトコル（または入力ポリシー TLV）をサポートしていない場合、入力ポリシーの設定は無視されます。

出力ポリシー

出力ポリシー マップをイーサネット インターフェイスにアソシエートし、指定されたトラフィック クラスの帯域幅を保証したり、出力キューを設定したりできます。

帯域割り当ての制限は、インターフェイス上のすべてのトラフィック（FCoE トラフィックを含む）に適用されます。

イーサネット インターフェイスごとに最大 8 つのキュー（システム クラスごとに 1 つ）をサポートします。キューには次のデフォルト設定があります。

- キュー ゼロは完全プライオリティ キューとして設定されます。CPU 宛ての制御トラフィックはこのキューを使用します。
- FCoE トラフィック（FCoE システム クラスにマッピングされるトラフィック）にキューが割り当てられます。このキューは、帯域幅の 50% で WRR スケジューリングを使用します。
- 標準イーサネット トラフィック（デフォルトのドロップ システム クラス内）にキューが割り当てられます。このキューは、帯域幅の 50% で WRR スケジューリングを使用します。

システム クラスを追加すると、キューがクラスに割り当てられます。影響を受けたすべてのインターフェイスで帯域割り当てを再設定する必要があります。帯域幅は、自動的にユーザ定義のシステム クラス専用にはなりません。

追加の完全プライオリティ キューを設定できます。このキューは、キュー ゼロ（データ トラフィックではなく制御トラフィックを伝送）以外の他のすべてのキューより先に処理されます。

マルチキャスト トラフィックの QoS

システムは、インターフェイスごとに 6 つのマルチキャスト キューを提供し、各システム クラスに 1 つのキューを割り当てます。デフォルトでは、すべてのマルチキャスト イーサネット トラフィックは、デフォルトのドロップ システム クラスに分類されます。このトラフィックは、1 つのマルチキャスト キューで処理されます。

最適化マルチキャスト機能により、未使用のマルチキャスト キューを使用して、マルチキャスト フレームのスループットを向上させることができます。最適化マルチキャストがデフォルトのドロップ システム クラスでイネーブルにされると、システムは 6 つのキューすべてを使用してマルチキャスト トラフィックを処理します（6 つのキューには同等のプライオリティが与えられます）。

新しいシステム クラスを定義すると、専用のマルチキャスト キューがこのクラスに割り当てられます。このキューは、最適化マルチキャストで利用できるキューのセットから削除されます。

最適化されたマルチキャスト機能では、マルチキャスト フレームのスループットが改善され、長さが 256 バイト未満のマルチキャスト フレームのパフォーマンスが向上します。

（注）　最適化マルチキャストは、Cisco Nexus 5020 スイッチの BF 以降のバージョンでサポートされます。モデル バージョンを確認するには、**show module 1** コマンドを入力します。モデル番号の末尾 2 文字がモデル バージョンです。最適化マルチキャストは、Cisco Nexus 5010 スイッチの全バージョンでサポートされます。

システムは、ブロードキャスト トラフィックまたはマルチキャスト トラフィックを照合するための定義済みのクラス マップを 2 つ備えています。これらのクラス マップは、ユニキャスト トラフィックとマルチキャスト トラフィックに別々のポリシー マップを作成する場合に便利です。定義済みのクラス マップは、次のとおりです。

- class-all-flood

  class-all-flood クラス マップは、すべてのブロードキャスト トラフィック、マルチキャスト トラフィック、および未知のユニキャスト トラフィック（すべての Cos 値）を照合します。class-all-flood クラス マップでポリシー マップを設定した場合、システムはこのトラフィックに利用できるすべてのマルチキャスト キューを自動的に使用します。

- class-ip-multicast

  class-ip-multicast クラス マップは、すべての IP マルチキャスト トラフィックを照合します。このクラス マップに設定されたポリシー オプションが、すべてのイーサネット CoS 値でトラフィックに適用されます。たとえば、このクラスの最適化マルチキャストをイネーブルにすると、IP マルチキャスト トラフィックはすべての CoS 値で最適化されます。

  このクラスを no-drop クラスとして設定すると、プライオリティ フロー制御機能がすべてのイーサネット CoS 値に適用されます。この設定では、ポーズがユニキャスト トラフィックおよびマルチキャスト トラフィックに適用されます。

（注）　これらの定義済みクラスのうち、1 つだけをシステム QoS ポリシーに設定できます。

ファイバ チャネル インターフェイスのポリシー

出力キューは、ネイティブ ファイバ チャネル インターフェイスに設定できません。次のように 2 つのキューが使用できます。

- ハイプライオリティ制御トラフィックを処理する完全プライオリティ キュー
- すべてのデータ トラフィックとロー プライオリティ制御トラフィックを処理するキュー

CPU 方向のトラフィックの QoS

スイッチは、CPU でパケットがフラッディングしないように、CPU 方向のトラフィックに自動的に QoS ポリシーを適用します。確実に配信するために、BPDU フレームなどの制御トラフィックにはより高いプライオリティが与えられます。

設定時の注意事項および制限事項

スイッチ リソース（バッファ、仮想出力キュー、および出力キューなど）は、デフォルト クラスおよびユーザ設定のシステム クラスに基づいて分割されます。スイッチ ソフトウェアは自動的にリソース割り当てを調整して、設定済みシステム クラスに対応します。

最適なスイッチ パフォーマンスを維持するには、システム クラスおよびポリシーの設定時に次の注意事項に従ってください。

- 4 つ未満のイーサネット クラスを定義する場合、最大 2 つのクラスを no-drop クラスとして設定できます。5 つ以上のイーサネット クラスを定義する場合、これらのクラスのうち 1 つだけを no-drop クラスとして設定できます。デフォルトの drop クラスはイーサネット クラスとしてカウントされます。
- イーサネット インターフェイスでプライオリティ フロー制御がイネーブルの場合、ポーズはドロップ システム クラスを持つトラフィックに適用されません。PFC はポーズをドロップ クラスに適用しません。PFC が設定されたインターフェイスでは、リンクレベル ポーズ機能はイネーブルになりません。
- イーサネット インターフェイス上のすべての FCoE トラフィックは 1 つの no-drop システム クラスにマッピングされます。別の値を設定できても、デフォルトではこのクラスに CoS 値 3 が関連付けられています。FCoE と同じ CoS 値を使用するように標準のイーサネット トラフィックを設定すると、スイッチは標準のイーサネット トラフィックにプライオリティ フロー制御を適用しません。このトラフィックは、デフォルトのドロップ システム クラスにマッピングされます。
- CoS 値 0 は、デフォルトのドロップ システム クラス用に予約されています。この値は、他のクラスにマッピングできません。

イーサネット ポート チャネルを設定する場合は、次の注意事項に注意してください。

- ポート チャネル インターフェイスに設定されたサービス ポリシーは、ポート チャネル内のすべてのメンバに適用されます。個々のメンバ インターフェイスに設定されたサービス ポリシーは無視されます。
- プライオリティ フロー制御は、ポート チャネルの個々のメンバ インターフェイスに設定されます。ポート チャネルが動作可能になるには、ポート チャネル内のすべてのメンバで PFC 設定が一貫している必要があります。

PFC および LLC の設定

Cisco Nexus 5000 シリーズ スイッチは、イーサネット インターフェイスで PFC および LLC をサポートします。イーサネット インターフェイスは、FCoE モードまたは標準イーサネット モードの 2 つの異なるモードで動作します。

インターフェイスが FCoE モードで動作している場合、イーサネット リンクは統合ネットワーク アダプタ（CNA）を使用してサーバ ポートに接続されます。インターフェイスが FCoE モードで動作している場合の PFC および LLC の設定については、第 29 章「FCoE の設定」を参照してください。

インターフェイスが標準イーサネット モードで動作している場合、イーサネット リンクは標準イーサネット ネットワーク アダプタ（NIC）を使用してサーバ ポートに接続されます。PFC または入力ポリシングをインターフェイスでサポートするには、ネットワーク アダプタで DCBX プロトコルをサポートする必要があります。

（注）　イーサネット トラフィックで動作するように PFC の no-drop イーサネット システム クラスを設定する必要があります（PFC は、このクラスに設定された CoS 値と一致するトラフィックに適用されます）。

標準イーサネットの PFC と LLC の設定の具体的な内容は、次のとおりです。

- プライオリティ フロー制御の設定（31-8 ページ）
- IEEE 802.3x リンクレベル フロー制御の設定（31-9 ページ）

プライオリティ フロー制御の設定

デフォルトでは、イーサネット インターフェイスは、DCBX プロトコルを使用してネットワーク アダプタと PFC 機能についてネゴシエーションします。PFC がイネーブルの場合、PFC は、no-drop イーサネット クラスに設定された CoS 値と一致するトラフィックに適用されます。

PFC 機能を強制的にイネーブルにすることで、ネゴシエーション結果を上書きできます。PFC 機能を強制的にイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface type slot/port`	変更するインターフェイスを指定します。
ステップ 3	`switch(config-if)# priority-flow-control mode {auto|on}`	選択したインターフェイスの PFC モードを設定します。 PFC を強制的にイネーブルにするには、**on** を指定します。 PFC 機能についてネゴシエーションを行うには、**auto** を指定します。

（注）　プライオリティ フロー制御は、ポート チャネルの個々のメンバ インターフェイスに設定されます。ポート チャネルが動作可能になるには、ポート チャネル内のすべてのメンバで PFC 設定が一貫している必要があります。

次に、インターフェイスで PFC を強制的にイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# priority-flow-control mode on
```

インターフェイスで PFC 機能をディセーブルにする手順は、次のとおりです。

コマンド	目的
`switch(config-if)# no priority-flow-control mode`	選択したインターフェイスの PFC 設定をディセーブルにします。

IEEE 802.3x リンクレベル フロー制御の設定

デフォルトでは、イーサネット インターフェイス上のリンクレベル フロー制御機能はディセーブルです。送受信方向でリンクレベル フロー制御機能をイネーブルにできます。リンクレベル フロー制御機能をイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface type slot/port`	変更するインターフェイスを指定します。
ステップ 3	`switch(config-if)# flowcontrol [receive {on|off}] [transmit {on|off}]`	選択したインターフェイスの IEEE 802.3x リンクレベル フロー制御をイネーブルにします。**receive** および **transmit** の **on** または **off** を設定します。

次に、インターフェイスでリンクレベル フロー制御フレームをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# flowcontrol receive on transmit on
```

リンクレベル フロー制御をディセーブルにする手順は、次のとおりです。

コマンド	目的
`switch(config-if)# no flowcontrol [receive {on|off}] [transmit {on|off}]`	選択したインターフェイスの IEEE 802.3x リンクレベル フロー制御をディセーブルにします。

システム クラスの設定

ここでは、スイッチでシステム クラスを設定する方法について説明します。システム クラスを設定する手順は、次のとおりです。

- クラス マップの設定（31-10 ページ）
- ポリシー マップの設定（31-11 ページ）
- システム サービス ポリシーの作成（31-12 ページ）
- システム クラスの例（31-13 ページ）
- ジャンボ MTU のイネーブル化（31-13 ページ）
- ジャンボ MTU の確認（31-13 ページ）

クラス マップの設定

class-map コマンドを実行すると、トラフィックのクラスを表す名前付きオブジェクトが作成されます。クラス マップでは、パケットを分類する一致基準を指定します。システム クラスの場合、サポートされる一致基準は **match cos** だけです。

システム クラスに no-drop 機能が設定されている場合、**match cos** コマンドは追加目的で機能します。スイッチは CoS 値をアダプタに送信するので、アダプタはこの CoS 値の PFC ポーズを適用します。

FCoE システム クラスのデフォルトの CoS 値は 3 です。**match cos** 設定を FCoE システム クラスに追加して、異なる CoS 値を設定できます。PFC ポーズは新しい値と一致するトラフィックに適用されます。

システム クラスのクラス マップを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# class-map name`	トラフィックのクラスを表す名前付きオブジェクトを作成します。クラス マップ名は、最大 40 文字の英字、ハイフン、またはアンダースコアを使用でき、大文字と小文字が区別されます。
ステップ 3	`switch(config-cmap)# match cos cos-value`	パケットをこのクラスに分類する場合に照合する CoS 値を指定します。CoS 値は、1 ～ 7 の範囲で設定できます。 **（注）** CoS 値 0 は、デフォルトのドロップ システム クラス（**class-default**）用に予約されています。

ポリシー マップの設定

policy-map コマンドを使用して、トラフィック クラスのセットに適用されるポリシーのセットを表す名前付きオブジェクトを作成します。

スイッチは、デフォルトのシステム クラス（ロスレス サービス用の no-drop クラスとベストエフォート型サービス用の drop クラス）を提供します。イーサネット トラフィックには最大 4 つの追加システム クラスを定義できます。

ポリシー マップを作成して、任意のユーザ定義のクラスにポリシーを指定する必要があります。このポリシー マップで、各クラスに QoS パラメータを設定できます。同じポリシー マップを使用して、デフォルト クラスの設定を変更できます。

（注） ポリシー マップを作成する前に、新しいシステム クラスごとにクラス マップを定義します。

ポリシー マップを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configure terminal`**	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`policy-map`** *`name`*	トラフィック クラスのセットに適用されるポリシーのセットを表す名前付きオブジェクトを作成します。ポリシー マップ名は、最大 40 文字の英字、ハイフン、または下線文字を使用でき、大文字と小文字が区別されます。
ステップ 3	`switch(config-pmap)#` **`class`** `class-name`	クラス マップをポリシー マップにアソシエートし、指定されたシステム クラスのコンフィギュレーション モードを開始します。
ステップ 4	`switch(config-pmap-c)#` **`pause no-drop`**	（任意）no-drop クラスを設定します。このサブコマンドを指定しない場合、デフォルトのポリシーはドロップです。 **（注）** ドロップ ポリシーの動作はテール ドロップと似ています。キューが割り当てサイズまで増加すると、着信パケットはドロップされます。
ステップ 5	`switch(config-pmap-c)#` **`mtu`** *`value`*	（任意）MTU 値をバイト単位で指定します。
ステップ 6	`switch(config-pmap-c)` **`bandwidth percent`** *`percentage`*	（任意）このクラスに割り当てられたインターフェイスの保証帯域幅の割合を指定します。
ステップ 7	`switch(config-pmap-c)` **`priority`**	（任意）このクラスの該当するトラフィックが絶対優先キューにマッピングされるよう指定します。
ステップ 8	`switch(config-pmap-c)` **`multicast-optimize`**	（任意）マルチキャスト最適化を有効化します。このクラスのマルチキャスト トラフィックは、使用可能なすべてのマルチキャスト キューによってサポートされます。 **（注）** ポリシー マップのクラスのうち、1 つだけをマルチキャストの最適化用に設定できます。

（注）　スイッチは、接続されたネットワーク アダプタにすべてのポリシー マップ設定値を配布します。

（注）　ポリシーマップは、インターフェイス サービス ポリシーにも設定できます。ただし、このポリシー マップでは異なるパラメータがサポートされます。「インターフェイスでの QoS の設定」セクション（31-14 ページ）を参照してください。

次に、デフォルトのイーサネット クラスに対して最適化マルチキャストをイネーブルにする方法を示します。

```
switch(config)# policy-map s1
switch(config-pmap)# class class-default
switch(config-pmap-c)# multicast-optimize
```

次に、no-drop イーサネット クラスでポリシー マップを作成する方法を示します。

```
switch(config)# class-map ethCoS4
switch(config-cmap)# match cos 4
switch(config-cmap)# exit
switch(config)# policy-map ethNoDrop
switch(config-pmap)# class ethCoS4
switch(config-pmap-c)# pause no-drop
```

システム サービス ポリシーの作成

service-policy コマンドを使用して、システム クラス ポリシー マップをシステムのサービス ポリシーとして関連付けます。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# system qos`	システム クラス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-sys-qos)# service-policy` *name*	ポリシー マップをシステムのサービス ポリシーとして使用するよう指定します。

次に、no-drop イーサネット ポリシー マップをシステム クラスとして設定する例を示します。

```
switch(config)# class-map ethCoS4
switch(config-cmap)# match cos 4
switch(config-cmap)# exit
switch(config)# policy-map ethNoDrop
switch(config-pmap)# class ethCoS4
switch(config-pmap-c)# pause no-drop
switch(config)# system qos
switch(config-system)# service-policy ethNoDrop
```

システム クラスの例

次の例では、新しいイーサネット no-drop システム クラスが作成され、デフォルトのシステム クラスの CoS 値はデフォルト値から変更されます。

```
switch(config)# class-map trading-data-no-drop
switch(config-cmap)# match cos 5
switch(config)# class-map class-fcoe
switch(config-cmap)# match cos 2
switch(config)# policy-map system-policy
switch(config-pmap)# class trading-data-no-drop
switch(config-pmap-c)# pause no-drop
switch(config-pmap-c)# mtu 2000
switch(config)# system qos
switch(config-system)# service-policy system-policy
```

この例では、最初の **class-map** コマンドを実行して、新しいイーサネット システム クラスを定義します。802.1p CoS 値 5 を持つシステム全体からのパケットは、この新しいシステム クラスに分類されます。

2 番めの **class-map** コマンドを実行して、デフォルトの no-drop システム クラスの match 値を変更します。

policy-map コマンドを実行すると、各トラフィック クラスに QoS ポリシーを定義します。新しいイーサネット クラスは、MTU が 2000 バイトの no-drop クラスとして設定されます。**pause no-drop** コマンドにより、PFC は、IEEE 802.1p プライオリティ値 5 を持つパケットのポーズ機能を適用します。

service-policy コマンドを実行すると、指定されたポリシーがシステム クラスとして設定されます。

ジャンボ MTU のイネーブル化

スイッチ全体のジャンボ MTU をイネーブルにするには、MTU を、デフォルトのイーサネット システム クラス（class-default）のポリシー マップの最大サイズ（9216 バイト）に設定します。

次の例では、デフォルトのイーサネット システム クラスはジャンボ MTU をサポートするよう設定されます。

```
switch(config)# policy-map jumbo
switch(config-pmap)# class class-default
switch(config-pmap-c)# mtu 9216
switch(config)# system qos
switch(config-system)# service-policy jumbo
```

（注）　**system jumbomtu** コマンドは、スイッチの最大 MTU サイズを定義します。ただし、ジャンボ MTU は **mtu** が設定されたシステム クラスに対してだけ、サポートされます。

ジャンボ MTU の確認

ジャンボ MTU がイネーブルであるか確認するには、ジャンボ MTU のあるトラフィックを伝送するイーサネット インターフェイスの **show interface ethernet** *slot/port* コマンドを入力します。

次に、Ethernet 2/1 のジャンボ MTU 情報の要約を表示する例を示します（出力の関連部分を太字で示します）。

```
switch# show interface ethernet 2/1
Ethernet2/1 is up
...
    Rx
    1547805598 Input Packets 1547805596 Unicast Packets 0 Multicast Packets
    0 Broadcast Packets 1301767362 Jumbo Packets 33690 Storm Suppression Packets
    7181776513802 バイト
    Tx
    1186564478 Output Packets 7060 Multicast Packets
    0 Broadcast Packets 997813205 Jumbo Packets
    4813632103603 バイト
...
```

次に、Ethernet 2/1 の詳細なジャンボ MTU 情報を表示する例を示します（出力の関連部分を太字で示します）。

```
switch# show interface ethernet 2/1 counters detailed
Rx Packets: 1547805598
Rx Unicast Packets: 1547805596
Rx Jumbo Packets: 1301767362
Rx Bytes: 7181776513802
Rx Storm Suppression: 33690
Rx Packets from 0 to 64 bytes: 169219
Rx Packets from 65 to 127 bytes: 10657133
Rx Packets from 128 to 255 bytes: 21644488
Rx Packets from 256 to 511 bytes: 43290596
Rx Packets from 512 to 1023 bytes: 86583071
Rx Packets from 1024 to 1518 bytes: 83693729
Rx Trunk Packets: 1547805596
Tx Packets: 1186564481
Tx Unicast Packets: 1005445334
Tx Multicast Packets: 7063
Tx Jumbo Packets: 997813205
Tx Bytes: 4813632103819
Tx Packets from 0 to 64 bytes: 137912
Tx Packets from 65 to 127 bytes: 8288443
Tx Packets from 128 to 255 bytes: 16596457
Tx Packets from 256 to 511 bytes: 33177999
Tx Packets from 512 to 1023 bytes: 66363944
Tx Packets from 1024 to 1518 bytes: 64186521
Tx Trunk Packets: 1005451729
```

インターフェイスでの QoS の設定

ここでは、イーサネット インターフェイスおよびポート チャネル インターフェイスで設定できる QoS パラメータについて説明します。

- タグなし CoS の設定（31-15 ページ）
- 入力ポリシーの設定（31-15 ページ）
- 出力ポリシーの設定（31-16 ページ）

タグなし CoS の設定

802.1p CoS 値でタグ付けされていない着信パケットは、デフォルトのタグなし CoS 値(0)に割り当てられます(これはデフォルトのイーサネット ドロップ システム クラスにマッピングされます)。イーサネット インターフェイスまたはポート チャネルのデフォルトのタグなし Cos 値は上書きできます。

タグなし CoS 値を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** {**ethernet** *slot/port*|**port-channel** *channel-number* }	指定されたインターフェイスまたはポート チャネルのコンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **untagged cos** *cos-value*	タグなし CoS 値を設定します。

入力ポリシーの設定

入力ポリシーは、イーサネット インターフェイスで着信トラフィックに適用されるサービス ポリシーです。アダプタの入力ポリシーは、指定されたクラスと一致するすべての発信トラフィックに適用されます。インターフェイスまたはポート チャネルの入力ポリシーを設定すると、スイッチはアダプタに設定データを送信します。

入力ポリシーを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **class-map** *class-name*	入力ポリシーのクラスを作成します。
ステップ 3	switch(config)# **policy-map** *policy1-name*	ポリシー マップを作成して、入力ポリシーの QoS パラメータを指定します。
ステップ 4	switch(config-pmap)# **class** *class-name*	このポリシーに入力クラスを関連付け、このクラスのコンフィギュレーション モードを開始します。
ステップ 5	switch(config-pmap-c) **bandwidth percent** *percentage*	(任意)このクラスの着信トラフィックに割り当てられる保証帯域幅の割合を指定します。
ステップ 6	switch(config-pmap-c) **priority**	(任意)このクラスの入力トラフィックが完全プライオリティ キューにマッピングされるように指定します。
ステップ 7	switch(config)# **interface interface** {**ethernet** *slot/port*|**port-channel** *channel-number* }	指定されたインターフェイスのコンフィギュレーション モードを開始します。 **(注)** ポート チャネルのサービス ポリシーによって、個々のメンバ インターフェイスのサービス ポリシー設定が上書きされます。
ステップ 8	switch(config-if)# **service-policy input** *policy-name*	インターフェイスにポリシー マップを適用します。

次の例では、システム クラス best-effort-drop-class に、インターフェイス eth1/1 上の帯域幅の 20% が保証されます。

```
switch(config)# class-map best-effort-drop-class
switch(config-cmap)# match cos 5
switch(config)# policy-map policy1
switch(config-pmap)# class best-effort-drop-class
switch(config-pmap-c)# bandwidth percent 20
switch(config)# int eth1/1
switch(config-if)# service-policy input policy1
```

出力ポリシーの設定

入力ポリシーは、イーサネット インターフェイスで発信トラフィックに適用されるサービス ポリシーです。出力ポリシーを設定して、指定されたトラフィック クラスの帯域幅を確保したり、出力キューを設定したりできます。

出力ポリシーを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# class-map class-name`	出力ポリシーのクラス名を定義します。
ステップ 3	`switch(config)# policy-map policy1-name`	ポリシー マップを作成して、出力ポリシーの QoS パラメータを指定します。
ステップ 4	`switch(config-pmap)# class class-name`	このポリシーに出力クラスを関連付け、このクラスのコンフィギュレーション モードを開始します。
ステップ 5	`switch(config-pmap-c) bandwidth percent percentage`	このクラスに割り当てられた保証帯域幅の割合を指定します。
ステップ 6	`switch(config-pmap-c) priority`	このクラスの出力トラフィックが完全プライオリティ キューにマッピングされるよう指定します。
ステップ 7	`switch(config)# interface {ethernet slot/port|port-channel channel-number }`	指定されたインターフェイスのコンフィギュレーション モードを開始します。 **（注）** ポート チャネルのサービス ポリシーによって、個々のメンバ インターフェイスのサービス ポリシー設定が上書きされます。
ステップ 8	`switch(config-if)# service-policy output policy-name`	インターフェイスにポリシー マップを適用します。

次の例では、システム クラス best-effort-drop-class に、インターフェイス eth1/1 上の帯域幅の 20% が保証されます。

```
switch(config)# class-map best-effort-drop-class
switch(config-cmap)# match cos 5
switch(config)# policy-map policy1-egress
switch(config-pmap)# class best-effort-drop-class
switch(config-pmap-c)# bandwidth percent 20
switch(config)# int eth1/1
switch(config-if)# service-policy output policy1-egress
```

CHAPTER 32

ファイバ チャネル インターフェイスの設定

この章では、ファイバ チャネル インターフェイスおよび仮想ファイバ チャネル インターフェイスのインターフェイス設定について説明します。この章は、次の項で構成されています。

- ファイバ チャネル インターフェイスの概要（32-1 ページ）
- ファイバ チャネル インターフェイスの設定（32-8 ページ）
- ファイバ チャネル インターフェイスのグローバル属性の設定（32-14 ページ）
- ファイバ チャネル インターフェイスの確認（32-15 ページ）
- デフォルト設定（32-18 ページ）

ファイバ チャネル インターフェイスの概要

ここでは、ファイバ チャネル インターフェイスおよび仮想ファイバ チャネル インターフェイスについて説明します。この項では、次のトピックについて取り上げます。

- ライセンス要件（32-1 ページ）
- 物理ファイバ チャネル インターフェイス（32-2 ページ）
- 仮想ファイバ チャネル インターフェイス（32-2 ページ）
- インターフェイス モード（32-2 ページ）
- インターフェイス ステート（32-5 ページ）
- Buffer-to-Buffer credit（BB_credit）（32-8 ページ）

ライセンス要件

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

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

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

物理ファイバ チャネル インターフェイス

Cisco Nexus 5000 シリーズ スイッチは最大 8 つの物理ファイバ チャネル アップリンクを提供します。ファイバ チャネル インターフェイスは任意の拡張モジュールでサポートされます。ファイバ チャネルおよびイーサネット拡張モジュールには 4 つのファイバ チャネル インターフェイスが含まれます。

各ファイバ チャネル ポートをダウンリンク（サーバに接続）、またはアップリンク（データセンター SAN ネットワークに接続）として使用できます。ファイバ チャネル インターフェイスは、F、NP、E、TE、および SD のモードをサポートします。

仮想ファイバ チャネル インターフェイス

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

ネイティブ ファイバ チャネル インターフェイスと仮想ファイバ チャネル インターフェイスは、同じ CLI コマンドを使用して設定します。仮想ファイバ チャネル インターフェイスは F モードだけをサポートし、ネイティブ ファイバ チャネル インターフェイスでサポートされる機能のサブセットを提供します。

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

- SAN ポート チャネル
- VSAN（仮想 SAN）トランキング。仮想ファイバ チャネルは 1 つの VSAN に関連付けられます。
- SPAN 宛先は仮想ファイバ チャネル インターフェイスになることはできません。
- Buffer-to-Buffer credit（BB_credit）
- Exchange Link Parameter（ELP）または Fabric Shortest Path First（FSPF）プロトコル
- 物理属性の設定（速度、レート、モード、トランスミッタ情報、MTU サイズ）
- ポート トラッキング

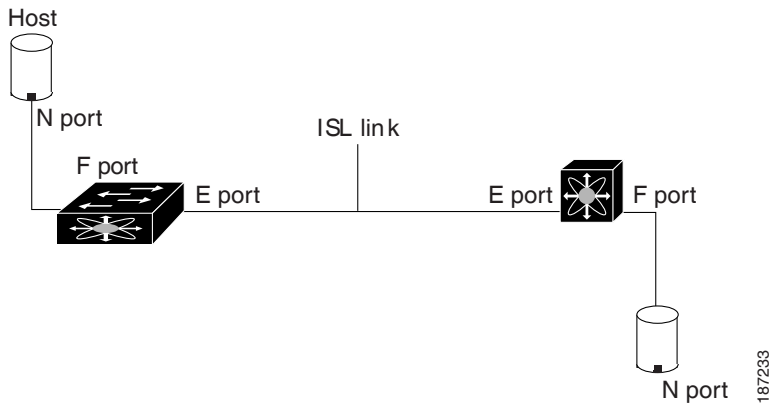
インターフェイス モード

スイッチ内の各物理ファイバ チャネル インターフェイスは、複数のポート モード（E モード、TE モード、F モード、および SD モード）のうちのいずれかで動作します（図 32-1 を参照）。物理ファイバ チャネル インターフェイスを E ポート、F ポート、または SD ポートとして設定できます。インターフェイスを auto モードに設定することもできます。ポート タイプは、インターフェイスの初期化中に判別されます。

NPV モードでは、ファイバ チャネル インターフェイスは NP モード、F モード、または SD モードで動作します。NPV モードの詳細については、第 34 章「NPV の設定」を参照してください。

仮想ファイバ チャネル インターフェイスは F モードでだけ設定できます。

図 32-1　　スイッチ ポート モード



（注） デフォルトでは、インターフェイスには VSAN 1 が自動的に割り当てられます。第 37 章「VSAN の設定と管理」を参照してください。

各インターフェイスには、管理設定と動作ステータスが対応付けられています。

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

ここでは、各インターフェイス モードの概要を示します。

- E ポート（32-3 ページ）
- F ポート（32-4 ページ）
- NP ポート（32-4 ページ）
- TE ポート（32-4 ページ）
- SD ポート（32-4 ページ）
- auto モード（32-4 ページ）

E ポート

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

別のスイッチに接続された E ポートも、SAN ポート チャネルを形成するように設定できます（第36 章「SAN ポート チャネルの設定」を参照）。

F ポート

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

NP ポート

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

NP ポートおよび NPV の詳細については、第 34 章「NPV の設定」を参照してください。

TE ポート

トランキング E ポート（TE ポート）モードでは、インターフェイスがトランキング拡張ポートとして機能します。別の TE ポートに接続し、2 つのスイッチ間で Extended ISL（EISL）を作成します。TE ポートは別の Cisco Nexus 5000 シリーズ スイッチまたは Cisco MDS 9000 ファミリ スイッチに接続します。E ポートの機能を拡張して、次の内容をサポートします。

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

TE ポート モードでは、すべてのフレームが VSAN 情報を含む EISL フレーム フォーマットで送信されます。相互接続されたスイッチは VSAN ID を使用して、1 つまたは複数の VSAN からのトラフィックを同一の物理リンク上で多重化します。この機能は、Cisco Nexus 5000 シリーズでは VSAN トランキングと呼ばれます（第35 章「VSAN トランキングの設定」を参照）。TE ポートは、クラス 3 およびクラス F サービスをサポートします。

SD ポート

SPAN 宛先ポート（SD ポート）モードでは、インターフェイスがスイッチド ポート アナライザ（SPAN）として機能します。SPAN 機能は、ファイバ チャネル インターフェイスを通過するネットワーク トラフィックを監視します。このモニタリングは、SD ポートに接続された標準ファイバ チャネル アナライザ（または同様のスイッチ プローブ）を使用して行われます。SD ポートはフレームを受信しません。送信元トラフィックのコピーを送信するだけです。SPAN 機能は他の機能に割り込むことなく、SPAN 送信元ポートのネットワーク トラフィックのスイッチングに影響しません。

auto モード

auto モードに設定されたインターフェイスは、F ポート、E ポート、または TE ポートのいずれかのモードで動作します。ポート モードは、インターフェイスの初期設定中に決定されます。たとえば、インターフェイスがノード（ホストまたはディスク）に接続されている場合、F ポート モードで動作します。インターフェイスがサードパーティ製のスイッチに接続されている場合、E ポート モードで動作します。インターフェイスが Cisco Nexus 5000 シリーズ または Cisco MDS 9000 ファミリの別のスイッチに接続されている場合、TE ポート モードで動作できます（第35 章「VSAN トランキングの設定」を参照）。

SD ポートは初期化で判別されず、管理上設定されます。

インターフェイス ステート

インターフェイス ステートは、インターフェイスの管理設定および物理リンクのダイナミックステートによって異なります。ここでは、ステートと、ステートに影響を与える設定について説明します。

- 管理ステート (32-5 ページ)
- 動作ステート (32-5 ページ)
- 理由コード (32-6 ページ)

管理ステート

管理のステートは、インターフェイスの管理設定を表します。表 32-1 に、管理ステートを示します。

表 32-1　管理ステート

管理ステート	説明
Up	インターフェイスはイネーブルです。
Down	インターフェイスはディセーブルです。インターフェイスをシャットダウンして管理上のディセーブル状態にした場合は、物理リンク層ステートの変更が無視されます。

動作ステート

動作ステートは、インターフェイスの現在の動作ステートを示します。表 32-2 に動作ステートを示します。

表 32-2　動作ステート

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

理由コード

理由コードは、インターフェイスの動作ステートによって異なります。表 32-3 に動作ステートの理由コードを示します。

表 32-3　インターフェイス ステートの理由コード

管理設定	動作ステータス	原因コード
Up	Up	なし。
Down	Down	管理上のダウン。インターフェイスを管理上ダウンの状態に設定する場合、インターフェイスをディセーブルにします。トラフィックが受信または送信されません。
Up	Down	表 32-4 を参照してください。

（注）　表 32-4 に示されている理由コードは一部だけです。

管理ステートが up で、動作ステートが down の場合、理由コードは、動作不能理由コードに基づいて異なります。表 32-4 に動作不能ステートの理由コードを示します。

表 32-4　非動作ステートの原因コード

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

表 32-4　非動作ステートの原因コード（続き）

理由コード（長いバージョン）	説明	適用可能なモード
Error disabled	エラー条件は、管理上の注意を必要とします。さまざまな理由でインターフェイスがエラーディセーブルになることがあります。次に例を示します。 • 設定障害。 • 互換性のない BB_credit 設定。 インターフェイスを正常に動作させるには、まずこのステートの原因となるエラー条件を修正し、次にインターフェイスを管理上シャットダウンにするか、インターフェイスをイネーブルにします。	
Isolation because limit of active port channels is exceeded.	スイッチにアクティブ SAN ポート チャネルの最大数がすでに設定されているので、インターフェイスは隔離されます。	
Isolation due to ELP failure	ポート ネゴシエーションが失敗しました。	E ポートと TE ポートのみ
Isolation due to ESC failure	ポート ネゴシエーションが失敗しました。	
Isolation due to domain overlap	Fibre Channel Domain（fcdomain）のオーバーラップ。	
Isolation due to domain ID assignment failure	割り当てられたドメイン ID が無効です。	
Isolation due to the other side of the link E port isolated	リンクのもう一方の端の E ポートが分離しています。	
Isolation due to invalid fabric reconfiguration	ファブリックの再設定によりポートが分離されました。	
Isolation due to domain manager disabled	fcdomain 機能がディセーブルです。	
Isolation due to zone merge failure	ゾーン結合に失敗しました。	
Isolation due to VSAN mismatch	ISL の両端の VSAN が異なります。	
port channel administratively down	SAN ポート チャネルに所属するインターフェイスがダウンの状態です。	SAN ポート チャネル インターフェイスのみ
Suspended due to incompatible speed	SAN ポート チャネルに所属するインターフェイスに互換性のない速度が存在します。	
Suspended due to incompatible mode	SAN ポート チャネルに所属するインターフェイスに互換性のないモードが存在します。	
Suspended due to incompatible remote switch WWN	不適切な接続が検出されました。SAN ポート チャネルのすべてのインターフェイスが同一のスイッチ ペアに接続されている必要があります。	
Bound physical interface down	仮想ファイバ チャネル インターフェイスにバインドされたイーサネット インターフェイスが動作していません。	仮想ファイバ チャネル インターフェイスのみ

表 32-4　非動作ステートの原因コード（続き）

理由コード（長いバージョン）	説明	適用可能なモード
STP not forwarding in FCoE mapped VLAN	仮想ファイバ チャネル インターフェイスにバインドされたイーサネット インターフェイスが、仮想ファイバ チャネル インターフェイスに関連付けられた VLAN に対して STP フォワーディング ステートではありません。	仮想ファイバ チャネル インターフェイスのみ

Buffer-to-Buffer credit（BB_credit）

BB_credit はフロー制御メカニズムで、ファイバ チャネル インターフェイスがフレームをドロップしないようにします。BB_creditは、ホップごとにネゴシエーションします。

Cisco Nexus 5000 シリーズ スイッチでは、BB_credit メカニズムは仮想ファイバ チャネル インターフェイスではなく、ファイバ チャネル インターフェイスで使用されます。仮想ファイバ チャネル インターフェイスは、基本の物理イーサネット インターフェイスの機能に基づいて、フロー制御を実行します。

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

（注）受信 BB_credit 値は、ポート モードによって異なります。物理ファイバ チャネル インターフェイスの場合、F モードおよび E モード インターフェイスのデフォルト値は 16 です。必要に応じて、この値を変更できます。最大値は 64 です。

（注）仮想ファイバ チャネル インターフェイスの場合、BB_credit は使用されません。

ファイバ チャネル インターフェイスの設定

ここでは、ファイバ チャネル インターフェイス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。

- ファイバ チャネル インターフェイスの設定（32-9 ページ）
- 管理ステートの設定インターフェイスの管理ステートの設定（32-9 ページ）
- インターフェイス モードの設定（32-10 ページ）
- インターフェイスの説明の設定（32-10 ページ）
- ポート速度の設定（32-11 ページ）
- SD ポート フレーム カプセル化の設定（32-11 ページ）
- 受信データ フィールド サイズの設定（32-12 ページ）
- ビット エラーしきい値の概要（32-12 ページ）
- BB_credit の設定（32-13 ページ）

ファイバ チャネル インターフェイスの設定

ファイバ チャネル インターフェイスを設定する手順は、次のとおりです。

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

インターフェイスの範囲を設定する手順は、次のとおりです。

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

管理ステートの設定インターフェイスの管理ステートの設定

インターフェイスを正常にシャットダウンする手順は、次のとおりです。

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

トラフィック フローをイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** {**fc** *slot/port*}|{**vfc** *vfc-id*}	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **no shutdown**	**no** プレフィックスが使用された場合（動作ステートは up）、管理上トラフィックを許可するようにトラフィック フローをイネーブルにします。 バインドされたイーサネット インターフェイスが動作し、その STP ポート ステートがアクティブである場合は、仮想ファイバ チャネル インターフェイスが動作状態になります。

インターフェイス モードの設定

インターフェイス モードを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** {**fc** *slot/port*}|{**vfc** *vfc-id*}	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport mode F**	仮想ファイバ チャネルの場合、F ポート モードだけがサポートされます。
	switch(config-if)# **switchport mode E | F | SD | auto**	ファイバ チャネル インターフェイスの場合、モードを E、F、または SD ポート モードに設定できます。E、F、または TE ポート モード動作（SD ポート モードは含まない）を自動ネゴシエーションするには、モードを auto に設定します。 **（注）** SD ポートを自動では設定できません。このポートは管理上設定する必要があります。

インターフェイスの説明の設定

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

インターフェイスの説明を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface** {**fc** *slot/port*}|{**vfc** *vfc-id*}	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	switch(config-if)# **switchport description cisco-HBA2**	インターフェイスの説明を設定します。ストリングの長さは、最大 80 文字まで可能です。
	switch(config-if)# **no switchport description**	インターフェイスの説明をクリアします。

ポート速度の設定

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

注意　ポート速度の変更は中断を伴う動作です。

インターフェイスのポート速度を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot/port*	指定されたインターフェイスを選択して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport speed 1000**	インターフェイスのポート速度を 1000 Mbps に設定します。 数値は、Mbps 単位の速度を表します。1 Gbps インターフェイスには **1000 Mbps** の速度、2 Gbps インターフェイスには **2000 Mbps** の速度、4 Gbps インターフェイスには **4000**、または **auto**（デフォルト）を設定できます。
	switch(config-if)# **no switchport speed**	インターフェイスの出荷時の設定（**auto**）管理速度に戻します。

自動検知

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

SD ポート フレーム カプセル化の設定

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

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

受信データ フィールド サイズの設定

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

受信データ フィールド サイズを設定する手順は、次のとおりです。

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

ビット エラーしきい値の概要

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

ビット エラーは次のような理由のため発生します。

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

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

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

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

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

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot/port*	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport ignore bit-errors**	ビット エラーしきい値イベントを検出したとき、インターフェイスがディセーブルにならないようにします。
	switch(config-if)# **no switchport ignore bit-errors**	ビット エラーしきい値イベントを検出したとき、インターフェイスがイネーブルにならないようにします。

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

BB_credit の設定

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

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot/port*	ファイバ チャネル インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport fcrxbbcredit default**	デフォルトの使用可能な値を選択されたインターフェイスに適用します。使用可能な値は、ポート モードによって異なります。デフォルト値は、ポート機能に応じて割り当てられます。
	switch(config-if)# **switchport fcrxbbcredit 5**	選択されたインターフェイスの BB_credit を 5 に割り当てます。BB_credit を割り当てる範囲は、1 ～ 64 です。
	switch(config-if)# **switchport fcrxbbcredit 5 mode E**	ポートが E モードまたは TE モードで動作する場合は、この値を割り当てます。BB_credit を割り当てる範囲は、1 ～ 64 です。
	switch(config-if)# **switchport fcrxbbcredit 5 mode Fx**	ポートが F モードで動作する場合は、この値を割り当てます。BB_credit を割り当てる範囲は、1 ～ 64 です。
ステップ 4	switch(config-if# **do show int fc** *slot/port*	送受信の BB_credit をこのインターフェイスのその他の関連インターフェイス情報とともに表示します。 （注）　レジスタが読み取られるとき、BB_credit は正しい値です。データ トラフィックが遅いときに状況を確認するのに役立ちます。

ファイバ チャネル インターフェイスのグローバル属性の設定

ここでは、スイッチのすべてのファイバ チャネル インターフェイスに適用されるグローバル属性の設定について説明します。この項では、次のトピックについて取り上げます。

- スイッチ ポート属性のデフォルト値の設定（32-14 ページ）
- N ポート識別子仮想化の概要（32-15 ページ）
- N ポート識別子仮想化のイネーブル化（32-15 ページ）

スイッチ ポート属性のデフォルト値の設定

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

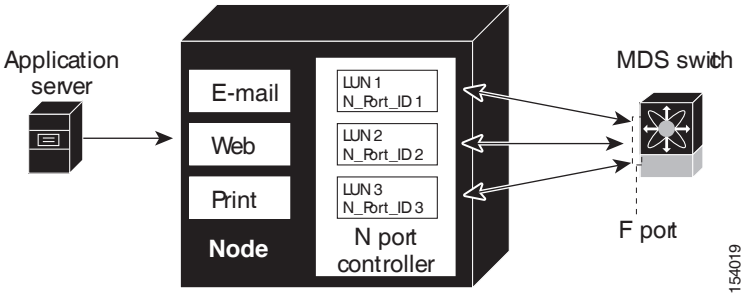
スイッチ ポート属性を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# no system default switchport shutdown san`	インターフェイス管理ステートのデフォルト設定を up に設定します（出荷時のデフォルト設定は down です）。 **ヒント**　このコマンドは、管理ステートに対してユーザ設定が存在しないインターフェイスにだけ適用されます。
	`switch(config)# system default switchport shutdown san`	インターフェイス管理ステートのデフォルト設定を down に設定します。これが出荷時のデフォルト設定です。 **ヒント**　このコマンドは、管理ステートに対してユーザ設定が存在しないインターフェイスにだけ適用されます。
	`switch(config)# system default switchport trunk mode auto`	インターフェイスの管理トランク モード ステートのデフォルト設定を auto に設定します。 **（注）**　デフォルト設定のトランク モードは on です。

N ポート識別子仮想化の概要

N ポート識別子仮想化（NPIV）は単一 N ポートに複数の FC ID を割り当てる手段を提供します。この機能を使用すると、N ポート上の複数のアプリケーションが異なる ID を使用したり、アクセス コントロール、ゾーニング、ポート セキュリティをアプリケーション レベルで実装したりできます。図 32-2 に、NPIV の使用例を示します。

図 32-2　NPIV の例



N ポート識別子仮想化のイネーブル化

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

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

スイッチの NPIV をイネーブルまたはディセーブルにする手順は、次のとおりです。

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

ファイバ チャネル インターフェイスの確認

ここでは、ファイバ チャネル インターフェイスを表示するコマンドについて説明します。

- SFP トランスミッタ タイプの確認（32-16 ページ）
- インターフェイス情報の確認（32-16 ページ）
- BB_credit 情報の確認（32-17 ページ）

SFP トランスミッタ タイプの確認

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

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

インターフェイス情報の確認

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

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

```
interface fc2/1 - 4 , fc3/2 - 3
```

次に、すべてのインターフェイスを表示する例を示します。

```
switch# show interface
fc3/1 is up
...
fc3/3 is up
...
Ethernet1/3 is up
...
mgmt0 is up
...
vethernet1/1 is up
...
vfc 1 is up
...
```

次に、指定された複数のインターフェイスを表示する例を示します。

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

次に、特定の 1 つのインターフェイスを表示する例を示します。

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

次に、インターフェイスの説明を表示する例を示します。

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

次に、すべてのインターフェイスを表示する例を示します（簡略）。

```
switch# show interface brief
```

次に、インターフェイス カウンタを表示する例を示します。

```
switch# show interface counters
```

次に、特定のインターフェイスのトランシーバ情報を表示する例を示します。

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

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

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

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

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

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

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

BB_credit 情報の確認

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

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

デフォルト設定

表 32-5 に、ネイティブ ファイバ チャネル インターフェイス パラメータのデフォルト設定値を示します。

表 32-5　デフォルトのネイティブ ファイバ チャネル インターフェイス パラメータ

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

表 32-5 に、仮想ファイバ チャネル インターフェイス パラメータのデフォルト設定値を示します。

表 32-6　デフォルトの仮想ファイバ チャネル インターフェイス パラメータ

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

CHAPTER 33

ドメイン パラメータの設定

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

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

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

この章は、次の項で構成されています。

- ファイバ チャネル ドメインの概要（33-1 ページ）
- ドメイン ID（33-7 ページ）
- FC ID（33-14 ページ）
- fcdomain 情報の確認（33-18 ページ）
- デフォルト設定（33-20 ページ）

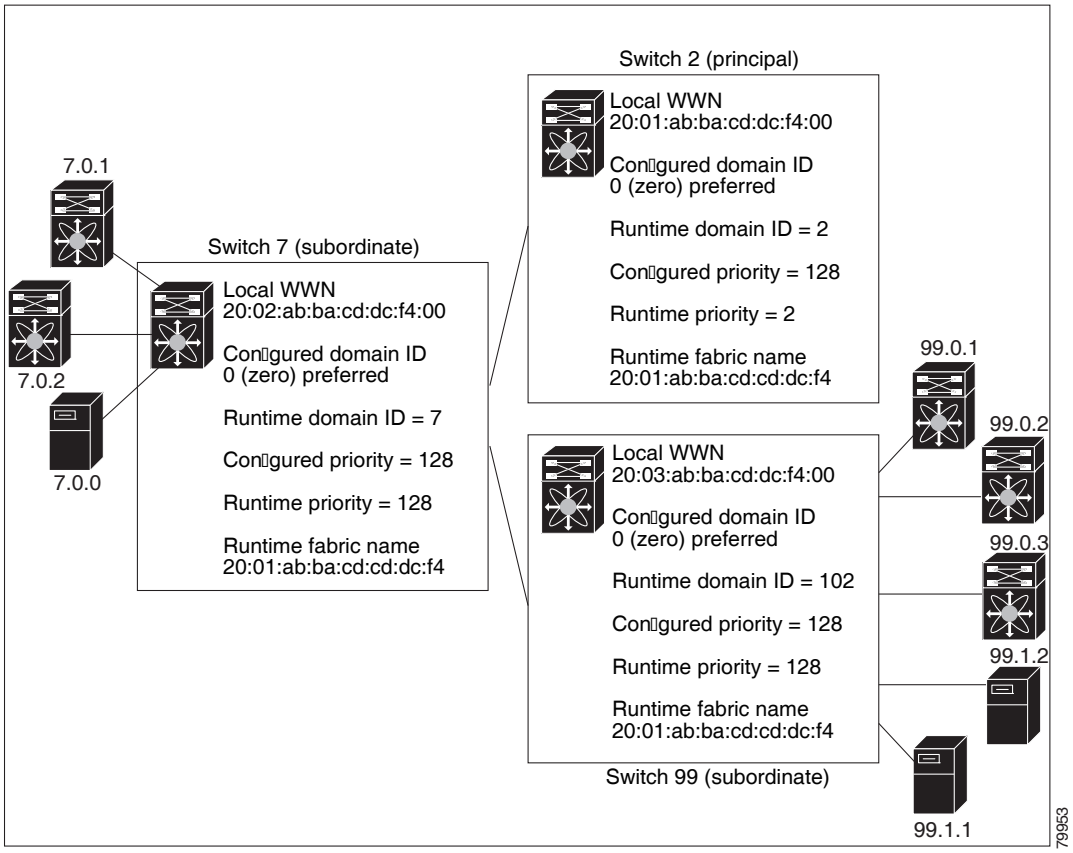
ファイバ チャネル ドメインの概要

ここでは、fcdomain の各フェーズについて説明します。

- 主要スイッチの選択：このフェーズでは、ファブリック内で一意の主要スイッチを選択できます。
- ドメイン ID の配信：このフェーズでは、ファブリック内のスイッチごとに、一意のドメイン ID を取得できます。
- FC ID の割り当て：このフェーズでは、ファブリック内の対応するスイッチに接続された各デバイスに、一意の FC ID を割り当てることができます。
- ファブリックの再設定：このフェーズでは、ファブリック内のすべてのスイッチを再同期化して、新しい主要スイッチ選択フェーズを同時に再開できるようにします。

設定の例については、図 33-1を参照してください。

図 33-1　　fcdomain の設定例



（注）　すべての手順で使用されるドメイン ID および VSAN 値は、単なる例です。必ずご使用の設定に適用される ID および値を使用してください。

ここでは、fcdomain 機能について説明します。ここで説明する内容は、次のとおりです。

- ドメインの再起動の概要（33-3 ページ）
- ドメインの再起動（33-3 ページ）
- ドメイン マネージャの高速再起動について（33-4 ページ）
- ドメイン マネージャの高速再起動のイネーブル化（33-4 ページ）
- スイッチ プライオリティの概要（33-4 ページ）
- スイッチ プライオリティの設定（33-5 ページ）
- fcdomain の開始について（33-5 ページ）
- fcdomain のディセーブル化または再イネーブル化（33-5 ページ）
- ファブリック名の設定（33-5 ページ）
- 着信 RCF について（33-6 ページ）
- 着信 RCF の拒否（33-6 ページ）

- 結合されたファブリックの自動再設定について（33-6 ページ）
- 自動再設定のイネーブル化（33-7 ページ）

ドメインの再起動の概要

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

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

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

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

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

fcdomain restart コマンドを使用すると、変更が実行時の設定に適用されます。**disruptive オプションを使用すると**、優先ドメイン ID などほとんどの設定は、対応する実行時の値に適用できます（「ドメイン ID の概要」セクション（33-7 ページ）を参照）。

ドメインの再起動

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

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

ドメイン マネージャの高速再起動について

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

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

ドメイン マネージャの高速再起動のイネーブル化

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

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

スイッチ プライオリティの概要

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

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

プライオリティ設定は、fcdomain の再起動の実行時に適用されます（「ドメインの再起動の概要」セクション（33-3 ページ）を参照）。この設定は、中断再起動および非中断再起動のどちらにも適用できます。

スイッチ プライオリティの設定

主要スイッチにプライオリティを設定する手順は、次のとおりです。

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

fcdomain の開始について

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

fcdomain のディセーブル化または再イネーブル化

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

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

ファブリック名の設定

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

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

着信 RCF について

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

rcf-reject オプションは即座に有効になります。

fcdomain の再起動は不要です。

（注）　仮想ファイバ チャネル インターフェイスは F ポート モードだけで動作するので、これらのインターフェイスに RCF reject オプションを設定する必要はありません。

着信 RCF の拒否

着信 RCF 要求フレームを拒否する手順は、次のとおりです。

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

結合されたファブリックの自動再設定について

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

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

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

自動再設定のイネーブル化

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

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

ドメイン ID

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

ここでは、ドメイン ID の設定方法について説明します。具体的な内容は次のとおりです。

- ドメイン ID の概要（33-7 ページ）
- スタティック ドメイン ID または優先ドメイン ID の指定（33-9 ページ）
- 許可ドメイン ID リストの概要（33-10 ページ）
- 許可ドメイン ID リストの設定（33-10 ページ）
- 許可ドメイン ID リストの CFS 配信について（33-11 ページ）
- 配信のイネーブル化（33-11 ページ）
- ファブリックのロック（33-11 ページ）
- 変更のコミット（33-11 ページ）
- 変更の破棄（33-12 ページ）
- ファブリックのロックのクリア（33-12 ページ）
- CFS 配信ステータスの表示（33-12 ページ）
- 保留中の変更の表示（33-13 ページ）
- セッション ステータスの表示（33-13 ページ）
- 連続ドメイン ID 割り当ての概要（33-13 ページ）
- 連続ドメイン ID 割り当てのイネーブル化（33-14 ページ）

ドメイン ID の概要

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

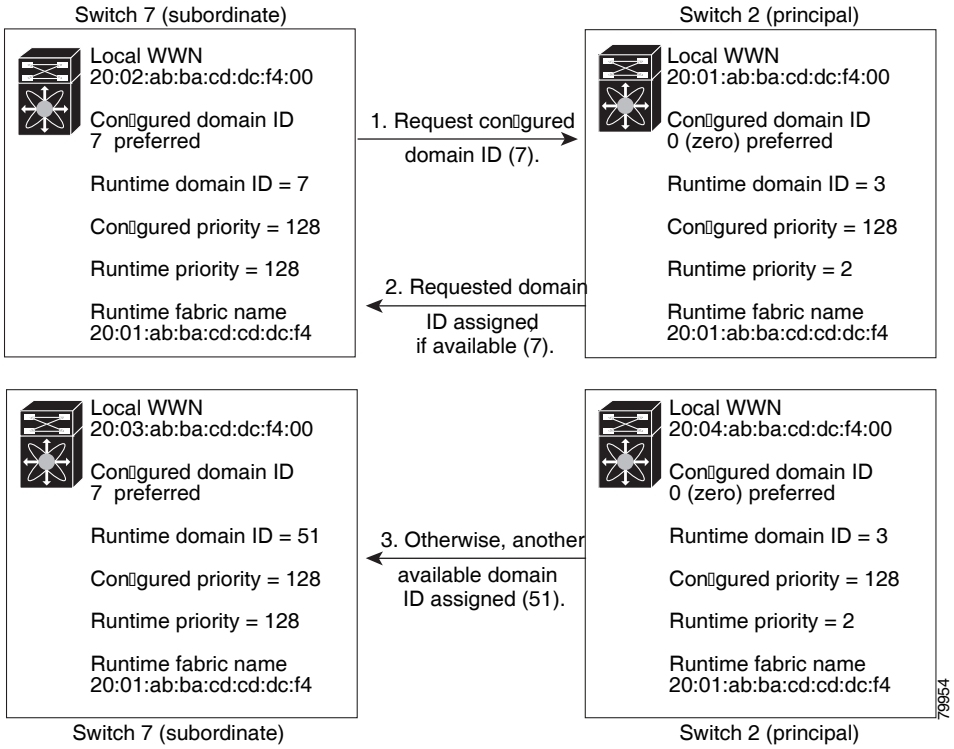
（注） 値 0（ゼロ）を設定できるのは、優先オプションを使用した場合だけです。

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

下位スイッチがドメインを要求する場合は、次のプロセスが実行されます（図 33-2 を参照）。

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

図 33-2　preferred オプションを使用した設定プロセス



下位スイッチの動作は、次の 3 つの要素により異なります。

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

状況に応じて、次のように変更されます。

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

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

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

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

（注）　許可ドメイン ID リストを設定した場合、追加するドメイン ID は VSAN のその範囲内にある必要があります。「許可ドメイン ID リストの概要」セクション（33-10 ページ）を参照してください。

スタティック ドメイン ID または優先ドメイン ID の指定

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

スタティック オプションは、中断再起動または非中断再起動後の実行時に適用できますが、優先オプションは中断再起動後の実行時にだけ適用できます（「ドメインの再起動の概要」セクション（33-3 ページ）を参照）。

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

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

	コマンド	目的
ステップ 1	`switch#` **`configuration terminal`** `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`fcdomain domain`** *`domain-id`* **`preferred vsan`** *`vsan-id`*	preferred ドメイン ID 3 を要求するために指定の VSAN 内のスイッチを設定し、主要スイッチによって割り当てられた値をすべて受け入れます。ドメインの範囲は 1 ～ 239 です。
	`switch(config)#` **`no fcdomain domain`** *`domain-id`* **`preferred vsan`** *`vsan-id`*	指定の VSAN 内の設定済みドメイン ID を 0（デフォルト）にリセットします。設定済みドメイン ID は 0 preferred になります。

	コマンド	目的
ステップ 3	switch(config)# **fcdomain domain** *domain-id* **static vsan** *vsan-id*	特定の値だけを受け入れるように指定の VSAN 内のスイッチを設定し、要求されたドメイン ID が許可されない場合は、指定の VSAN 内のローカル インターフェイスを隔離ステートに移行します。
	switch(config)# **no fcdomain domain** *domain-id* **static vsan** *vsan-id*	設定済みドメイン ID を、指定 VSAN 内の出荷時のデフォルト設定にリセットします。設定済みドメイン ID は 0 preferred になります。

許可ドメイン ID リストの概要

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

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

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

許可ドメイン ID リストは、次の条件を満たす必要があります。

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

許可ドメイン ID リストの設定

許可ドメイン ID リストを設定する手順は、次のとおりです。

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

許可ドメイン ID リストの CFS 配信について

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

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

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

CFS の詳細については、第 21 章「CFS の使用」を参照してください。

配信のイネーブル化

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

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

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

ファブリックのロック

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

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

変更のコミット

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

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

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

変更の破棄

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

保留中のドメイン設定変更を廃棄して、ファブリックのロックを解除する手順は、次のとおりです。

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

ファブリックのロックのクリア

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

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

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

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

CFS 配信ステータスの表示

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

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

保留中の変更の表示

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

```
switch# show fcdomain pending vsan 10

Pending Configured Allowed Domains
----------------------------------

VSAN 10
Assigned or unallowed domain IDs: 1-9,24,100,231-239.
[User] configured allowed domain IDs: 10-230.
```

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

```
switch# show fcdomain pending-diff vsan 10

Current Configured Allowed Domains
----------------------------------

VSAN 10
Assigned or unallowed domain IDs: 24,100.
[User] configured allowed domain IDs: 1-239.

Pending Configured Allowed Domains
----------------------------------

VSAN 10
Assigned or unallowed domain IDs: 1-9,24,100,231-239.
[User] configured allowed domain IDs: 10-230.
```

セッション ステータスの表示

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

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

連続ドメイン ID 割り当ての概要

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

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

連続ドメイン ID 割り当てのイネーブル化

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

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

FC ID

Cisco Nexus 5000 シリーズ スイッチにログインしたN ポートには、FC ID が割り当てられます。デフォルトでは、固定的 FC ID 機能はイネーブルです。この機能がディセーブルの場合は、次のようになります。

- N ポートは Cisco Nexus 5000 シリーズ スイッチにログインします。要求元 N ポートの WWN および割り当てられた FC ID が維持され、揮発性キャッシュに格納されます。この揮発性キャッシュの内容は、再起動時に保存されません。
- スイッチは、FC ID と WWN のバインディングをベストエフォート方式で保持するように設計されています。たとえば、スイッチから 1 つの N ポートを切断したあとに、別のデバイスから FC ID が要求されると、この要求が許可されて、WWN と初期 FC ID の関連付けが解除されます。
- 揮発性キャッシュには、WWN と FC ID のバインディングのエントリを 4000 まで格納できます。このキャッシュが満杯になると、新しい（より最近の）エントリによって、キャッシュ内の最も古いエントリが上書きされます。この場合、最も古いエントリの対応する WWN と FC ID の関連付けが失われます。
- N ポートを取り外し、同じスイッチの任意のポートに接続すると、（このポートが同じ VSAN に属するかぎり）この N ポートには同じ FC ID が割り当てられます。

ここでは FC ID の設定について説明します。具体的な内容は次のとおりです。

- 永続的 FC ID について（33-15 ページ）
- 固定的 FC ID 機能のイネーブル化（33-15 ページ）
- 永続的 FC ID 設定時の注意事項（33-15 ページ）
- 固定的 FC ID の設定（33-16 ページ）
- HBA に対する一意のエリア FC ID について（33-16 ページ）
- HBA に対する一意のエリア FC ID の設定（33-16 ページ）
- 固定的 FC ID の選択消去の概要（33-18 ページ）
- 固定的 FC ID の消去（33-18 ページ）

永続的 FC ID について

永続的 FC ID がイネーブルの場合は、次のようになります。

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

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

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

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

固定的 FC ID 機能のイネーブル化

永続的 FC ID 機能をイネーブルにする手順は、次のとおりです。

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

永続的 FC ID 設定時の注意事項

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

永続的 FC ID を手動で設定するための要件は、次のとおりです。

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

固定的 FC ID の設定

永続的 FC ID を設定する手順は、次のとおりです。

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

HBA に対する一意のエリア FC ID について

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

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

Cisco Nexus 5000 シリーズ スイッチでは、FC ID の永続性機能によってこの要件が満たされます。この機能を使用すると、ストレージ ポートまたは HBA ポートに異なるエリアを持つ FC ID を事前に割り当てることができます。

HBA に対する一意のエリア FC ID の設定

次のタスクでは、111（16 進値では 6f）のスイッチ ドメインの設定例を使用します。サーバは FCoE を介してスイッチに接続されます。HBA ポートはインターフェイス vfc20/1 に接続され、ストレージ ポートは同じスイッチのインターフェイス fc2/3 に接続されます。

HBA ポートに異なるエリア ID を設定する手順は、次のとおりです。

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

```
switch# show flogi database
--------------------------------------------------------------------------------------
INTERFACE    VSAN    FCID        PORT NAME                   NODE NAME
--------------------------------------------------------------------------------------
 vfc10/1     3       0x6f7703    50:05:08:b2:00:71:c8:c2     50:05:08:b2:00:71:c8:c0
 fc2/3       3       0x6f7704    50:06:0e:80:03:29:61:0f     50:06:0e:80:03:29:61:0f
```

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

ステップ 2　Cisco Nexus 5000 シリーズ スイッチの HBA インターフェイスをシャットダウンします。

```
switch# configuration terminal
switch(config)# interface vfc20/1
switch(config-if)# shutdown
switch(config-if)# end
switch#
```

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

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

この機能がディセーブルの場合は、この手順を継続して、固定的 FC ID をイネーブルにします。

この機能がすでにイネーブルの場合は、ステップ 5 に進みます。

ステップ 4　Cisco Nexus 5000 シリーズ スイッチで永続的 FC ID をイネーブルにします。

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

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

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

ステップ 6　Cisco Nexus 5000 シリーズ スイッチの HBA インターフェイスをイネーブルにします。

```
switch# configuration terminal
switch(config)# interface vfc20/1
switch(config-if)# no shutdown
switch(config-if)# end
switch#
```

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

```
switch# show flogi database
--------------------------------------------------------------------------------
INTERFACE   VSAN    FCID        PORT NAME                   NODE NAME
--------------------------------------------------------------------------------
 vfc20/1    3       0x6fee00    50:05:08:b2:00:71:c8:c2     50:05:08:b2:00:71:c8:c0
 fc2/3      3       0x6f7704    50:06:0e:80:03:29:61:0f     50:06:0e:80:03:29:61:0f
```

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

固定的 FC ID の選択消去の概要

固定的 FC ID は、選択的に消去できます。現在使用中のスタティック エントリおよび FC ID は、削除できません。表 33-1 に、固定的 FC ID の消去時に削除または保持される FC ID エントリを示します。

表 33-1　消去される FC ID

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

固定的 FC ID の消去

永続的 FC ID を消去する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# purge fcdomain fcid vsan vsan-id`	指定の VSAN の未使用のダイナミック FC ID をすべて消去します。
	`switch# purge fcdomain fcid vsan vsan-id - vsan-id`	指定の VSAN 範囲の未使用のダイナミック FC ID をすべて消去します。

fcdomain 情報の確認

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

次に、fcdomain 設定に関する情報を表示する例を示します。

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

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

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

```
switch# show fcdomain domain-list vsan 76

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

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

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

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

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

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

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

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

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

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

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

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

デフォルト設定

表 33-2 に、すべての fcdomain パラメータのデフォルト設定値を示します。

表 33-2　デフォルト fcdomain パラメータ

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

CHAPTER 34

NPV の設定

この章では、Cisco Nexus 5000 シリーズ スイッチで N ポート 仮想化（NPV）を設定する方法を説明します。

この章は、次の項で構成されています。

- NPV について（34-1 ページ）
- 注意事項および制約事項（34-6 ページ）
- NPV の設定（34-6 ページ）
- NPV の確認（34-9 ページ）

NPV について

ここでは、NPV 設定について説明します。具体的な内容は次のとおりです。

- NPV の概要（34-1 ページ）
- NPV モード（34-2 ページ）
- サーバ インターフェイス（34-2 ページ）
- NP アップリンク（外部インターフェイス）（34-3 ページ）
- FLOGI 動作（34-3 ページ）
- NPV トラフィック管理（34-4 ページ）
- NPV トラフィック管理の注意事項（34-5 ページ）

NPV の概要

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

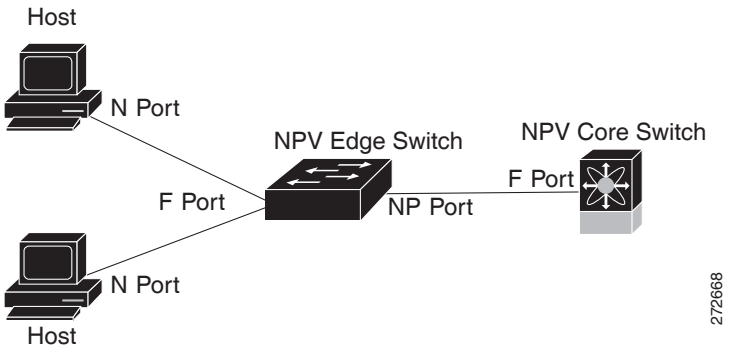
ファブリック モードでは、SAN に参加する各スイッチにドメイン ID が割り当てられます。各 SAN（または VSAN）は、最大 239 個のドメイン ID 数をサポートするため、SAN におけるスイッチ数は 239 台に制限されます。多数のエッジ スイッチが配置されている SAN トポロジでは、SAN はこの制限を超えて拡張する必要がある場合があります。NPV は、コア スイッチのドメイン ID を複数のエッジ スイッチ間で共有することによって、このドメイン ID の制限を解消します。

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

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

図 34-1 に、インターフェイスレベルでの NPV 構成を示します。

図 34-1　NPV のインターフェイスでの設定



NPV モード

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

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

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

サーバ インターフェイス

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

（注） NPIV を使用するには、NPIV 機能をイネーブルにし、複数のデバイスをサポートするサーバ インターフェイスを再初期化します。NPIV の詳細については、「N ポート識別子仮想化の概要」セクション（32-15 ページ）を参照してください。

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

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

NP アップリンク（外部インターフェイス）

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

NP アップリンクは、エッジ スイッチの NP ポートからコア スイッチの F ポートまでの接続です。NP アップリンクが確立されると、エッジ スイッチは、コア スイッチにファブリック ログイン メッセージ（FLOGI）を送信し、FLOGI が正常に実行された場合は、エッジ スイッチ自身をコア スイッチのネーム サーバに登録します。この NP アップリンクに接続されたエンド デバイスからの以降の FLOGI は、ファブリック検出メッセージ（FDISC）に変換されます。ファブリック ログインの詳細については、「ファブリック ログインに関する情報」セクション（41-1 ページ）を参照してください。

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

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

FLOGI 動作

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

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

表 34-1に、NPV モードで使用されるエッジ スイッチのポートおよびノード名を示します。

表 34-1　エッジ スイッチ FLOGI パラメータ

パラメータ	派生元
pWWN	エッジ スイッチの NP ポートの fWWN
nWWN	エッジ スイッチの VSAN ベースの sWWN
シンボリック ポート名	エッジ スイッチ名および NP ポート インターフェイスの文字列 **（注）** スイッチ名が使用できない場合、"switch" が出力されます。たとえば、switch: fc 1/5 のようになります。
IP アドレス	エッジ スイッチの IP アドレス
シンボリック ノード名	エッジ スイッチ名

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

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

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

ゾーン分割の詳細については、「ゾーン分割に関する情報」セクション（38-1 ページ）を参照してください。

NPV トラフィック管理

Cisco Nexus 5000 シリーズ スイッチは、NPV トラフィック管理機能を備えています。ここでは NPV トラフィック管理について説明します。具体的な内容は次のとおりです。

- 自動アップリンク選択（34-4 ページ）
- トラフィック マップ（34-4 ページ）
- ディスラプティブ ロード バランシング（34-5 ページ）

自動アップリンク選択

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

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

トラフィック マップ

リリース 4（1a）N2（1）以降のソフトウェア リリースでは、NPV はトラフィック マップをサポートします。トラフィック マップにより、サーバ インターフェイスがコア スイッチに接続するために使用可能な NP アップリンクを指定できます。

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

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

- 特定のサーバ インターフェイス（またはサーバ インターフェイスの範囲）に NP アップリンクの事前設定された設定を割り当てることによって、トラフィック エンジニアリングが容易になります。

- インターフェイスの再初期化またはスイッチの再起動後に、サーバ インターフェイスは常に同じ NP アップリンク（または指定された NP アップリンクのセットのいずれか）に接続するので、永続的な FC ID 機能の適切な動作が確保されます。

ディスラプティブ ロード バランシング

リリース 4(0)N1(2a) 以降のソフトウェア リリースでは、NPV はディスラプティブ ロード バランシングをサポートします。ディスラプティブ ロード バランシングがイネーブルの場合、新しい NP アップリンクが動作すると、NPV はすべての利用可能な NP アップリンク全体にサーバ インターフェイスを再配布します。サーバ インターフェイスを 1 つの NP アップリンクからの別の NP アップリンクに移動するために、NPV はサーバ インターフェイスを強制的に再初期化して、サーバがコア スイッチへのログインを新たに実行するようにします。

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

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

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

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

NPV トラフィック管理の注意事項

NPV トラフィック管理を導入する際には、次の注意事項に従ってください。

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

注意事項および制約事項

NPV を設定する場合、次の注意事項および制限事項に注意してください。

- NPV モードでは、2 つのエンド デバイス間のやり取りに、エッジ スイッチからコアへの同じアップリンクが使用されるため、順序どおりのデータ配信を行う必要はありません。エッジ スイッチのアップストリームのコア スイッチが設定されている場合は、順序どおりの配信を実行します。
- コア スイッチ上で使用できるすべてのメンバ タイプを使用して、エッジ スイッチに接続されているエンド デバイスのゾーン分割を設定できます。fWWN、sWWN、ドメイン、またはポートベースのゾーン分割では、コンフィギュレーション コマンドでコア スイッチの fWWN、sWWN、ドメイン、またはポートを使用してください。
- NPV モードでは、ポート トラッキングはサポートされません。
- NPV スイッチを介してログインするデバイスには、コア スイッチでポート セキュリティがサポートされます。ポート セキュリティは、コア スイッチでインターフェイスごとにイネーブルにされます。NPV スイッチを介してログインするデバイスのコア スイッチでセキュリティ ポートをイネーブルにするには、次の要件に従う必要があります。
  - 内部 FLOGI がポート セキュリティ データベースに存在している必要があります。これによりコア スイッチのポートで通信やリンクが許可されます。
  - すべてのエンド デバイスの pWWN もポート セキュリティ データベースに存在する必要があります。
- エッジ スイッチは複数のコア スイッチに接続できます。つまり、異なる NP ポートを異なるコア スイッチに接続できます。
- NPV は初回ログイン時にロード バランシング アルゴリズムを使用して、自動的に VSAN 内のエンド デバイスを NP アップリンクの 1 つ（同じ VSAN 内）に割り当てます。同じ VSAN に複数の NP アップリンクがある場合は、エンド デバイスを特定の NP アップリンクに割り当てることはできません。
- サーバ インターフェイスがダウンしてから使用可能状態に戻った場合、インターフェイスは同じ NP アップリンクに割り当てられるとはかぎりません。
- 割り当てられた NP アップリンクが動作可能になると、サーバ インターフェイスだけが使用できます。
- NPV モードならば、サーバとターゲットの両方をスイッチに接続できます。
- ファイバ チャネル スイッチングは、エッジ スイッチで実行されません。すべてのトラフィックはコア スイッチでスイッチングされます。
- NPV は NPIV 対応サーバをサポートします。この機能は階層型 NPIV と呼ばれます。
- 2 台の Cisco NPV スイッチを互いに接続する構成はサポートされていません。
- NPV モードでは F、NP、および SD ポートだけがサポートされます。

NPV の設定

ここでは、NPV モードの設定ついて説明します。具体的な内容は次のとおりです。

- NPV のイネーブル化（34-7 ページ）
- NPV インターフェイスの設定（34-7 ページ）
- NPV トラフィック管理の設定（34-8 ページ）

NPV のイネーブル化

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

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

NPV をイネーブルにする手順は、次のとおりです。

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

NPV インターフェイスの設定

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

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

サーバ インターフェイスを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface {fc slot/port | vfc vfc-id}`	サーバ インターフェイスを選択します。

	コマンド	目的
ステップ 3	`switch(config-if)# switchport mode F` `switch(config-if)# no shutdown`	このインターフェイスを F ポートとして設定します。 インターフェイスをアップにします。

NPV トラフィック管理の設定

インターフェイスを NPV モードに設定すると、NPV トラフィック管理を設定できます。

この項では、次のトピックについて取り上げます。

- NPV トラフィック マップの設定（34-8 ページ）
- ディスラプティブ ロード バランシングのイネーブル化（34-9 ページ）

NPV トラフィック マップの設定

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

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

トラフィック マップを設定する手順は、次のとおりです。

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

（注）トラフィック マップの設定は、マップで指定された各サーバ インターフェイスを再初期化した後でだけ有効になります。

ディスラプティブ ロード バランシングのイネーブル化

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

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

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

（注） ディスラプティブ ロード バランシングをイネーブルにすると、1 つ以上ののサーバ インターフェイスが強制的に再初期化されることがあります。このアクションにより、接続されたデバイスのトラフィックが中断されます。

NPV の確認

NPV に関する情報を表示する手順は、次のとおりです。

コマンド	目的
`switch#` **`show npv flogi-table`** `[all]`	NPV 設定を表示します。

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

```
switch# show npv flogi-table
--------------------------------------------------------------------------------
SERVER                                                                  EXTERNAL
INTERFACE VSAN FCID             PORT NAME               NODE NAME       INTERFACE
--------------------------------------------------------------------------------
vfc3/1    1    0xee0008 10:00:00:00:c9:60:e4:9a 20:00:00:00:c9:60:e4:9a fc2/1
vfc3/1    1    0xee0009 20:00:00:00:0a:00:00:01 20:00:00:00:c9:60:e4:9a fc2/2
vfc3/1    1    0xee000a 20:00:00:00:0a:00:00:02 20:00:00:00:c9:60:e4:9a fc2/3
vfc3/1    1    0xee000b 33:33:33:33:33:33:33:33 20:00:00:00:c9:60:e4:9a fc2/4

Total number of flogi = 4
```

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

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

```
switch# show npv status
npiv is enabled

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

  Number of External Interfaces: 4

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

  Number of Server Interfaces: 1
```

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

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

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

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

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

NPV トラフィック管理の確認

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

```
NPV Traffic Map Information:
----------------------------------------
Server-If       External-If(s)
----------------------------------------
fc1/3           fc1/10,fc1/11
fc1/5           fc1/1,fc1/2
----------------------------------------
```

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

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

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

CHAPTER 35

VSAN トランキングの設定

この章では、Cisco Nexus 5000 シリーズ スイッチが提供する VSAN トランキング機能について説明します。

この章は、次の項で構成されています。

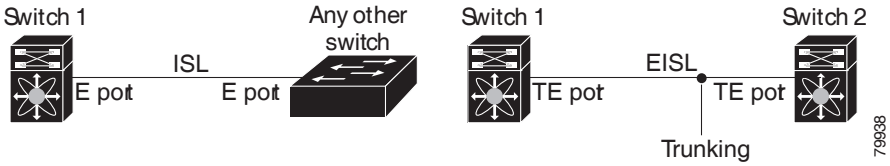
- VSAN トランキングの概要(35-1 ページ)
- VSAN トランキングの設定(35-3 ページ)
- VSAN トランキング情報の表示(35-7 ページ)
- デフォルト設定(35-7 ページ)

VSAN トランキングの概要

VSAN トランキングにより、相互接続したポートが Enhanced ISL(EISL)フレーム フォーマットを使用して同一物理リンク上の 2 つ以上の VSAN(仮想 SAN)でフレームを送受信することができます(図 35-1 を参照)。

VSAN トランキングは、仮想ファイバ チャネル インターフェイスではなく、ネイティブ ファイバ チャネル インターフェイスでサポートされます。

図 35-1　VSAN トランキング



VSAN トランキング機能には、次の制限事項があります。

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

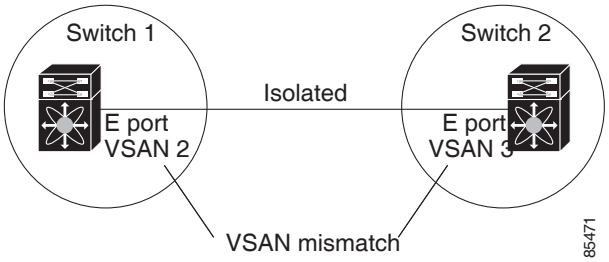
VSAN トランキングに関する追加情報については、次で説明します。

- VSAN トランキングの不一致（35-2 ページ）
- VSAN トランキング プロトコル（35-2 ページ）

VSAN トランキングの不一致

E ポート間で VSAN が正しく設定されなかった場合、2 つの VSAN でトラフィックが結合される（その結果、2 つの VSAN が一致しなくなる）などの問題が発生します。VSAN トランキング プロトコルは、VSAN インターフェイスを ISL の両端で検証し、VSAN の結合を防ぎます（図 35-2 を参照）。

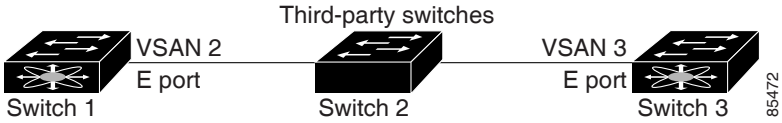
図 35-2　VSAN の不一致



この例では、トランキング プロトコルは発生する可能性のある VSAN の結合を検出し、関係しているポートを分離します。

2 台の Cisco Nexus 5000 シリーズ スイッチ間にサードパーティ製のスイッチが配置された場合、トランキング プロトコルは VSAN の結合を検出できません（図 35-3 を参照）。

図 35-3　サードパーティ製スイッチによる VSAN の不一致



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

VSAN トランキング プロトコル

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

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

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

VSAN トランキングの設定

ここでは、VSAN トランキングの設定方法および次の内容について説明します。

- 注意事項および制約事項（35-3 ページ）
- VSAN トランキング プロトコルのイネーブル化/ディセーブル化（35-3 ページ）
- トランク モードについて（35-4 ページ）
- トランク モードの設定（35-4 ページ）
- トランク許可 VSAN リストについて（35-5 ページ）
- VSAN の allowed-active リストの設定（35-6 ページ）

注意事項および制約事項

VSAN トランキングを設定する場合、次の点に注意してください。

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

VSAN トランキング プロトコルのイネーブル化/ディセーブル化

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

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

トランク モードについて

デフォルトでは、トランク モードは、すべてのファイバ チャネル インターフェイスでイネーブルです。ただし、トランク モード設定は E ポート モードでしか有効になりません。トランク モードを on（イネーブル）、off（ディセーブル）、または auto（自動）に設定できます。デフォルトのトランク モードは on です。リンクの両端のトランク モード設定によって、両端のリンクおよびポート モードのトランキング ステートが決まります（表 35-1 を参照）。

表 35-1　スイッチ間のトランク モード ステータス

トランク モードの設定		最終的なステートとポート モード	
スイッチ 1	**スイッチ 2**	**トランキング ステート**	**ポート モード**
オン	auto または on	トランキング（EISL）	TE ポート
消灯	auto、on、または off	トランキングなし（ISL）	E ポート
自動	auto	トランキングなし（ISL）	E ポート

ヒント　Cisco Nexus 5000 シリーズ スイッチでの推奨コンフィギュレーションは、トランクの一方が auto、反対側が on 設定です。

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

トランク モードの設定

トランク モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface fc slot/port` `switch(config-if)#`	指定されたインターフェイスを設定します。
ステップ 3	`switch(config-if)# switchport trunk mode on`	指定されたインターフェイスのトランク モードをイネーブルにします（デフォルト）。
	`switch(config-if)# switchport trunk mode off`	指定されたインターフェイスのトランク モードをディセーブルにします。
	`switch(config-if)# switchport trunk mode auto`	インターフェイスの自動検知を提供するトランク モードを **auto** モードに設定します。

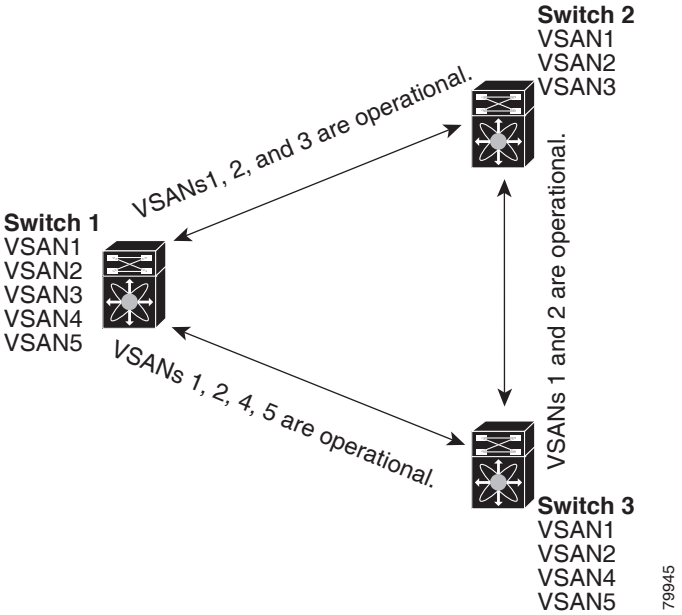
トランク許可 VSAN リストについて

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

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

図 35-4 では、トランク許可 VSAN のデフォルトでスイッチ 1 は VSAN 1 ～ 5、スイッチ 2 は VSAN 1 ～ 3、スイッチ 3 は VSAN 1、2、4、および 5 が設定されています。3 つすべてのスイッチに設定された VSAN はすべて、allowed-active です。ただし、図 35-4 に示すように、ISL の両端における allowed-active VSAN の共通のセットだけが通信可能になります。

図 35-4　allowed-active VSAN のデフォルト設定



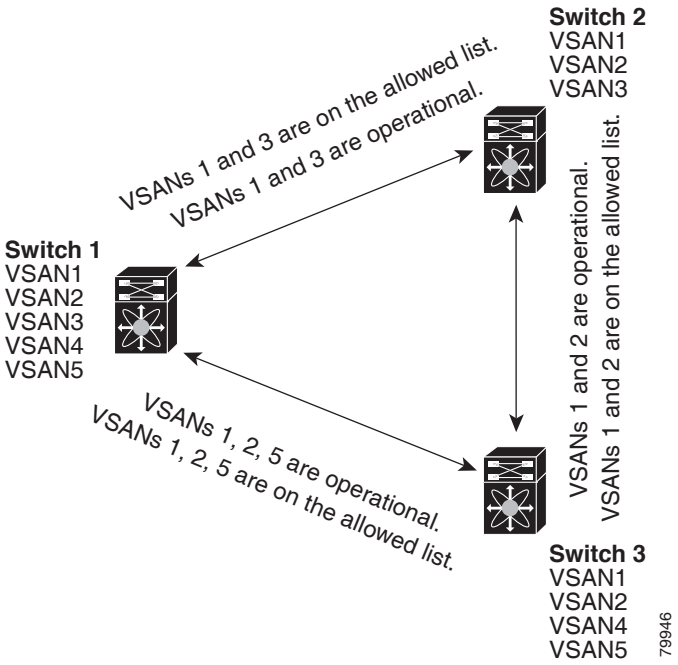
allowed-active リストから選択した VSAN セットを設定して、トランキング ISL に指定された VSAN へのアクセスを制御できます。

例として 図 35-4 を使用して、インターフェイスごとに許可 VSAN リストを設定できます（図 35-5 を参照）。たとえば、スイッチ 1 に接続された ISL の許可 VSAN リストから VSAN 2 と VSAN 4 を削除する場合、各 ISL の通信可能な VSAN リストは次のようになります。

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

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

図 35-5　　通信可能な許可 VSAN の設定



VSAN の allowed-active リストの設定

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

	コマンド	目的
ステップ 1	`switch#` **`configuration terminal`**	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`interface fc`** *`slot/port`* `switch(config-if)#`	指定されたインターフェイスを設定します。
ステップ 3	`switch(config-if)#` **`switchport trunk allowed vsan`** *`vsan-id`* **`-`** *`vsan-id`*	指定された VSAN 範囲の許可リストを変更します。
	`switch(config-if)#` **`switchport trunk allowed vsan add`** *`vsan-id`* `updated trunking membership`	指定された VSAN を新しい許可リストに追加します。
	`switch(config-if)#` **`no switchport trunk allowed vsan`** *`vsan-id`* **`-`** *`vsan-id`*	指定された VSAN 範囲を削除します。
	`switch(config-if)#` **`no switchport trunk allowed vsan add`** *`vsan-id`*	追加された許可リストを削除します。

VSAN トランキング情報の表示

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

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

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

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

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

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

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

デフォルト設定

表 35-2 に、トランキング パラメータのデフォルト設定値を示します。

表 35-2　デフォルト トランク設定パラメータ

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

CHAPTER 36

SAN ポート チャネルの設定

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

Cisco Nexus 5000 シリーズ スイッチでは、SAN ポート チャネルは物理ファイバ チャネル インターフェイスを含むことがありますが、仮想ファイバ チャネル インターフェイスを含みません。SAN ポート チャネルには、最大 8 つのファイバ チャネル インターフェイスを含むことができます。

この章では、スイッチで利用できる SAN ポート チャネル機能について説明します。この章の内容は、次のとおりです。

- SAN ポート チャネルに関する情報（36-1 ページ）
- SAN ポート チャネルの設定（36-4 ページ）
- SAN ポート チャネルのインターフェイス（36-9 ページ）
- ポート チャネル プロトコル（36-12 ページ）
- SAN ポート チャネル設定の確認（36-16 ページ）
- デフォルト設定（36-17 ページ）

SAN ポート チャネルに関する情報

SAN ポート チャネルには、次の機能があります。

- ISL（スイッチ間リンク）（E ポート）または EISL（TE ポート）を介してポイントツーポイントで接続できます。複数のリンクを SAN ポート チャネルに結合できます。
- チャネル内で機能するすべてのリンクにトラフィックを分配して、ISL 上の集約帯域幅を増加させます。
- 複数のリンク間で負荷を分散し、最適な帯域利用率を維持します。ロード バランシングは、送信元 ID、宛先 ID、Originator Exchange ID（OX ID）に基づきます。
- ISL にハイ アベイラビリティを提供します。いずれか 1 つのリンクに障害が発生したら、それまでそのリンクで伝送されていたトラフィックが残りのリンクに切り替えられます。SAN ポート チャネルでリンクが 1 つダウンしても、上位層プロトコル（ULP）はそのことを認識しません。ULP から見れば、帯域幅は減っていても引き続きリンクが存在しています。リンク障害によるルーティング テーブルへの影響はありません。

Cisco Nexus 5000 シリーズ スイッチでは、最大 4 つの SAN ポート チャネル（ポート チャネルあたり 8 つのインターフェイス）をサポートします。ポート チャネル番号は、各チャネル グループに関連付けられた（スイッチごとに）一意の識別番号です。この番号の範囲は 1 ～ 256 です。

ここでは SAN について説明します。具体的な内容は次のとおりです。

- ポート チャネルと VSAN トランキングの概要（36-2 ページ）
- ロード バランシングの概要（36-3 ページ）

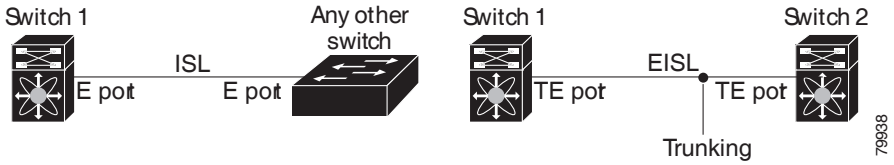
ポート チャネルと VSAN トランキングの概要

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

- SAN ポート チャネルでは、複数の物理リンクを 1 つの集約論理リンクに結合できます。
- 業界標準の E ポートは、他のベンダー スイッチにリンクでき、スイッチ間リンク（ISL）と呼ばれます（図 36-1 の左側を参照）。
- VSAN トランキングを使用すると、複数の VSAN のトラフィックを伝送する EISL 形式でのフレーム伝送が可能になります。トランキングが E ポートで動作可能な場合、その E ポートは TE ポートになります。EISL はシスコ スイッチ間でだけ接続されます（図 36-1 の右側を参照）。

トランク インターフェイスの詳細については、第35 章「VSAN トランキングの設定」を参照してください。

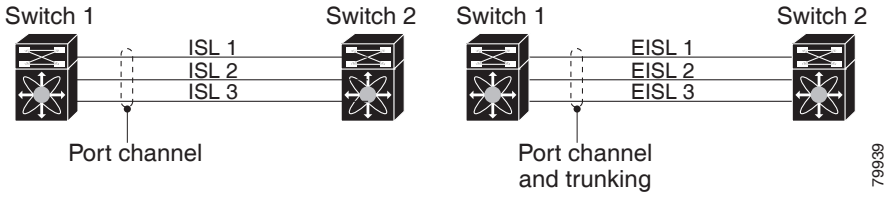
図 36-1　　VSAN トランキングのみ



E ポートであるメンバで SAN ポート チャネルを作成できます（図 36-2 の左側を参照）。この設定では、ポート チャネルは論理 ISL（1 つの VSAN のトラフィックを伝送する）を実装します。

TE ポートであるメンバで SAN ポート チャネルを作成できます（図 36-2 の右側を参照）。この設定では、ポート チャネルは論理 EISL（複数の VSAN のトラフィックを伝送する）を実装します。

図 36-2　　ポート チャネルと VSAN トランキング



ロード バランシングの概要

ロード バランシング機能は、次の方式を使用して提供できます。

- フロー ベース：送信元と宛先間のすべてのフレームが所定のフローで同一のリンクをたどります。つまり、フローの最初のエクスチェンジで選択されたリンクが、後続のすべてのエクスチェンジで使用されます。
- エクスチェンジ ベース：エクスチェンジの最初のフレームがリンクに割り当てられ、エクスチェンジの後続のフレームが同一のリンクをたどります。ただし、後続のエクスチェンジは、別のリンクを使用できます。この方式によって、より精度の高いロード バランシングが可能になり、さらに各エクスチェンジでのフレームの順序が維持されます。

図 36-3 に、フロー ベースのロード バランシングがどのように機能するかを示します。フローの最初のフレームが転送のためにインターフェイスで受信されると、リンク 1 が選択されます。そのフローの各後続のフレームが、同一のリンク上に送信されます。SID1 および DID1 のフレームは、リンク 2 を使用しません。

図 36-3　SID1、DID1、およびフロー ベースのロード バランシング

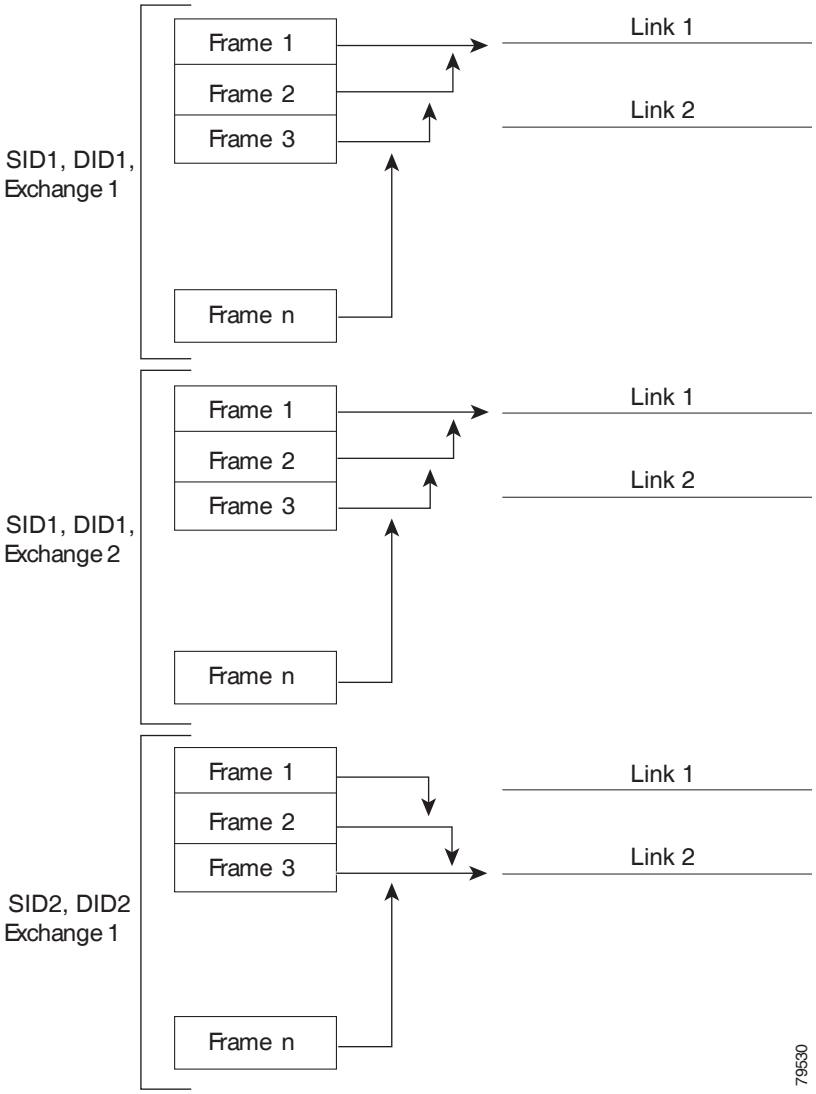
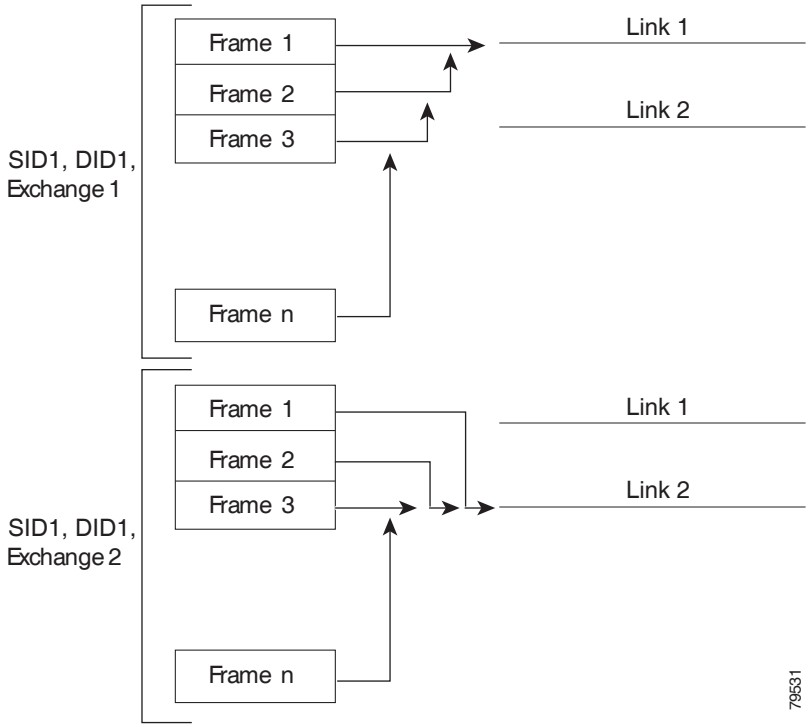


図 36-4 に、エクスチェンジ ベースのロード バランシングがどのように機能するかを示します。エクスチェンジで最初のフレームが転送用にインターフェイスで受信されると、リンク 1 がハッシュ アルゴリズムによって選択されます。その特定のエクスチェンジにある残りすべてのフレームが同一のリンクに送信されます。エクスチェンジ 1 では、リンク 2 を使用するフレームはありません。次のエクスチェンジでは、ハッシュ アルゴリズムによってリンク 2 が選択されます。ここではエクスチェンジ 2 のすべてのフレームが、リンク 2 を使用します。

図 36-4　SID1、DID1、およびエクスチェンジ ベースのロード バランシング



SAN ポート チャネルの設定

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

図 36-5 に、有効な SAN ポート チャネルの設定例を示します。

図 36-5　有効な SAN ポート チャネルの設定

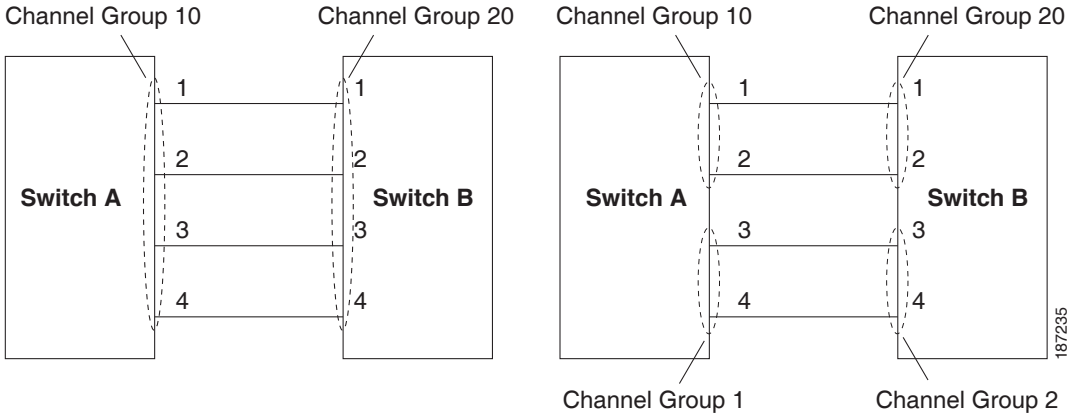
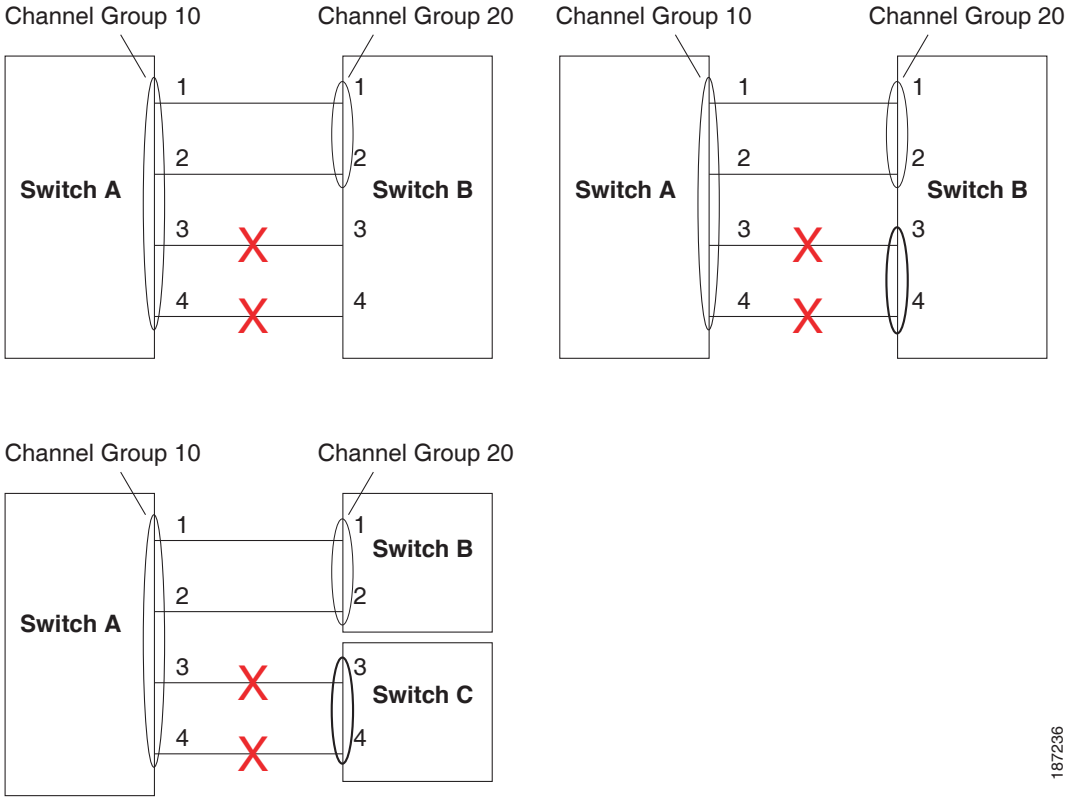


図 36-6 に、無効な設定例を示します。リンクが 1、2、3、4 の順番でアップした場合、ファブリックの設定が誤っているため、リンク 3 および 4 は動作上ダウンします。

図 36-6　誤った設定



ここでは、SAN ポート チャネルの設定と修正方法について説明します。具体的な内容は次のとおりです。

- SAN ポート チャネルの設定時の注意事項（36-6 ページ）
- SAN ポート チャネルの作成（36-6 ページ）
- SAN ポート チャネル モードについて（36-7 ページ）
- SAN ポート チャネルの削除について（36-8 ページ）
- SAN ポート チャネルの削除（36-8 ページ）

SAN ポート チャネルの設定時の注意事項

SAN ポート チャネルを設定する前に、次の注意事項を守ってください。

- 両方の拡張モジュールからファイバ チャネル ポートを使用して SAN ポート チャネルを設定し、アベイラビリティを向上させます（いずれかの拡張モジュールが故障した場合）。
- 1 つの SAN ポート チャネルが異なるスイッチ群に接続されないようにします。SAN ポート チャネルでは、同一のスイッチ群内でのポイントツーポイント接続が必要です。

SAN ポート チャネルを誤って設定すると、誤設定メッセージを受け取る場合があります。このメッセージを受け取った場合、エラーが検出されてポート チャネルの物理リンクはディセーブルになります。

次の要件を満たしていない場合に、SAN ポート チャネルのエラーが検出されます。

- SAN ポート チャネルの両側のスイッチが、同じ数のインターフェイスに接続されている必要があります。
- 各インターフェイスは、対応する反対側のインターフェイスに接続される必要があります（無効な設定例については、図 36-6 を参照してください）。
- ポート チャネルを設定したあとで、SAN ポート チャネルのリンクを変更できません。ポート チャネルを設定したあとにリンクを変更する場合は、必ずそのポート チャネル内でリンクをインターフェイスに再接続し、再度イネーブルにしてください。

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

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

SAN ポート チャネルの作成

SAN ポート チャネルを作成する手順は、次のとおりです。

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

次の例では、SAN ポート チャネルを作成します。

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

SAN ポート チャネル モードについて

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

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

表 36-1 は、2 つのモードの比較表です。

表 36-1　チャネル グループ設定の相違点

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

アクティブ モードを設定する手順は、次のとおりです。

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

アクティブ モードを設定する手順は、次のとおりです。

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

SAN ポート チャネルの削除について

SAN ポート チャネルを削除すると、関連するチャネル メンバーシップも削除されます。削除された SAN ポート チャネルのすべてのインターフェイスは、個々の物理リンクに変換されます。SAN ポート チャネルを削除すると、使用されているモード（アクティブおよびオン）に関係なく、各端のポートが正常にシャットダウンされます。これは、インターフェイスのシャットダウン時にフレームが失われないことを意味します（「管理ステートの設定インターフェイスの管理ステートの設定」セクション（32-9 ページ）を参照）。

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

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

SAN ポート チャネルの削除

SAN ポート チャネルを削除する手順は、次のとおりです。

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

次に、SAN ポート チャネルを削除する例を示します。

```
switch(config)# no interface san-port-channel 1
san-port-channel 1 deleted and all its members disabled
please do the same operation on the switch at the other end of the san-port-channel
```

SAN ポート チャネルのインターフェイス

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

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

ここでは SAN ポート チャネルのインターフェイス設定について説明します。具体的な内容は次のとおりです。

- SAN ポート チャネルへのインターフェイスの追加について（36-9 ページ）
- SAN ポート チャネルへのインターフェイスの追加（36-10 ページ）
- インターフェイスの強制追加（36-10 ページ）
- SAN ポート チャネルからのインターフェイスの削除について（36-11 ページ）
- SAN ポート チャネルからのインターフェイスの削除（36-11 ページ）

SAN ポート チャネルへのインターフェイスの追加について

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

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

互換性チェック

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

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

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

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

中断および隔離ステート

動作パラメータに互換性がない場合、互換性チェックは失敗し、インターフェイスは設定されたモードに基づいて中断状態または隔離状態になります。

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

「理由コード」セクション（32-6 ページ）を参照してください。

SAN ポート チャネルへのインターフェイスの追加

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

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

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

```
switch(config)# interface fc2/3
switch(config-if)# channel-group 15
fc2/3 added to san-port-channel 15 and disabled
please do the same operation on the switch at the other end of the san-port-channel, then
do "no shutdown" at both ends to bring them up
```

インターフェイスの強制追加

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

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

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

メンバを強制的に追加すると、使用されているモード（アクティブおよびオン）に関係なく、各端のポートが正常にシャットダウンされます。これは、インターフェイスのシャットダウン時にフレームが失われないことを意味します（「管理ステートの設定インターフェイスの管理ステートの設定」セクション（32-9 ページ）を参照）。

SAN ポート チャネルへポートを強制的に追加する手順は、次のとおりです。

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

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

```
switch(config)# interface fc2/3
switch(config-if)# channel-group 15 force
fc2/3 added to san-port-channel 15 and disabled
please do the same operation on the switch at the other end of the san-port-channel, then
do "no shutdown" at both ends to bring them up
```

SAN ポート チャネルからのインターフェイスの削除について

物理インターフェイスが SAN ポート チャネルから削除された場合は、チャネル メンバーシップが自動更新されます。削除されたインターフェイスが最後の動作可能なインターフェイスである場合は、ポート チャネルのステータスは、down ステートに変更されます。SAN ポート チャネルからインターフェイスを削除すると、SAN ポート チャネルのチャネル サイズと帯域幅が減少します。

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

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

SAN ポート チャネルからのインターフェイスの削除

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

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

SAN ポート チャネルからインターフェイスを削除する手順は、次のとおりです。

```
switch(config)# interface fc2/3
switch(config-if)# no channel-group 15
fc2/1 removed from san-port-channel 2 and disabled.Please do the same operation on the
switch at the other end of the san-port-channel
```

ポート チャネル プロトコル

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

ポート チャネルの設定を交換するプロトコルが Cisco SAN スイッチで使用できます。これにより、互換性のない ISL でのポート チャネル管理が簡素化されます。追加された自動作成モードでは、互換性のあるパラメータを持つ ISL でチャネル グループを自動的に作成でき、手動での作業は必要ありません。

デフォルトではポート チャネル プロトコルがイネーブルになっています。

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

ポート チャネル プロトコルは、次の 2 つのサブプロトコルを使用します。

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

ここでは、ポート チャネル プロトコルの設定方法について説明します。具体的な内容は次のとおりです。

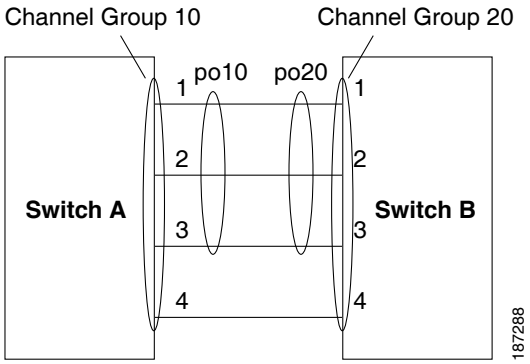
- チャネル グループの作成について（36-13 ページ）
- 自動作成の注意事項（36-14 ページ）
- 自動作成のイネーブル化および設定（36-15 ページ）
- 手動設定チャネル グループの概要（36-15 ページ）
- 手動設定チャネル グループへの変更（36-15 ページ）

チャネル グループの作成について

チャネル グループの自動作成がイネーブルの場合、ISL は手動介入なしにチャネル グループに自動的に設定できます。図 36-7 に、チャネル グループの自動作成例を示します。

最初の ISL は個別リンクとしてアップします。図 36-7 の例では、これはリンク A1-B1 です。次のリンク（たとえば A2-B2）がアップすると、ポート チャネル プロトコルは、このリンクがリンク A1-B1 と互換性があるかどうかを識別し、それぞれのスイッチでチャネル グループ 10 および 20 を自動的に作成します。それぞれのポートの設定に互換性がある場合、リンク A3-B3 はチャネル グループ（およびポート チャネル）に参加できます。リンク A4-B4 はチャネル グループ内の既存のメンバ ポートと互換性がないため、個別のリンクとして動作します。

図 36-7　　チャネル グループの自動作成



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

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

表 36-2 に、ユーザ設定のチャネル グループと自動設定のチャネル グループの相違点を示します。

表 36-2　　チャネル グループ設定の相違点

ユーザ設定のチャネル グループ	自動設定のチャネル グループ
ユーザが手動で設定します。	2 つの互換性のあるスイッチ間で互換性のあるリンクがアップしたときに自動的に作成されます（両端のすべてのポートでチャネル グループの自動作成がイネーブルになっている場合）。
メンバ ポートはチャネル グループの自動作成には参加できません。自動作成機能は設定できません。	これらのポートは、ユーザ設定のチャネル グループのメンバにはなりません。
チャネル グループのポートの一部を使用して SAN ポート チャネルを作成できます。オン モードまたはアクティブ モードの設定に応じて、互換性のないポートは中断ステートまたは隔離ステートのままになります。	チャネル グループに含まれるすべてのポートが SAN ポート チャネルに参加します。いずれのメンバ ポートも隔離ステートまたは中断ステートになりません。その代わりに、リンクに互換性がない場合、メンバ ポートはチャネル グループから削除されます。

表 36-2　チャネル グループ設定の相違点（続き）

ユーザ設定のチャネル グループ	自動設定のチャネル グループ
SAN ポート チャネルに対する管理設定は、チャネル グループのすべてのポートに適用され、ポート チャネル インターフェイスの設定は保存できます。	SAN ポート チャネルに対する管理設定は、チャネル グループのすべてのポートに適用され、メンバ ポートの設定は保存されますが、ポート チャネル インターフェイスの設定は保存されません。このチャネル グループは、必要に応じて明示的に変更できます。
任意のチャネル グループの削除およびチャネル グループへのメンバの追加が可能です。	チャネルグループは削除できません。チャネル グループのメンバの追加および削除はできません。メンバ ポートが存在しない場合、チャネル グループは削除されます。

自動作成の注意事項

自動作成プロトコルを使用する場合、次の注意事項に従ってください。

- 自動作成機能がイネーブルの場合、ポートを SAN ポート チャネルの一部として設定できません。これらの 2 つの設定を同時に使用できません。
- 自動作成は、SAN ポート チャネルのネゴシエーションを行うローカル ポートとピア ポートの両方でイネーブルにする必要があります。
- 集約は、次の 2 通りの方法で実行されます。
  - ポートを互換性のある自動作成 SAN ポート チャネルへ集約する。
  - ポートを互換性のある別のポートと集約して新しい SAN ポート チャネルを構成する。
- 新しく作成される SAN ポート チャネルには、最大利用可能ポート チャネルからアベイラビリティに基づいて番号が降順に割り当てられます。すべてのポート チャネル番号を使い切ると、集約は許可されなくなります。
- メンバーシップの変更または自動作成された SAN ポート チャネルの削除はできません。
- 自動作成をディセーブルにすると、メンバ ポートはすべて自動作成された SAN ポート チャネルから削除されます。
- 自動作成された SAN ポート チャネルからすべてのメンバが削除されると、チャネルは自動的に削除され、チャネル番号は再利用できるように解放されます。
- 自動作成された SAN ポート チャネルは、再起動後は存在しません。自動作成された SAN ポート チャネルを手動で設定すると、再起動後も維持できます。SAN ポート チャネルを手動で設定すると、自動作成機能はすべてのメンバ ポートでディセーブルになります。
- 自動作成機能は、ポート単位またはスイッチ内のすべてのポートに対して、イネーブルまたはディセーブルに設定できます。この設定がイネーブルの場合、チャネル グループ モードはアクティブと見なされます。このタスクのデフォルトはディセーブルです。
- インターフェイスに対してチャネル グループの自動作成がイネーブルになっている場合、最初に自動作成をディセーブルにしてから、以前のソフトウェア バージョンにダウングレードするか、または手動設定されたチャネル グループでインターフェイスを設定する必要があります。

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

自動作成のイネーブル化および設定

自動チャネル グループを設定する手順は、次のとおりです。

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

次に、自動チャネル グループを設定する例を示します。

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

手動設定チャネル グループの概要

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

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

手動設定チャネル グループへの変更

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

SAN ポート チャネル設定の確認

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

show san-port-channel summary コマンドを実行すると、スイッチ内の SAN ポート チャネルの概要が表示されます。各 SAN ポート チャネルの 1 行ずつの概要には、管理ステート、動作可能ステート、接続されてアクティブな状態（アップ）のインターフェイスの数、コントロールプレーン トラフィック（ロード バランシングなし）を伝送するために SAN ポート チャネルで選択された主要な動作可能インターフェイスである First Operational Port（FOP）を表示します。FOP は SAN ポート チャネルで最初にアップするポートで、このポートがダウンした場合は変わることがあります。FOP はアスタリスク（*）でも識別できます。

VSAN の設定情報を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
switch# **show san-port-channel summary** | **database** | **consistency** [**details**] | **usage** | **compatibility-parameters**	SAN ポート チャネルの情報を表示します。
switch# **show san-port-channel database interface san-port-channel** *channel-number*	指定された SAN ポート チャネルの情報を表示します。
switch# **show interface fc** *slot/port*	指定されたファイバ チャネル インターフェイスの VSAN 設定情報を表示します。

次に、SAN ポート チャネル情報の概要を表示する例を示します。

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

次に、SAN ポート チャネルの一貫性を表示する例を示します。

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

次に、使用および未使用ポート チャネル番号の詳細を表示する例を示します。

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

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

```
switch# show interface fc2/1
fc2/1 is trunking
    Hardware is Fibre Channel, FCOT is short wave laser
    Port WWN is 20:0a:00:0b:5f:3b:fe:80
    ...
```

```
    Receive data field Size is 2112
    Beacon is turned off
  Port-channel auto creation is enabled
    Belongs to port-channel 123
...
```

デフォルト設定

表 36-3 に、SAN ポート チャネルのデフォルト設定値を示します。

表 36-3　デフォルト SAN ポート チャネル パラメータ

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

CHAPTER 37

VSAN の設定と管理

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

- VSAN に関する情報（37-1 ページ）
- VSAN の設定（37-5 ページ）
- スタティック VSAN 設定の表示（37-11 ページ）
- デフォルト設定（37-12 ページ）

VSAN に関する情報

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

ここでは VSAN について説明します。具体的な内容は次のとおりです。

- VSAN トポロジ（37-1 ページ）
- VSAN の利点（37-4 ページ）
- VSAN とゾーン（37-4 ページ）

VSAN トポロジ

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

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

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

図 37-1 に、3 つのスイッチによるファブリック（各階にスイッチは 1 つ）を示します。スイッチと接続された装置の地理的な配置は、論理 VSAN の区分けには依存しません。VSAN 間では通信できません。各 VSAN 内では、すべてのメンバが相互に対話できます。

図 37-1　論理 VSAN の区分け

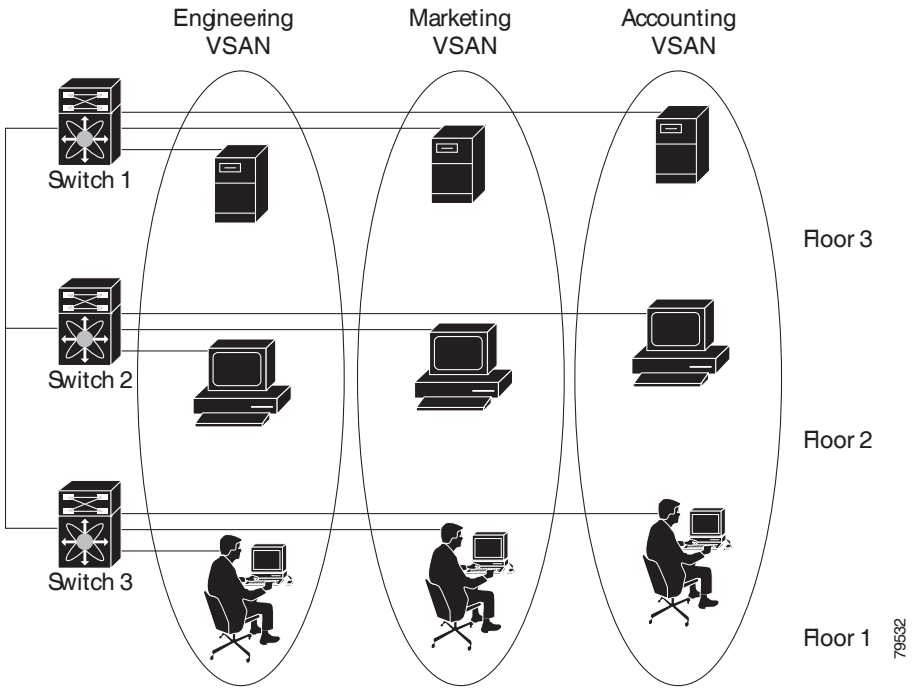
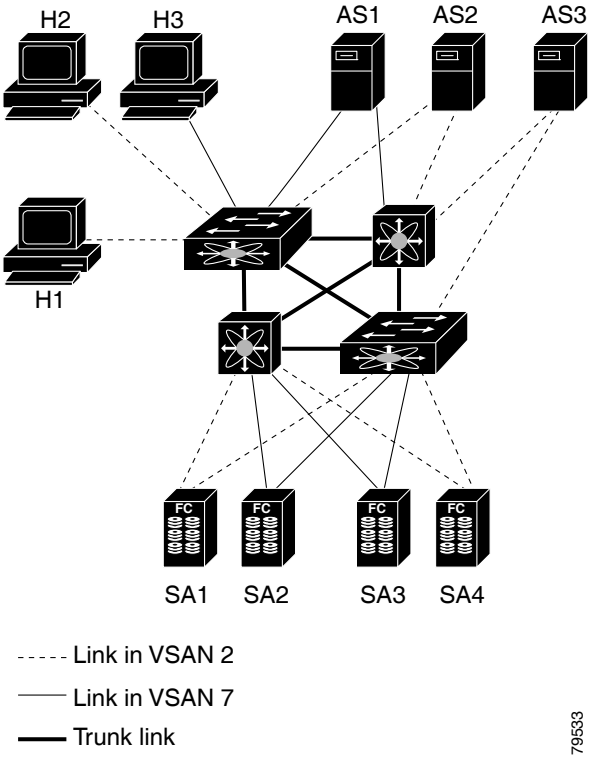


図 37-2 に、VSAN 2（破線）と VSAN 7（実線）の 2 つの定義済み VSAN からなるファイバ チャネル スイッチングの物理インフラストラクチャを示します。VSAN 2 には、ホスト H1 と H2、アプリケーション サーバ AS2 と AS3、ストレージ アレイ SA1 と SA4 が含まれます。VSAN 7 は、H3、AS1、SA2、および SA3 と接続します。

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

図 37-2　　2 つの VSAN の例



このネットワークにある 4 つのスイッチは、VSAN 2 トラフィックおよび VSAN 7 トラフィックを伝送する VSAN トランク リンクによって相互接続されています。各 VSAN に異なるスイッチ間トポロジを設定できます。図 37-2 では、VSAN 2 と VSAN 7 のスイッチ間トポロジは同じです。

VSAN がもしなければ、SAN ごとに別個のスイッチとリンクが必要です。VSAN をイネーブルにすることによって、同一のスイッチとリンクが複数の VSAN で共有されることがあります。VSAN では、スイッチ精度ではなく、ポート精度で SAN を作成できます。図 37-2 は、VSAN が物理 SAN で定義された仮想トポロジを使用して相互に通信するホストまたはストレージ デバイスのグループであることを表しています。

このようなグループを作成する基準は、VSAN トポロジによって異なります。

- VSAN は、次の条件に基づいてトラフィックを分離できます。
  - ストレージ プロバイダー データセンター内の異なるお客様
  - 企業ネットワークの業務またはテスト
  - ロー セキュリティおよびハイ セキュリティの要件
  - 別個の VSAN によるバックアップ トラフィック
  - ユーザ トラフィックからのデータの複製
- VSAN は、特定の部門またはアプリケーションのニーズを満たせます。

VSAN の利点

VSAN には、次のような利点があります。

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

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

VSAN とゾーン

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

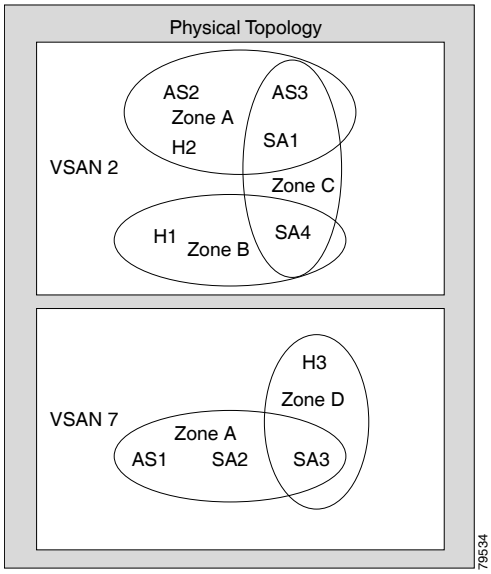
2 つの VSAN は未接続の 2 つの SAN に相当するので、VSAN 1 のゾーン A は、VSAN 2 のゾーン A とは異なる、別個のものです。表 37-1 に、VSAN とゾーンの相違点を示します。

表 37-1　VSAN とゾーンの比較

VSAN 特性	ゾーン特性
VSAN は、SAN とルーティング、ネーミング、およびゾーン分割プロトコルが同じです。	ルーティング、ネーミング、およびゾーニング プロトコルは、ゾーン単位で利用できません。
VSAN は、ユニキャスト、マルチキャスト、およびブロードキャスト トラフィックを制限します。	ゾーンは、ユニキャスト トラフィックを制限します。
メンバーシップは、一般的に VSAN ID を使用して F ポートに定義されます。	メンバーシップは、通常 pWWN によって定義されます。
HBA またはストレージ デバイスは、1 つの VSAN（F ポートに対応付けられた VSAN）だけに所属できます。	HBA またはストレージ デバイスは、複数のゾーンに所属できます。
VSAN は、各 E ポート、送信元ポート、および宛先ポートでメンバーシップを実行します。	ゾーンは、送信元ポートおよび宛先ポートだけでメンバーシップを実行します。
VSAN は、規模が大きい環境（ストレージ サービス プロバイダー）で定義されます。	ゾーンは、ゾーンの外部に表示されないイニシエータおよびターゲットのセットで定義されます。
VSAN は、ファブリック全体を網羅します。	ゾーンは、ファブリック エッジで設定されます。

図 37-3 に、VSAN とゾーンとの可能な組み合わせを示します。VSAN 2 には、ゾーン A、ゾーン B、およびゾーン C という 3 つのゾーンが定義されています。ゾーン C は、ファイバ チャネル標準規格に従ってゾーン A とゾーン B の両方にオーバーラップしています。VSAN 7 には、ゾーン A とゾーン D という 2 つのゾーンが定義されています。VSAN の境界を越えるゾーンはありません。VSAN 2 に定義されたゾーン A は、VSAN 7 に定義されたゾーン A とは別個のものです。

図 37-3　　VSAN とゾーン分割



VSAN の設定

VSAN には、次の属性があります。

- VSAN ID：VSAN ID は、デフォルト VSAN（VSAN 1）、ユーザ定義の VSAN（VSAN 2 ～ 4093）、および独立 VSAN（VSAN 4094）で VSAN を識別します。
- ステート：VSAN の管理ステートを active（デフォルト）または suspended ステートに設定できます。VSAN が作成されると、VSAN はさまざまな状態またはステートに置かれます。
  - VSAN の active ステートは、VSAN が設定されイネーブルであることを示します。VSAN をイネーブルにすることによって、VSAN のサービスをアクティブにします。
  - VSAN の suspended ステートは、VSAN が設定されているがイネーブルではないことを示します。この VSAN にポートが設定されている場合、ポートはディセーブルの状態です。このステートを使用して、VSAN の設定を失うことなく VSAN を非アクティブにします。suspended ステートの VSAN のすべてのポートは、ディセーブルの状態です。VSAN を suspended ステートにすることによって、ファブリック全体のすべての VSAN パラメータを事前設定し、VSAN をただちにアクティブにできます。
- VSAN 名：このテキスト ストリングは、管理目的で VSAN を識別します。名前は、1 ～ 32 文字で指定できます。また、すべての VSAN で一意である必要があります。デフォルトでは、VSAN 名は VSAN と VSAN ID を表す 4 桁のストリングを連結したものです。たとえば、VSAN 3 のデフォルト名は VSAN0003 です。

（注）　VSAN 名は一意である必要があります。

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

ここでは、VSAN の作成および設定方法について説明します。具体的な内容は次のとおりです。

- VSAN の作成について（37-6 ページ）
- VSAN の静的な作成（37-6 ページ）
- ポートの VSAN メンバーシップについて（37-7 ページ）
- スタティック ポートの VSAN メンバーシップの割り当て（37-7 ページ）
- VSAN スタティック メンバーシップの表示（37-8 ページ）
- デフォルト VSAN の概要（37-8 ページ）
- 分離された VSAN の概要（37-9 ページ）
- 独立 VSAN メンバーシップの表示（37-9 ページ）
- VSAN の動作ステート（37-9 ページ）
- スタティック VSAN の削除の概要（37-9 ページ）
- スタティック VSAN の削除（37-10 ページ）
- ロード バランシングについて（37-10 ページ）
- ロード バランシングの設定（37-11 ページ）
- Interop モードの概要（37-11 ページ）

VSAN の作成について

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

VSAN の静的な作成

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

VASN を作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch#` **`configuration terminal`**	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`vsan database`** `switch(config-vsan-db)#`	VSAN に対するデータベースを設定します。アプリケーション特有の VSAN パラメータは、このプロンプトから設定できません。
ステップ 3	`switch(config-vsan-db)#` **`vsan`** *`vsan-id`*	VSAN が存在しない場合は、指定された ID で VSAN を作成します。

	コマンド	目的
ステップ 4	switch(config-vsan-db)# **vsan** *vsan-id* **name** *name* updated vsan 2	割り当てられた名前で VSAN をアップデートします。
ステップ 5	switch(config-vsan-db)# **vsan** *vsan-id* **suspend**	選択された VSAN を中断します。
ステップ 6	switch(config-vsan-db)# **no vsan** *vsan-id* **suspend**	前のステップで入力した **suspend** コマンドを無効にします。
ステップ 7	switch(config-vsan-db)# **end** switch#	EXEC モードに戻ります。

ポートの VSAN メンバーシップについて

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

- スタティック：ポートに VSAN を割り当てます。

  「スタティック ポートの VSAN メンバーシップの割り当て」セクション（37-7 ページ）を参照してください。

- ダイナミック：デバイス WWN に基づいて VSAN を割り当てます。この方式は、Dynamic Port VSAN Membership（DPVM）と呼ばれます。Cisco Nexus 5000 シリーズ スイッチは DPVM をサポートしません。

VSAN トランキング ポートは、許可リストの一部である VSAN の対応リストを持ちます（第35章「VSAN トランキングの設定」を参照）。

スタティック ポートの VSAN メンバーシップの割り当て

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

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **vsan database** switch(config-vsan-db)#	VSAN に対するデータベースを設定します。
ステップ 3	switch(config-vsan-db)# **vsan** *vsan-id*	VSAN が存在しない場合は、指定された ID で VSAN を作成します。
ステップ 4	switch(config-vsan-db)# **vsan** *vsan-id* **interface fc** *slot/port* または switch(config-vsan-db)# **vsan** *vsan-id* **interface vfc** *slot/port*	指定されたインターフェイスのメンバーシップを VSAN に割り当てます。
ステップ 5	switch(config-vsan-db)# **vsan** *vsan-id* **interface vfc** *slot/port*	変更された VSAN を反映させるために、インターフェイスのメンバーシップ情報を更新します。
	switch(config-vsan-db)# **no vsan** *vsan-id* **interface fc** *slot/port*	VSAN からインターフェイスを削除します。

VSAN スタティック メンバーシップの表示

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

次に、指定された VSAN のメンバーシップ情報を表示する例を示します。

```
switch # show vsan 1 membership
vsan 1 interfaces:
        fc2/1   fc2/2   fc2/3   fc2/4
        san-port-channel 3  vfc1/1
```

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

次に、すべての VSAN のメンバーシップ情報を表示する例を示します。

```
switch # show vsan membership
vsan 1 interfaces:
        fc2/1   fc2/2   fc2/3   fc2/4
        san-port-channel 3  vfc3/1
vsan 2 interfaces:
        fc2/3 vfc4/1
vsan 7 interfaces:
vsan 100 interfaces:
vsan 4094(isolated vsan) interfaces:
```

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

```
Displays Static Membership Information for a Specified Interface
switch # show vsan membership interface fc2/1
fc2/1
        vsan:1
        allowed list:1-4093
```

デフォルト VSAN の概要

Cisco Nexus 5000 シリーズ では、スイッチの出荷時の設定値は、デフォルト VSAN 1 だけイネーブルです。VSAN 1 を実稼働環境の VSAN として使用しないことを推奨します。VSAN が設定されていない場合、ファブリック内のすべてのデバイスはデフォルト VSAN に含まれていると見なされます。デフォルトでは、デフォルト VSAN にすべてのポートが割り当てられています。

（注） VSAN 1 は削除できませんが、中断できます。

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

分離された VSAN の概要

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

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

注意 独立 VSAN を使用してポートを設定しないでください。

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

独立 VSAN メンバーシップの表示

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

VSAN の動作ステート

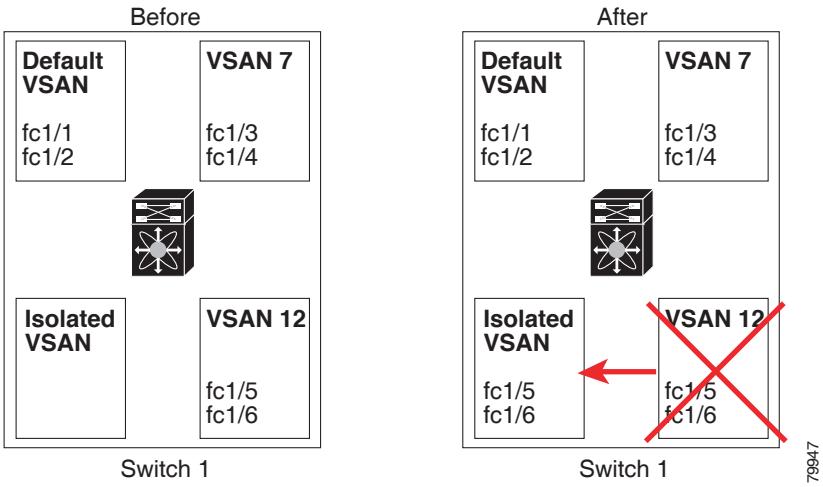
VSAN がアクティブの状態で、最低 1 つのポートがアップの状態であれば、VSAN は動作ステートにあります。このステートは、トラフィックがこの VSAN を通過できることを示します。このステートは設定できません。

スタティック VSAN の削除の概要

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

- VSAN 属性およびポート メンバーシップの詳細は、VSAN マネージャによって保持されます。コンフィギュレーションから VSAN を削除すると、この機能が影響を受けます。VSAN が削除されると、VSAN 内のすべてのポートが非アクティブになり、ポートが独立 VSAN に移動されます。同一の VSAN が再作成されると、ポートはその VSAN に自動的に割り当てられることはありません。明示的にポート VSAN メンバーシップを再設定する必要があります（図 37-4を参照）。

図 37-4　VSAN ポート メンバーシップの詳細



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

（注） 許可 VSAN リストは、VSAN が削除されても影響を受けません（第35 章「VSAN トランキングの設定」を参照）。

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

スタティック VSAN の削除

VSAN および各種の属性を削除するには、次の作業を行います。

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

ロード バランシングについて

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

ロード バランシングの設定

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

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

Interop モードの概要

インターオペラビリティを使用すると、複数ベンダーによる製品の間で相互に接続できます。ファイバ チャネル標準規格では、ベンダーに対して共通の外部ファイバ チャネル インターフェイスを作成することを推奨しています。詳細は、「スイッチの相互運用性」セクション（43-9 ページ）を参照してください。

スタティック VSAN 設定の表示

次に、特定の VSAN に関する情報を表示する例を示します。

```
switch# show vsan 100
...
```

次に、VSAN 使用状況を表示する例を示します。

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

次に、すべての VSAN を表示する例を示します。

```
switch# show vsan
```

デフォルト設定

表 37-2 では、設定されたすべての VSAN のデフォルト設定値を示します。

表 37-2　デフォルト VSAN パラメータ

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

CHAPTER 38

ゾーンの設定と管理

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

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

この章は、次の項で構成されています。

- ゾーン分割に関する情報（38-1 ページ）
- ゾーンの設定（38-7 ページ）
- ゾーン セット（38-8 ページ）
- ゾーン セットの配信（38-13 ページ）
- ゾーン セット配信（38-15 ページ）
- ゾーン情報の確認（38-17 ページ）
- 拡張ゾーン分割（38-18 ページ）
- ゾーン データベースの圧縮（38-24 ページ）
- ゾーンおよびゾーン セットの分析（38-25 ページ）
- デフォルト設定（38-25 ページ）

（注） 表 37-1（37-4 ページ）に、ゾーンと VSAN の相違点を示します。

ゾーン分割に関する情報

ここでは、ゾーン分割について説明します。具体的な内容は次のとおりです。

- ゾーン分割の特徴（38-2 ページ）
- ゾーン分割の例（38-3 ページ）
- ゾーン実装（38-4 ページ）
- アクティブおよびフル ゾーン セットの設定時の注意事項（38-5 ページ）

ゾーン分割の特徴

ゾーン分割には、次の特徴があります。

- ゾーンは、複数のゾーン メンバで構成されます。
  - ゾーンのメンバ同士はアクセスできますが、異なるゾーンのメンバ同士はアクセスできません。
  - ゾーン分割がアクティブでない場合、すべてのデバイスがデフォルト ゾーンのメンバとなります。
  - ゾーン分割がアクティブの場合、アクティブ ゾーン（アクティブ ゾーン セットに含まれるゾーン）にないデバイスがデフォルト ゾーンのメンバとなります。
  - ゾーンのサイズを変更できます。
  - デバイスは複数のゾーンに所属できます。
  - 物理ファブリックでは、最大 16,000 メンバを収容できます。これには、ファブリック内のすべての VSAN が含まれます。
- ゾーン セットは、1 つまたは複数のゾーンで構成されます。
  - ゾーン セットは、単一エンティティとしてファブリックのすべてのスイッチでアクティブまたは非アクティブにできます。
  - アクティブにできるのは、常に 1 つのゾーン セットだけです。
  - 1 つのゾーンを 複数のゾーン セットのメンバにできます。
  - ゾーン スイッチあたりの最大ゾーン セット数は 500 です。
- ゾーン分割は、ファブリックの任意のスイッチから管理できます。
  - 任意のスイッチからゾーンをアクティブにした場合、ファブリックのすべてのスイッチがアクティブ ゾーン セットを受信します。また、ファブリック内のすべてのスイッチにフルゾーン セットが配布されます（この機能が送信元スイッチでイネーブルである場合）。
  - 既存のファブリックに新しいスイッチが追加されると、新しいスイッチによってゾーン セットが取得されます。
- ゾーンの変更を中断せずに設定できます。
  - 影響を受けないポートまたはデバイスのトラフィックを中断させることなく、新しいゾーンおよびゾーン セットをアクティブにできます。
- ゾーン メンバーシップは、次の識別情報を使用して指定できます。
  - Port World Wide Name（pWWN）：スイッチに接続された N ポートの pWWN をゾーンのメンバとして指定します。
  - ファブリック pWWN：ファブリック ポートの WWN（スイッチ ポートの WWN）を指定します。このメンバーシップは、ポートベース ゾーン分割とも呼ばれます。
  - FC ID：スイッチに接続された N ポートの FC ID をゾーンのメンバとして指定します。
  - インターフェイスおよび Switch WWN（sWWN）：sWWN によって識別されたスイッチのインターフェイスを指定します。このメンバーシップは、インターフェイス ゾーン分割とも呼ばれます。
  - インターフェイスおよびドメイン ID：ドメイン ID によって識別されたスイッチのインターフェイスを指定します。
  - ドメイン ID およびポート番号：シスコ スイッチ ドメインのドメイン ID を指定し、さらに他社製スイッチに所属するポートを指定します。

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

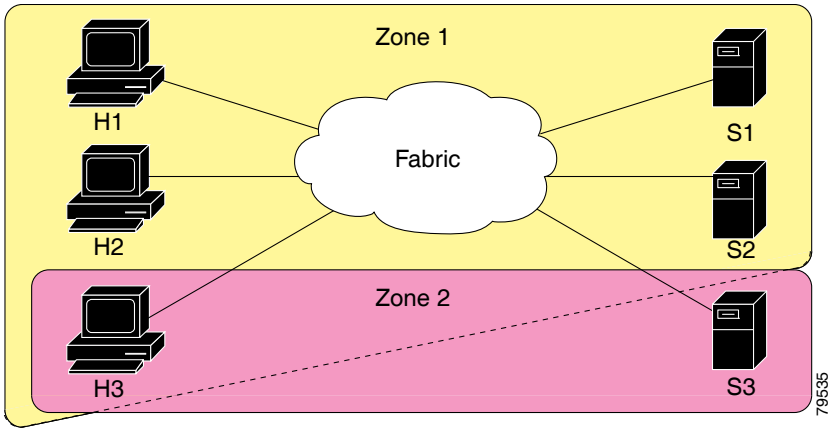
- デフォルト ゾーン メンバーシップには、特定のメンバーシップとの関係を持たないすべてのポートまたは WWN が含まれます。デフォルト ゾーン メンバ間のアクセスは、デフォルト ゾーン ポリシーによって制御されます。
- VSAN あたり最大 8000 ゾーン、スイッチ上の全 VSAN で最大 8000 ゾーンを設定できます。

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

ゾーン分割の例

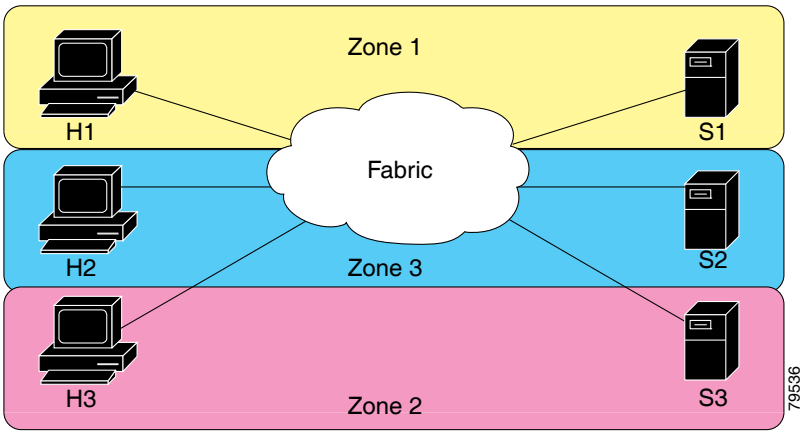
図 38-1 に、ファブリックの 2 つのゾーン（ゾーン 1 およびゾーン 2）で構成されるゾーン セットを示します。ゾーン 1 は、3 つすべてのホスト（H1、H2、H3）からストレージ システム S1 と S2 に存在するデータへのアクセスを提供します。ゾーン 2 では、S3 のデータに H3 からだけアクセスできます。H3 は、両方のゾーンに存在します。

図 38-1　　2 つのゾーンによるファブリック



ほかの方法を使用して、このファブリックを複数のゾーンに分割することもできます。図 38-2 に、別の方法を示します。新しいソフトウェアをテストするために、ストレージ システム S2 を分離する必要があると想定します。これを実行するために、ホスト H2 とストレージ S2 だけを含むゾーン 3 が設定されます。ゾーン 3 ではアクセスを H2 と S2 だけに限定し、ゾーン 1 ではアクセスを H1 と S1 だけに限定できます。

図 38-2　　3 つのゾーンによるファブリック



ゾーン実装

Cisco Nexus 5000 シリーズ スイッチは、自動的に次の基本的なゾーン機能をサポートします（設定を追加する必要はありません）。

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

必要に応じて、さらに次のゾーン機能を設定できます。

- VSAN 単位ですべてのスイッチにフル ゾーン セットを伝播します。
- ゾーン分割されていないメンバのデフォルト ポリシーを変更します。
- VSAN を interop モードに設定することによって、他のベンダーと相互運用できます。相互に干渉することなく、同じスイッチ内で 1 つの VSAN を interop モードに、別の VSAN を基本モードに設定することもできます。
- E ポートを分離状態から復旧します。

アクティブおよびフル ゾーン セットの設定時の注意事項

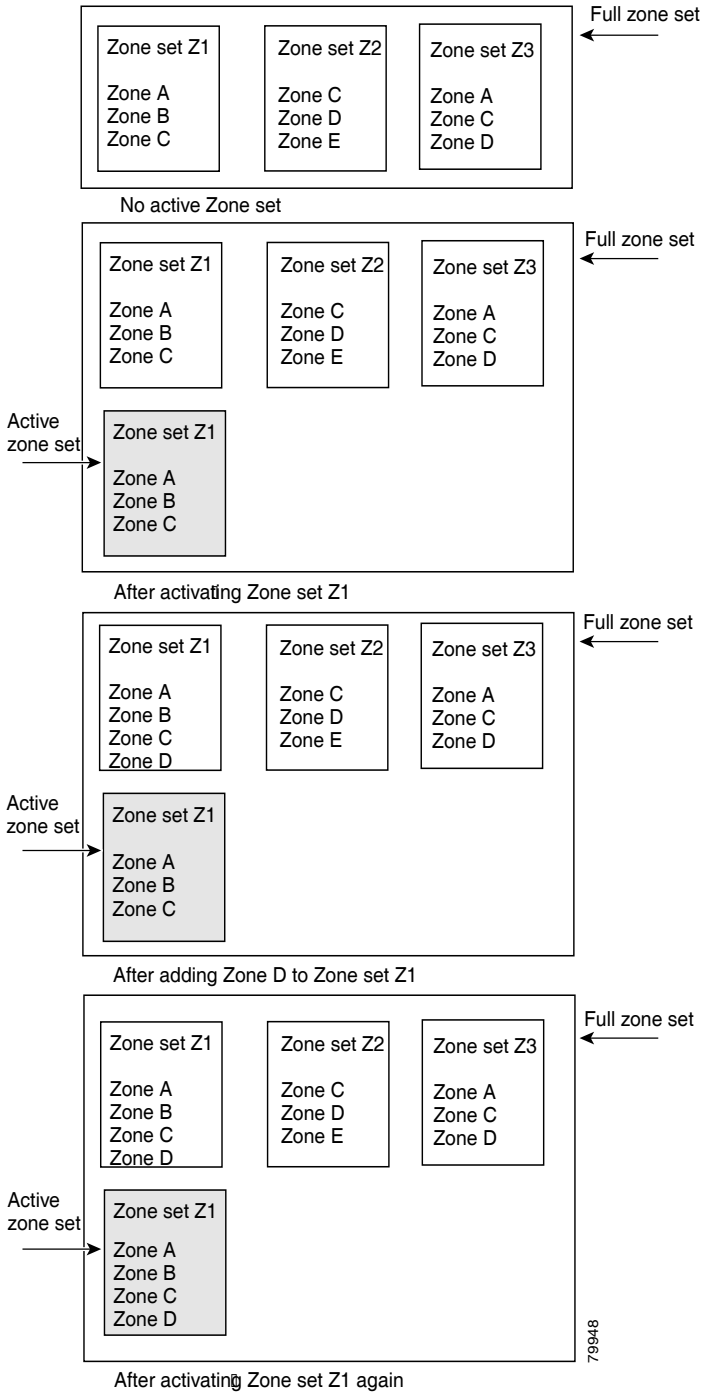
ゾーン セットを設定する前に、次の注意事項について検討してください。

- 各 VSAN は、複数のゾーン セットを持つことができますが、アクティブにできるのは常に 1 つのゾーン セットだけです。
- ゾーン セットを作成すると、そのゾーン セットは、フル ゾーン セットの一部となります。
- ゾーン セットがアクティブな場合は、フル ゾーン セットからのゾーン セットのコピーがゾーン分割の実行に使用されます。これは、アクティブ ゾーン セットと呼ばれます。アクティブ ゾーン セットは変更できません。アクティブ ゾーン セットに含まれるゾーンは、アクティブ ゾーンと呼ばれます。
- 管理者は、同一名のゾーン セットがアクティブであっても、フル ゾーン セットを変更できます。ただし、加えられた変更が有効になるのは、再アクティブ化したときです。
- アクティブ化が実行されると、永続的なコンフィギュレーションにアクティブ ゾーン セットが自動保存されます。これにより、スイッチのリセットにおいてもスイッチはアクティブ ゾーン セット情報を維持できます。
- ファブリックのその他すべてのスイッチは、アクティブ ゾーン セットを受信するので、それぞれのスイッチでゾーン分割を実行できます。
- ハードおよびソフト ゾーン分割は、アクティブ ゾーン セットを使用して実装されます。変更は、ゾーン セットのアクティブ化によって有効になります。
- アクティブ ゾーン セットに含まれない FC ID または Nx ポートは、デフォルト ゾーンに所属します。デフォルト ゾーン情報は、他のスイッチに配信されません。

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

図 38-3 に、アクティブにされたゾーン セットに追加されるゾーンを示します。

図 38-3　　アクティブおよびフル ゾーン セット



ゾーンの設定

ゾーンを設定し、ゾーン名を割り当てるには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# zone name zone-name vsan vsan-id` `switch(config-zone)#`	指定された VSAN にゾーンを設定します。 **（注）** すべての英数字か、または記号（$、-、^、_）のうち 1 つがサポートされます。

ステップ 3	`switch(config-zone)# member type value`
	pWWN の例:
	`switch(config-zone)# member pwwn pwwn-id`
	ファブリック pWWN の例:
	`switch(config-zone)# member fwwn fwwn-id`
	FC ID の例:
	`switch(config-zone)# member fcid fcid`
	FC エイリアスの例:
	`switch(config-zone)# member fcalias Payroll`
	ドメイン ID の例:
	`switch(config-zone)# member domain-id domain-id portnumber number`
	ローカル sWWN インターフェイスの例:
	`switch(config-zone)# member interface type slot/port`
	リモート sWWN インターフェイスの例:
	`switch(config-zone)# member interface type slot/port swwn swwn-id`
	ドメイン ID インターフェイスの例:
	`switch(config-zone)# member interface fc slot/port domain-id domain-id`
		指定されたタイプ（pWWN、ファブリック pWWN、FC ID、FC エイリアス、ドメイン ID、またはインターフェイス）および値に基づいて、指定されたゾーンにメンバを設定します。
		注意 同じファブリック内に FabricWare を実行する Cisco MDS 9020 スイッチがある場合には、Cisco NX-OS を実行するすべての SAN スイッチには、pWWN タイプのゾーン分割だけを設定する必要があります。

	ヒント 該当する表示コマンド（たとえば、**show interface** または **show flogi database**）を使用して、必要な値を 16 進表記で取得します。	

ヒント **show wwn switch** コマンドを使用して sWWN を取得します。sWWN を指定しない場合、ソフトウェアは自動的にローカル sWWN を使用します。

次に、ゾーン メンバを設定する例を示します。

```
switch(config-zone)# member type value
pWWN の例:
switch(config-zone)# member pwwn 10:00:00:23:45:67:89:ab
ファブリック pWWN の例:
switch(config-zone)# member fwwn 10:01:10:01:10:ab:cd:ef
FC ID の例:
switch(config-zone)# member fcid 0xce00d1
FC エイリアスの例:
switch(config-zone)# member fcalias Payroll
ドメイン ID の例:
switch(config-zone)# member domain-id 2 portnumber 23
```

```
ローカル sWWN インターフェイスの例:
switch(config-zone)# member interface fc 2/1
リモート sWWN インターフェイスの例:
switch(config-zone)# member interface fc2/1 swwn 20:00:00:05:30:00:4a:de
ドメイン ID インターフェイスの例:
switch(config-zone)# member interface fc2/1 domain-id 25
```

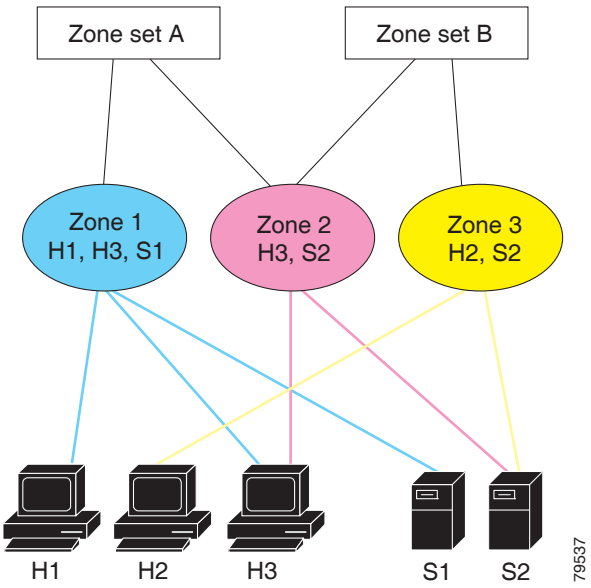
ゾーン セット

ここではゾーン セットについて説明します。具体的な内容は次のとおりです。

- ゾーン セットのアクティブ化(38-9 ページ)
- デフォルト ゾーンの概要(38-9 ページ)
- デフォルト ゾーンのアクセス権限の設定(38-10 ページ)
- FC エイリアスの作成の概要(38-10 ページ)
- FC エイリアスの作成(38-10 ページ)
- ゾーン セットの作成とメンバ ゾーンの追加(38-11 ページ)
- ゾーンの適用(38-12 ページ)

図 38-4 では、それぞれ独自のメンバーシップ階層とゾーン メンバーを持つ別個の 2 つのセットが作成されています。

図 38-4　ゾーン セット、ゾーン、ゾーン メンバの階層



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

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

ゾーン セットのアクティブ化

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

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

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

デフォルト ゾーンの概要

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

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

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

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

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

（注） デフォルト ゾーン設定のデフォルト設定値は変更できます。

デフォルト ポリシーが permit として設定される場合、またはゾーン セットがアクティブのとき、デフォルト ゾーン メンバは明示的に表示されます。デフォルト ポリシーが deny として設定されている場合、アクティブ ゾーン セットを表示すると、このゾーンのメンバの一覧表示は明示されません。

デフォルト ゾーンのアクセス権限の設定

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

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# zone default-zone permit vsan vsan-id`	デフォルト ゾーン メンバへのトラフィック フローを許可します。
	`switch(config)# no zone default-zone permit vsan vsan-id`	デフォルト ゾーン メンバへのトラフィック フローを拒否（デフォルト）します。

FC エイリアスの作成の概要

次の値を使用して、エイリアス名を割り当て、エイリアス メンバを設定できます。

- pWWN：N ポートの 16 進表記の WWN（10:00:00:23:45:67:89:ab など）
- fWWN：ファブリック ポート名の WWN は 16 進形式です（10:00:00:23:45:67:89:ab など）。
- FC ID：0xhhhhhh 形式の N ポート ID（0xce00d1 など）
- ドメインID：ドメインID は 1 ～ 239 の整数です。このメンバーシップ設定を完了するには、他社製スイッチの必須ポート番号が必要です。
- インターフェイス：インターフェイスベース ゾーン分割は、スイッチ インターフェイスがゾーンを設定するのに使用される点でポートベース ゾーン分割と似ています。スイッチ インターフェイスをローカル スイッチとリモート スイッチの両方でゾーン メンバとして指定できます。リモート スイッチを指定するには、特定の VSAN 内のリモート Switch WWN（sWWN）またはドメイン ID を入力します。

ヒント　スイッチは、VSAN あたり最大 2048 のエイリアスをサポートします。

FC エイリアスの作成

エイリアスを作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fcalias name AliasSample vsan vsan-id` `switch(config-fcalias)#`	エイリアス名（AliasSample）を設定します。

	コマンド	目的
ステップ 3	switch(config-fcalias)# **member** *type value* pWWN の例: switch(config-fcalias)# **| pwwn** *pwwn-id* fWWN の例: switch(config-fcalias)# **| fwwn** *fwwn-id* FC ID の例: switch(config-fcalias)# **| fcid 0x222222** ドメイン ID の例: switch(config-fcalias)# **| domain-id** *domain-id* **portnumber** *number* ローカル sWWN インターフェイスの例: switch(config-fcalias)# **| interface** *type slot/port* **[swwn | domain-id 25]**	指定されたタイプ（pWWN、ファブリック pWWN、FC ID、ドメイン ID、またはインターフェイス）および値に基づいて、指定された FC エイリアス（AliasSample）にメンバを設定します。 **（注）** 複数のメンバを複数の行で指定できます。

次に、異なるタイプのメンバ エイリアスを設定する例を示します。

```
switch(config)# fcalias name AliasSample vsan 3
switch(config-fcalias)# member type value
pWWN の例:
switch(config-fcalias)# member pwwn 10:00:00:23:45:67:89:ab
fWWN の例:
switch(config-fcalias)# member fwwn 10:01:10:01:10:ab:cd:ef
FC ID の例:
switch(config-fcalias)# member fcid 0x222222
ドメイン ID の例:
switch(config-fcalias)# member domain-id 2 portnumber 23
ローカル sWWN インターフェイスの例:
switch(config-fcalias)# member interface fc2/1
リモート sWWN インターフェイスの例:
switch(config-fcalias)# member interface fc2/1 swwn 20:00:00:05:30:00:4a:de
ドメイン ID インターフェイスの例:
switch(config-fcalias)# member interface fc2/1 domain-id 25
```

ゾーン セットの作成とメンバ ゾーンの追加

複数のゾーンを含むゾーン セットを作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **zone*set* name** *zoneset-name* **vsan** *vsan-id* switch(config-zoneset)#	Zoneset1 というゾーン セットを設定します。 **ヒント** ゾーン セットをアクティブにするには、まずゾーンとゾーン セットを 1 つ作成する必要があります。
ステップ 3	switch(config-zoneset)# **member** *name*	指定されたゾーン セット（Zoneset1）に Zone1 をメンバとして追加します。 **ヒント** 指定されたゾーン名が事前に設定されていない場合、このコマンドを実行すると "zone not present" エラーメッセージが返されます。

	コマンド	目的
ステップ 4	`switch(config-zoneset)# zone name zone-name` `switch(config-zoneset-zone)#`	指定されたゾーン セットにゾーンを追加します。 **ヒント**　ゾーン セット プロンプトからゾーンを作成する必要がある場合は、このステップを実行します。
ステップ 5	`switch(config-zoneset-zone)# member fcid fcid` `switch(config-zoneset-zone)#`	新しいゾーンに新しいメンバを追加します。 **ヒント**　ゾーン セット プロンプトからゾーンにメンバを追加する必要がある場合は、このステップを実行します。

ヒント　アクティブ ゾーン セットを保存するために、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーする必要はありません。ただし、フル ゾーン セットを明示的に保存するには、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーする必要があります。

（注）　デバイス エイリアス モードをイネーブルにする前に、これらのモードについて充分に理解してください。デバイス エイリアス モードに関する詳細と要件については、第 39 章「DDAS」を参照してください。

ゾーンの適用

ゾーン分割は、ソフトとハードの 2 つの方法で実行できます。各エンド デバイス（N ポート）は、ネーム サーバにクエリーを送信することでファブリック内の他のデバイスを検出します。デバイスがネーム サーバにログインすると、ネーム サーバはクエリー元デバイスがアクセスできる他のデバイスのリストを返します。N ポートがゾーンの外部にあるその他のデバイスの FCID を認識しない場合、そのデバイスにアクセスできません。

ソフト ゾーン分割では、ゾーン分割の制限がネーム サーバとエンド デバイス間の対話時にだけ適用されます。エンド デバイスが何らかの方法でゾーン外部のデバイスの FCID を認識できる場合、そのデバイスにアクセスできます。

ハード ゾーン分割は、N ポートから送信される各フレームでハードウェアによって実行されます。スイッチにフレームが着信した時点で、送信元/宛先 ID と許可済みの組み合わせが照合されるため、ワイヤスピードでフレームを送信できます。ハード ゾーン分割は、ゾーン分割のすべての形式に適用されます。

（注）　ハード ゾーン分割は、すべてのフレームでゾーン分割制限を実行し、不正なアクセスを防ぎます。

Cisco Nexus 5000 シリーズ のスイッチは、ハードとソフトの両方のゾーン分割をサポートします。

ゾーン セットの配信

フル ゾーン セットは、EXEC モード レベルで **zoneset distribute vsan** コマンドを使用する一時配信、またはコンフィギュレーション モード レベルで **zoneset distribute full vsan** コマンドを使用するフル ゾーン セット配信のどちらかの方式を使用して配信できます。表 38-1 に、これらの方式の相違点を示します。

表 38-1　ゾーン セット配信の相違点

一時配信 zoneset distribute vsan コマンド （EXEC モード）	フル ゾーン セット配信 zoneset distribute full vsan コマンド (コンフィギュレーション モード)
フル ゾーン セットはすぐに配信されます。	フル ゾーン セットはすぐには配信されません。
アクティブ化、非アクティブ化、または結合時には、アクティブ ゾーン セットと同時にフル ゾーン セット情報を伝播しません。	アクティブ化、非アクティブ化、または結合時には、アクティブ ゾーン セットと同時にフル ゾーン セット情報を伝播します。

ここではゾーン セットの配信について説明します。具体的な内容は次のとおりです。

- フル ゾーン セット配信のイネーブル化（38-13 ページ）
- 一時配信のイネーブル化（38-13 ページ）
- リンク分離からの回復の概要（38-14 ページ）
- ゾーン セットのインポートおよびエクスポート（38-15 ページ）

フル ゾーン セット配信のイネーブル化

Cisco Nexus 5000 シリーズのすべてのスイッチは、新しい E ポート リンクが立ち上がったとき、または新しいゾーン セットが VSAN でアクティブにされたときに、アクティブ ゾーン セットを配信します。ゾーン セットの配信は、隣接スイッチへのマージ要求の送信時、またはゾーン セットのアクティブ化の際に行われます。

VSAN 単位で、VSAN 上のすべてのスイッチへのフル ゾーン セットおよびアクティブ ゾーン セットの配信をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch#` **`configuration terminal`**	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`zoneset distribute full vsan`** *`vsan-id`*	アクティブ ゾーン セットとともにフル ゾーン セットの送信をイネーブルにします。

一時配信のイネーブル化

ファブリック全体に、非アクティブで未変更のゾーン セットを一度だけ配信します。

この配信を実行するには、EXEC モードで **zoneset distribute vsan** *vsan-id* コマンドを使用します。

```
switch# zoneset distribute vsan 2
Zoneset distribution initiated. check zone status
```

このコマンドではフル ゾーン セット情報の配信だけを実行し、スタートアップ コンフィギュレーションへの情報の保存は行いません。フル ゾーン セット情報をスタートアップ コンフィギュレーションに保存する場合は、**copy running-config start-config** コマンドを明示的に入力する必要があります。

（注）フル ゾーン セットの一時配信は interop 2 および interop 3 モードでサポートされており、interop 1 モードではサポートされていません。

ゾーン セット一時配信要求のステータスを確認するには、**show zone status vsan** *vsan-id* コマンドを使用します。

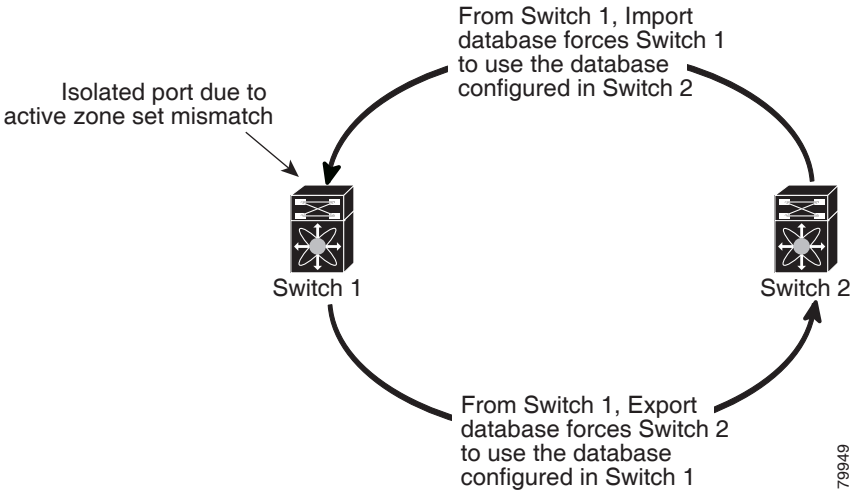
```
switch# show zone status vsan 3
VSAN: 3 default-zone: permit distribute: active only Interop: 100
    mode:basic merge-control:allow
    session:none
    hard-zoning:enabled
Default zone:
    qos:none broadcast:disabled ronly:disabled
Full Zoning Database :
    Zonesets:0  Zones:0 Aliases: 0
Active Zoning Database :
    Name: nozoneset  Zonesets:1  Zones:2
Status: Zoneset distribution completed at 04:01:06 Aug 28 2004
```

リンク分離からの回復の概要

ファブリックの 2 つのスイッチが TE ポートまたは E ポートを使用して結合される場合、アクティブ ゾーン セットのデータベースが 2 つのスイッチまたはファブリック間で異なると、この TE ポートおよび E ポートが分離する可能性があります。TE ポートまたは E ポートが分離した場合、次の 3 つのオプションのいずれかを使用して分離状態からポートを回復できます。

- 近接スイッチのアクティブ ゾーン セットのデータベースをインポートし、現在のアクティブ ゾーン セットと交換します（図 38-5 を参照）。
- 現在のデータベースを近接スイッチにエクスポートします。
- フル ゾーン セットを編集し、修正されたゾーン セットをアクティブにしてから、リンクを立ち上げることにより、手動で矛盾を解決します。

図 38-5　データベースのインポートとエクスポート



ゾーン セットのインポートおよびエクスポート

ゾーン セット情報を隣接スイッチにエクスポート、または隣接スイッチからインポートするには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# zoneset import interface fc slot/port vsan vsan-id`	VSAN の指定されたインターフェイスを介して接続された隣接スイッチからゾーン セットをインポートします。
	`switch# zoneset import interface fc slot/port vsan vsan-id`	VSAN 範囲の指定されたインターフェイスを介して接続された隣接スイッチからゾーン セットをインポートします。
ステップ 2	`switch# zoneset export vsan vsan-id`	指定された VSAN を介して接続された隣接スイッチにゾーン セットをエクスポートします。
	`switch# zoneset export vsan vsan-id`	VSAN の指定された範囲を介して接続された隣接スイッチにゾーン セットをエクスポートします。

（注） インポートとエクスポートの操作は、1 つのスイッチから行ってください。1 つのスイッチからインポートし、別のスイッチからエクスポートすると、リンクが再び分離する可能性があります。

ゾーン セット配信

コピーを作成し、既存のアクティブ ゾーン セットを変更することなく編集できます。アクティブ ゾーン セットを bootflash: ディレクトリ、volatile: ディレクトリ、または slot0 から次のいずれかのエリアにコピーできます。

- フル ゾーン セット
- リモート ロケーション（FTP、SCP、SFTP、または TFTP を使用）

アクティブ ゾーン セットは、フル ゾーン セットに含まれません。フル ゾーン セットが失われた場合または伝播されなかった場合に、既存のゾーン セットに変更を加えても、アクティブにできません。

注意　同一名のゾーンがフル ゾーン データベースにすでに存在する場合、アクティブ ゾーン セットをフル ゾーン セットにコピーすると、その同一名のゾーンが上書きされることがあります。

この項では、次のトピックについて取り上げます。

- ゾーン セットのコピー（38-16 ページ）
- ゾーン、ゾーン セット、エイリアスの名前の変更（38-16 ページ）
- ゾーン、ゾーン セット、FC エイリアス、ゾーン属性グループのコピー（38-17 ページ）
- ゾーン サーバ データベースのクリア（38-17 ページ）

ゾーン セットのコピー

Cisco Nexus 5000 シリーズ スイッチでは、アクティブ ゾーン セットは編集できません。ただし、アクティブ ゾーン セットをコピーして、編集可能な新しいゾーン セットを作成できます。

ゾーン セットのコピーを作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# zone copy active-zoneset full-zoneset vsan vsan-id` `Please enter yes to proceed.(y/n) [n]? y`	指定された VSAN のアクティブ ゾーン セットのコピーをフル ゾーン セットに作成します。
	`switch# zone copy vsan vsan-id active-zoneset scp://guest@myserver/tmp/active_zoneset.txt`	SCP を使用して、指定された VSAN のアクティブ ゾーンをリモート ロケーションにコピーします。

ゾーン、ゾーン セット、エイリアスの名前の変更

ゾーン、ゾーン セット、FC エイリアス、またはゾーン属性グループの名前を変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# zoneset rename oldname newname vsan vsan-id`	指定された VSAN のゾーン セット名を変更します。
	`switch(config)# zone rename oldname newname vsan vsan-id`	指定された VSAN のゾーン名を変更します。
	`switch(config)# fcalias rename oldname newname vsan vsan-id`	指定された VSAN の fcalias 名を変更します。
	`switch(config)# zone-attribute-group rename oldname newname vsan vsan-id`	指定された VSAN のゾーン属性グループ名を変更します。
ステップ 3	`switch(config)# zoneset activate name newname vsan vsan-id`	ゾーン セットをアクティブにし、アクティブ ゾーン セット内の新しいゾーン名に更新します。

ゾーン、ゾーン セット、FC エイリアス、ゾーン属性グループのコピー

ゾーン、ゾーン セット、FC エイリアス、またはゾーン属性グループをコピーするには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# zoneset clone oldname newname vsan vsan-id`	指定された VSAN のゾーン セットをコピーします。
	`switch(config)# zone clone oldname newname vsan number`	指定された VSAN 内のゾーンをコピーします。
	`switch(config)# fcalias clone oldname newname vsan vsan-id`	指定された VSAN の FC エイリアス名をコピーします。
	`switch(config)# zone-attribute-group clone oldname newname vsan vsan-id`	指定された VSAN のゾーン属性グループをコピーします。
ステップ 3	`switch(config)# zoneset activate name newname vsan vsan-id`	ゾーン セットをアクティブにし、アクティブ ゾーン セット内の新しいゾーン名に更新します。

ゾーン サーバ データベースのクリア

指定された VSAN のゾーン サーバ データベース内のすべての設定情報をクリアできます。

ゾーン サーバ データベースをクリアするには、次のコマンドを使用します。

```
switch# clear zone database vsan 2
```

（注）　**clear zone database** コマンドを入力したあとに、明示的に **copy running-config startup-config** を入力して、次にスイッチを起動するときに確実に実行コンフィギュレーションが使用されるようにする必要があります。

（注）　ゾーン セットをクリアすると、フル ゾーン データベースだけが消去され、アクティブ ゾーン データベースは消去されません。

ゾーン情報の確認

ゾーン情報を表示するには、**show** コマンドを使用します。特定のオブジェクトの情報（たとえば、特定のゾーン、ゾーン セット、VSAN、エイリアス、または **brief** や **active** などのキーワード）を要求する場合、指定されたオブジェクトの情報だけが表示されます。

次に、すべての VSAN のゾーン情報を表示する例を示します。

```
switch# show zone
```

次に、特定の VSAN のゾーン情報を表示する例を示します。

```
switch# show zone vsan 1
```

次に、VSAN 範囲に設定されたゾーン セットを表示する例を示します。

```
switch# show zoneset vsan 2-3
```

次に、特定のゾーンのメンバを表示する例を示します。

```
switch# show zone name Zone1
```

次に、FC エイリアス設定を表示する例を示します。

```
switch# show fcalias vsan 1
```

次に、メンバが属しているすべてのゾーンを表示する例を示します。

```
switch# show zone member pwwn 21:00:00:20:37:9c:48:e5
```

次に、他のスイッチと交換される制御フレームの数を表示する例を示します。

```
switch# show zone statistics
```

次に、アクティブ ゾーン セットを表示する例を示します。

```
switch# show zoneset active
```

次に、アクティブ ゾーンを表示する例を示します。

```
switch# show zone active
```

次に、ゾーン ステータスを表示する例を示します。

```
switch# show zone status
```

拡張ゾーン分割

ゾーン分割機能は、FC-GS-4 および FC-SW-3 規格に準拠しています。どちらの規格も、前の項で説明した基本ゾーン分割機能と、この項で説明する拡張ゾーン分割機能をサポートしています。

この項では、次のトピックについて取り上げます。

- 拡張ゾーン分割の概要（38-19 ページ）
- 基本ゾーン分割から拡張ゾーン分割への変更（38-19 ページ）
- 拡張ゾーン分割から基本ゾーン分割への変更（38-20 ページ）
- 拡張ゾーン分割のイネーブル化（38-20 ページ）
- ゾーン データベースの変更（38-21 ページ）
- ゾーン データベース ロックの解除（38-21 ページ）
- データベースのマージ（38-22 ページ）
- ゾーン結合制御ポリシーの設定（38-23 ページ）
- デフォルトのゾーン ポリシー（38-23 ページ）
- システムのデフォルト ゾーン分割設定値の設定（38-23 ページ）
- 拡張ゾーン情報の確認（38-24 ページ）

拡張ゾーン分割の概要

表 38-2 は、Cisco Nexus 5000 シリーズのすべてのスイッチの拡張ゾーン分割機能の利点を示しています。

表 38-2　拡張ゾーン分割の利点

基本ゾーン分割	拡張ゾーン分割	拡張ゾーン分割の利点
複数の管理者が設定変更を同時に行うことができます。アクティブ化すると、ある管理者が別の管理者の設定変更を上書きできます。	単一のコンフィギュレーション セッションですべての設定を実行できます。セッションを開始すると、スイッチは変更を行うファブリック全体をロックします。	ファブリック全体を 1 つのコンフィギュレーション セッションで設定するため、ファブリック内での整合性が確保されます。
ゾーンが複数のゾーン セットに含まれる場合、各ゾーン セットにこのゾーンのインスタンスを作成します。	ゾーンが定義されると、必要に応じて、ゾーン セットがゾーンを参照します。	ゾーンが参照されるため、ペイロード サイズが縮小されています。データベースが大きくなるほど、サイズの縮小も顕著になります。
デフォルト ゾーン ポリシーがスイッチごとに定義されます。ファブリックをスムーズに動作させるため、ファブリック内のスイッチはすべて同一のデフォルト ゾーン設定を使用する必要があります。	ファブリック全体でデフォルト ゾーン設定を実行および交換します。	ポリシーがファブリック全体に適用されるため、トラブルシューティングの時間が短縮されます。
スイッチ単位でのアクティブ化の結果を取得するため、管理スイッチはアクティブ化に関する複合ステータスを提供します。この場合、障害のあるスイッチは特定されません。	各リモート スイッチからアクティブ化の結果と問題の特性を取得します。	エラー通知機能が強化されているため、トラブルシューティングが容易になります。
ゾーン分割データベースを配信するには、同じゾーン セットを再度アクティブ化する必要があります。再度アクティブ化すると、ローカル スイッチおよびリモート スイッチのハード ゾーン分割のハードウェア変更に影響することがあります。	ゾーン分割データベースに対して変更を行い、再度アクティブ化することなく変更を配信します。	アクティブ化せずにゾーン セットを配信すると、スイッチのハード ゾーン分割のハードウェア変更が回避されます。
シスコ固有のゾーン メンバ タイプ（シンボリック ノード名およびその他のタイプ）は他社製スイッチによって使用されることがあります。結合時に、シスコ固有のタイプは他社製スイッチによって誤って解釈されることがあります。	メンバ タイプを一意に識別するために、ベンダー固有のタイプ値とベンダー ID が提供されます。	ベンダー タイプが一意です。
fWWN ベースのゾーン メンバーシップは、シスコの interop モードでだけサポートされます。	標準の interop モード（interop モード 1）で fWWN ベースのメンバーシップがサポートされます。	fWWN ベースのメンバ タイプは標準化されています。

基本ゾーン分割から拡張ゾーン分割への変更

基本ゾーン分割モードから拡張ゾーン分割モードに変更するには、次の作業を行います。

ステップ 1　ファブリック内のすべてのスイッチが拡張モードで動作できることを確認します。

1 つ以上のスイッチが拡張モードで動作できない場合、拡張モードへ変更できません。

ステップ 2　動作モードを拡張ゾーン分割モードに設定します。

セッションが自動的に開始され、ファブリック全体のロック、拡張ゾーン分割のデータ構造を使用するアクティブおよびフル ゾーン分割データベースの配信、ゾーン分割ポリシーの配信、およびロックの解除が実行されます。ファブリック内のすべてのスイッチは、拡張ゾーン分割モードに移行します。

ヒント　基本ゾーン分割から拡張ゾーン分割への移行が完了したら、実行コンフィギュレーションを保存することを推奨します。

拡張ゾーン分割から基本ゾーン分割への変更

Cisco SAN スイッチでは、ほかの Cisco NX-OS リリースへのダウングレードおよびアップグレードを可能にするために、拡張ゾーン分割から基本ゾーン分割に変更できます。

拡張ゾーン分割モードから基本ゾーン分割モードに変更するには、次の作業を行います。

ステップ 1　アクティブおよびフル ゾーン セットに拡張ゾーン分割モード固有の設定が含まれていないことを確認します。

このような設定が存在する場合は、次に進む前にこれらの設定を削除します。既存の設定を削除しないと、スイッチ ソフトウェアは自動的にこれらの設定を削除します。

ステップ 2　動作モードを基本ゾーン分割モードに設定します。

セッションが自動的に開始され、ファブリック全体のロック、基本ゾーン分割のデータ構造を使用するゾーン分割情報の配信、設定変更の適用、およびファブリック内のすべてのスイッチのロック解除が実行されます。ファブリック内のすべてのスイッチは、基本ゾーン分割モードに移行します。

拡張ゾーン分割のイネーブル化

デフォルトでは、拡張ゾーン分割機能はすべての Cisco Nexus 5000 シリーズ スイッチでディセーブルです。

VSAN 内で拡張ゾーン分割をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# zone mode enhanced vsan vsan-id` `Set zoning mode command initiated.Check zone status`	指定された VSAN で拡張ゾーン分割をイネーブルにします。
	`switch(config)# no zone mode enhanced vsan vsan-id` `Set zoning mode command initiated.Check zone status`	指定された VSAN で拡張ゾーン分割をディセーブルにします。

ゾーン データベースの変更

ゾーン データベースに対する変更は、セッション内で実行されます。セッションは、コンフィギュレーション コマンドが初めて正常に実行されたときに作成されます。セッションが作成されると、ゾーン データベースのコピーが作成されます。セッションでの変更は、ゾーン分割データベースのコピー上で実行されます。ゾーン分割データベースのコピー上で行われる変更は、コミットするまで有効なゾーン分割 データベースには適用されません。変更を適用すると、セッションはクローズします。

ファブリックが別のユーザによってロックされ、何らかの理由でロックがクリアされない場合は、強制的に実行し、セッションをクローズします。このスイッチでロックをクリアする権限（ロール）が必要です。また、この操作は、セッションが作成されたスイッチから実行する必要があります。

VSAN 内のゾーン分割 データベースに対する変更をコミットまたは廃棄するには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# zone commit vsan vsan-id` `No pending info found`	拡張ゾーン データベースに変更を適用し、セッションをクローズします。
	`switch(config)# zone commit vsan vsan-id force`	拡張ゾーン データベースに変更を強制的に適用し、別のユーザが作成したセッションをクローズします。
	`switch(config)# no zone commit vsan vsan-id`	拡張ゾーン データベースへの変更を廃棄し、セッションをクローズします。
	`switch(config)# no zone commit vsan vsan-id force`	拡張ゾーン データベースへの変更を強制的に廃棄し、別のユーザが作成したセッションをクローズします。

ゾーン データベース ロックの解除

VSAN 内のスイッチのゾーン分割 データベースのセッション ロックを解除するには、最初にデータベースをロックしたスイッチから **no zone commit vsan** コマンドを使用します。

```
switch# configuration terminal
switch(config)# no zone commit vsan 2
```

no zone commit vsan コマンドを実行したあとも、リモート スイッチ上でセッションがロックされたままの場合、リモート スイッチ上で **clear zone lock vsan** コマンドを使用できます。

```
switch# clear zone lock vsan 2
```

（注） ファブリック内のセッション ロックを解除するには、最初に **no zone commit vsan** コマンドを使用することを推奨します。そのコマンドが失敗した場合は、セッションがロックされたままのリモート スイッチで、**clear zone lock vsan** コマンドを使用してください。

データベースのマージ

結合方式は、ファブリック全体の結合制御設定によって異なります。

- 制限:2 つのデータベースが同一でない場合、スイッチ間の ISL は分離されます。
- 許可:2 つのデータベースは、表 38-3 で指定された結合規則を使用して結合されます。

表 38-3　データベースのゾーン結合ステータス

ローカル データベース	隣接データベース	結合ステータス	結合結果
データベースに、名前[1]は同じだが、異なるゾーン、エイリアス、および属性グループを持つゾーン セットが含まれる。		成功	ローカル データベースおよび隣接データベースが結合されます。
データベースに、名前は [1]で同じだが、異なる番号を持つゾーン、ゾーン エイリアス、またはゾーン属性グループ オブジェクトが含まれる。		失敗	ISL は分離されます。
データなし	データあり	成功	ローカル データベースには隣接データベースの情報が存在します。
データあり	データなし	成功	隣接データベースにはローカル データベースの情報が存在します。

1. 拡張ゾーン分割モードでは、interop モード 1 のアクティブ ゾーン セットには名前がありません。ゾーン セット名が存在するのは、フル ゾーン セットの場合だけです。

結合プロセスは次のように動作します。

1. ソフトウェアがプロトコル バージョンを比較します。プロトコル バージョンが異なる場合、ISL は分離されます。
2. プロトコル バージョンが同じである場合、ゾーン ポリシーが比較されます。ゾーン ポリシーが異なる場合、ISL は分離されます。
3. ゾーン結合オプションが同じである場合、結合制御設定に基づいて比較が行われます。
   a. 設定が「制限」の場合、アクティブ ゾーン セットとフル ゾーン セットが同じになる必要があります。これらが同じでない場合、リンクは分離されます。
   b. 設定が「許可」の場合、結合規則を使用して結合が行われます。

ゾーン結合制御ポリシーの設定

結合制御ポリシーを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **configuration terminal** switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **zone merge-control restrict vsan** *vsan-id*	現在の VSAN の結合制御設定を「制限」に設定します。
	switch(config)# **no zone merge-control restrict vsan** *vsan-id*	現在の VSAN の結合制御設定をデフォルトの「許可」に設定します。
	switch(config)# **zone commit vsan** *vsan-id*	指定された VSAN に対する変更をコミットします。

デフォルトのゾーン ポリシー

デフォルト ゾーン内のトラフィックを許可または拒否するには、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **zone default-zone permit vsan** *vsan-id*	デフォルト ゾーン メンバへのトラフィック フローを許可します。
	switch(config)# **no zone default-zone permit vsan** *vsan-id*	デフォルト ゾーン メンバへのトラフィック フローを拒否し、出荷時の設定に戻します。
ステップ 3	switch(config)# **zone commit vsan** *vsan-id*	指定された VSAN に対する変更をコミットします。

システムのデフォルト ゾーン分割設定値の設定

スイッチ上の新しい VSAN のデフォルトのゾーン ポリシーおよびフル ゾーン配信のデフォルト設定値を設定できます。スイッチ全体のデフォルト設定値を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **system default zone default-zone permit**	スイッチ上の新しい VSAN のデフォルト ゾーン分割ポリシーとして permit（許可）を設定します。
	switch(config)# **no system default zone default-zone permit**	スイッチ上の新しい VSAN のデフォルト ゾーン分割ポリシーとして deny（拒否）（デフォルト）を設定します。

	コマンド	目的
ステップ 3	switch(config)# **system default zone distribute full**	スイッチ上の新しい VSAN のデフォルトとして、フル ゾーン データベース配信をイネーブルにします。
ステップ 4	switch(config)# **no system default zone distribute full**	スイッチ上の新しい VSAN のデフォルトとして、フル ゾーン データベース配信をディセーブル（デフォルト）にします。アクティブ ゾーン データベースだけが配信されます。

（注）　VSAN 1 はデフォルト VSAN であり、常にスイッチ上に存在するため、**system default zone** コマンドは VSAN 1 に対しては無効です。

拡張ゾーン情報の確認

次に、指定された VSAN のゾーン ステータスを表示する例を示します。

```
switch# show zone status vsan 2
```

ゾーン データベースの圧縮

過剰なゾーンを削除し、VSAN のゾーン データベースを圧縮できます。

（注）　スイッチが VSAN あたり 2000 を超えるゾーンをサポートしていても、ネイバーがサポートしていない場合、結合は失敗します。また、そのスイッチが VSAN あたり 2000 を超えるゾーンをサポートしていても、ファブリック内のすべてのスイッチが VSAN あたり 2000 を超えるゾーンをサポートしていない場合には、ゾーン セットのアクティブ化に失敗することがあります。

VSAN のゾーンを削除して、ゾーン データベースを圧縮するには、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **configuration terminal** switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **no zone name** *zone-name* **vsan** *vsan-id*	ゾーンを削除し、ゾーン数を 2000 以下にします。
ステップ 3	switch(config)# **zone compact vsan** *vsan-id*	指定された VSAN のゾーン データベースを圧縮し、ゾーンが削除されたときに開放されたゾーン ID を回復します。

ゾーンおよびゾーン セットの分析

スイッチ上のゾーンおよびゾーン セットをより的確に管理するために、**show zone analysis** コマンドを使用して、ゾーン情報とゾーン セット情報を表示できます。

次に、フル ゾーン分割の分析を表示する例を示します。

```
switch# show zone analysis vsan 1
```

次に、アクティブ ゾーニングの分析を表示する例を示します。

```
switch# show zone analysis active vsan 1
```

コマンド出力に表示される情報の詳細については、『*Cisco Nexus 5000 シリーズ Switch Command Reference*』を参照してください。

デフォルト設定

表 38-4 に、基本ゾーン パラメータのデフォルト設定値を示します。

表 38-4　デフォルトの基本ゾーン パラメータ

パラメータ	デフォルト
デフォルト ゾーン ポリシー	すべてのメンバで拒否
フル ゾーン セット配信	フル ゾーン セットは配信されない
拡張ゾーン分割	ディセーブル

CHAPTER 39

DDAS

Cisco Nexus 5000 シリーズのスイッチは、ファブリック規模単位で分散デバイス エイリアス サービス（デバイス エイリアス）をサポートします。

この章は、次の項で構成されています。

- デバイス エイリアスの概要（39-1 ページ）
- デバイス エイリアス データベース（39-3 ページ）
- レガシー ゾーン エイリアスの設定について（39-8 ページ）
- データベース マージに関するガイドライン（39-9 ページ）
- デバイス エイリアス設定の確認（39-9 ページ）
- デフォルト設定（39-10 ページ）

デバイス エイリアスの概要

Cisco Nexus 5000 シリーズ スイッチで（ゾーン分割、Dynamic Port VSAN Membership [DPVN]、ポート セキュリティなど）異なる機能を設定するためにデバイスのポート WWN（pWWN）が指定されている必要がある場合、設定を行うたびに適切なデバイス名を割り当てなければなりません。デバイス名が間違っていると、予期しない結果を引き起こす可能性があります。pWWN にわかりやすい名前を定義し、必要とされるすべてのコンフィギュレーション コマンドでこの名前を使用すれば、こうした問題を回避できます。このようなわかりやすい名前を*デバイス エイリアス*と呼びます。

この項では、次のトピックについて取り上げます。

- デバイス エイリアスの特徴（39-1 ページ）
- デバイス エイリアスの要件（39-2 ページ）
- ゾーン エイリアスとデバイス エイリアス（39-2 ページ）

デバイス エイリアスの特徴

デバイス エイリアスには、次のような特徴があります。

- デバイス エイリアス情報は、VSAN 設定とは無関係です。
- デバイス エイリアス設定および配布は、ゾーン サーバおよびゾーン サーバ データベースとは無関係です。

- データを失うことなく、従来のゾーン エイリアス設定をインポートできます。
- デバイス エイリアス アプリケーションは Cisco Fabric Services（CFS）インフラストラクチャを使用して、効率的なデータベースの管理および配布を実現します。デバイス エイリアスは、協調型配布モードおよびファブリック規模の配布範囲を使用します（第 21 章「CFS の使用」を参照）。
- 基本モードと拡張モード。「デバイス エイリアスのモード」セクション（39-4 ページ）を参照してください。
- ゾーン、IVR ゾーン、またはポート セキュリティ機能を設定するために使用されたデバイス エイリアスは、それぞれの pWWN と一緒に、**show** コマンド出力に自動的に表示されます。

デバイス エイリアスの要件

デバイス エイリアスには、次の要件があります。

- デバイス エイリアスを割り当てることができるのは pWWN だけです。
- pWWN とマッピングされるデバイス エイリアスは、1 対 1 の関係である必要があります。
- デバイス エイリアス名には、最大 64 文字の英数字を使用でき、次の文字を 1 つまたは複数加えることができます。
  - a ～ z および A ～ Z
  - デバイス エイリアス名は、先頭の文字が英数字である必要があります（a ～ z または A ～ Z）。
  - 1 ～ 9
  - -（ハイフン）および _（下線）
  - $（ドル記号）および ^（キャレット）記号

ゾーン エイリアスとデバイス エイリアス

表 39-1 に、ゾーンベースのエイリアス設定とデバイス エイリアス設定の違いを示します。

表 39-1　ゾーン エイリアスとデバイス エイリアスの比較

ゾーン ベースのエイリアス	デバイス エイリアス
エイリアスは指定した VSAN に限定されます。	VSAN 番号を指定せずにデバイス エイリアスを定義できます。また、同一の定義を何の制約もなく 1 つまたは複数の VSAN で使用できます。
ゾーン エイリアスは、ゾーン分割設定の一部です。他の機能の設定にはエイリアス マッピングを使用できません。	pWWN を使用するすべての機能にデバイス エイリアスを使用できます。
エンド デバイスを指定するのにすべてのゾーン メンバ タイプを使用できます。	pWWN だけがサポートされます。
設定はゾーン サーバ データベース内に含まれ、他の機能では使用できません。	デバイス エイリアスは、ゾーン分割に限定されていません。デバイス エイリアス設定を FCNS、ゾーン、fcping、および traceroute アプリケーションで使用することができます。

デバイス エイリアス データベース

デバイス エイリアス機能は 2 つのデータベースを使用して、デバイス エイリアス設定を受け入れ、実装します。

- 有効なデータベース：ファブリックが現在使用しているデータベース
- 保留中のデータベース：保留中のデバイス エイリアス設定の変更は保留中のデータベースに保存されます。

デバイス エイリアス設定を変更する場合、変更している間はファブリックがロックされたままの状態なので、変更をコミットまたは廃棄する必要があります。

デバイス エイリアス データベースの変更は、アプリケーションによって検証されます。いずれかのアプリケーションがデバイス エイリアス データベースの変更を受け入れることができない場合、これらの変更は拒否されます。これは、コミットまたは結合の操作によって行われたデバイス エイリアス データベースの変更に適用されます。

この項では、次のトピックについて取り上げます。

- デバイス エイリアスの作成（39-3 ページ）
- デバイス エイリアスのモード（39-4 ページ）
- デバイス エイリアス モードの変更時の注意事項（39-4 ページ）
- デバイス エイリアス モードの設定（39-5 ページ）
- デバイス エイリアスの配布について（39-6 ページ）
- ファブリックのロック（39-6 ページ）
- 変更のコミット（39-6 ページ）
- 変更の廃棄（39-7 ページ）
- ファブリックのロックの上書き（39-7 ページ）
- デバイス エイリアスの配布のディセーブル化とイネーブル化（39-8 ページ）

デバイス エイリアスの作成

保留データベースにデバイス エイリアスを作成する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# device-alias database` `switch(config-device-alias-db)#`	保留データベース コンフィギュレーション サブモードを開始します。

	コマンド	目的
ステップ 3	`switch(config-device-alias-db)# device-alias name device-name pwwn pwwn-id`	pWWN によって識別されるデバイスのデバイス名を指定します。これが最初に入力されたデバイス エイリアス コンフィギュレーション コマンドであるため、保留データベースへの書き込みを開始し、同時にファブリックをロックします。
	`switch(config-device-alias-db)# no device-alias name device-name`	pWWN によって識別されるデバイスのデバイス名を削除します。
	`switch(config-device-alias-db)# device-alias rename old-device-name new-device-name`	既存のデバイス エイリアスを新しい名前に変更します。

デバイス エイリアス設定を表示するには、**show device-alias name** コマンドを使用します。

```
switch# show device-alias name x
device-alias name x pwwn 21:01:00:e0:8b:2e:80:93
```

デバイス エイリアスのモード

エイリアスが基本モードまたは拡張モードで動作するように指定できます。

基本モード（デフォルト モード）で動作する場合、デバイス エイリアスはすぐに pWWN に展開されます。基本モードで、デバイス エイリアスがたとえば新しい Host Bus Adapter（HBA）を指定するように変更された場合、その変更はゾーン サーバには反映されません。ユーザは以前の HBA の pWWN を削除して新しい HBA の pWWN を追加し、ゾーンセットを再度アクティブ化する必要があります。

拡張モードで動作する場合、アプリケーションは「ネイティブ」形式でのデバイス エイリアス名を受け入れます。デバイス エイリアスを pWWN に展開する代わりに、デバイス エイリアス名が設定に保存され、ネイティブ デバイス エイリアス形式で配布されます。このため、ゾーン サーバ、PSM、または DPVM などのアプリケーションは、自動的にデバイス エイリアス メンバーシップの変更を追跡し、それに応じて変更を実行します。拡張モードでの動作の主な利点は、変更の実施を 1 カ所で行えるということです。

デバイス エイリアス モードを変更すると、デバイス エイリアスの配布がイネーブルまたはオンの場合にだけ、変更がネットワーク内のほかのスイッチに配布されます。イネーブルまたはオン以外の場合、モード変更はローカル スイッチでだけ行われます。

（注）　拡張モードまたはネイティブ デバイス エイリアス ベースの設定は、interop モードの VSAN では受け入れられません。対応するゾーンにネイティブ デバイス エイリアス ベースのメンバがある場合、IVR ゾーンセットのアクティベーションは interop モードの VSAN で失敗します。

デバイス エイリアス モードの変更時の注意事項

デバイス エイリアス モードを変更する場合は、次の注意事項に従ってください。

- 異なるデバイス エイリアス モードで稼働している 2 つのファブリックが結合されると、デバイス エイリアスの結合は失敗します。結合プロセス中、一方のモードまたは他方のモードに自動的に変換できません。このような状況では、どちらか一方のモードを選択する必要があります。

- 拡張モードから基本モードに変更する前に、最初にローカル スイッチとリモート スイッチの両方からすべてのネイティブ デバイス エイリアス ベースの設定を明示的に削除するか、またはすべてのデバイス エイリアス ベース設定のメンバを対応する pWWN に置き換える必要があります。
- デバイス エイリアス データベースからデバイス エイリアスを削除すると、すべてのアプリケーションは対応するデバイス エイリアスの実行を自動的に中止します。対応するデバイス エイリアスがアクティブなゾーンセットの一部である場合、その pWWN を出入りするすべてのトラフックが中断されます。
- デバイス エイリアス名を変更すると、デバイス エイリアス データベース内のデバイス エイリアス名が変更されるだけでなく、すべてのアプリケーションの対応するデバイス エイリアス設定も置き換えられます。
- デバイス エイリアス データベースに新しいデバイス エイリアスが追加され、そのデバイス エイリアスにアプリケーション設定が存在する場合、設定は自動的に有効になります。たとえば、対応するデバイス エイリアスがアクティブなゾーンセットの一部で、デバイスがオンラインの場合、ゾーン分割が自動的に実行されます。ゾーンセットを再度アクティブ化する必要はありません。
- デバイス エイリアス名が新しい HBA の pWWN にマッピングされると、それに応じてアプリケーションの適用方法が変更されます。この場合、ゾーン サーバは、新しい HBA の pWWN に基づいて自動的にゾーン分割を適用します。

デバイス エイリアス モードの設定

デバイス エイリアスが拡張モードで動作するように設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# device-alias mode enhanced` `switch(config)#`	拡張モードで動作するデバイス エイリアスを割り当てます。
	`switch(config)# no device-alias mode enhance`	基本モードで動作するデバイス エイリアスを割り当てます。

現在のデバイス エイリアス モード設定を表示するには、**show device-alias status** コマンドを入力します。

```
switch# show device-alias status
Fabric Distribution: Enabled
Database:- Device Aliases 0  Mode: Basic
Locked By:- User "admin" SWWN 20:00:00:0d:ec:30:90:40
Pending Database:- Device Aliases 0  Mode: Basic
```

デバイス エイリアスの配布について

デフォルトでは、デバイス エイリアスの配布はイネーブルになっています。デバイス エイリアス機能は CFS を使用して、ファブリック内のすべてのスイッチに変更内容を配布します。

デバイス エイリアスの配布がディセーブルの場合、データベースの変更内容はファブリック内のスイッチに配布されません。ファブリック内のすべてのスイッチで同じ変更を手動で行い、デバイス エイリアス データベースを最新の状態に維持する必要があります。すぐにデータベースの変更が行われるので、保留中のデータベースおよびコミットまたは中断の操作はありません。変更をコミットしていない状態で配布をディセーブルにすると、コミット作業は失敗します。

次に、失敗したデバイス エイリアスのステータスを表示する例を示します。

```
switch# show device-alias status
Fabric Distribution: Disabled
Database:- Device Aliases 25
Status of the last CFS operation issued from this switch:
==========================================================
Operation: Commit
Status: Failed (Reason: Operation is not permitted as the fabric distribution is
 currently disabled.)
```

ファブリックのロック

デバイス エイリアス設定作業を行うと（どのデバイス エイリアス作業かに関係なく）、ファブリックはデバイス エイリアス機能に対して自動的にロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザがこの機能の設定に変更を加えることができなくなります。
- 有効なデータベースのコピーが取得され、保留データベースとして使用されます。保留中のデータベースに対して、以降の変更が行われます。保留中のデータベースへの変更内容をコミットまたは廃棄（中断）するまで、保留中のデータベースは使用されます。

変更のコミット

保留中のデータベースに行われた変更内容をコミットした場合、次のイベントが発生します。

1. 有効なデータベースの内容が、保留中のデータベースの内容に上書きされます。
2. 保留中のデータベースがファブリック内のスイッチに配布され、これらのスイッチの有効なデータベースが新しい変更内容に上書きされます。
3. 保留中のデータベースの内容が空になります。
4. ファブリック ロックがこの機能に対して解除されます。

変更内容をコミットする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# device-alias commit`	現在アクティブなセッションに対する変更をコミットします。

変更の廃棄

保留中のデータベースで行われた変更内容を廃棄した場合、次のイベントが発生します。

1. 有効なデータベースの内容は影響を受けません。
2. 保留中のデータベースの内容が空になります。
3. ファブリック ロックがこの機能に対して解除されます。

デバイス エイリアス セッションを廃棄する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configuration terminal** switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **device-alias abort**	現在アクティブなセッションを廃棄します。

廃棄操作のステータスを表示するには、show **device alias status** コマンドを使用します。

```
switch# show device-alias status
Fabric Distribution: Enabled
Database:- Device Aliases 24
Status of the last CFS operation issued from this switch:
==========================================================
Operation: Abort
Status: Success
```

ファブリックのロックの上書き

ロック操作（クリア、コミット、中断）は、デバイス エイリアスの配布がイネーブルの場合にだけ使用できます。ユーザがデバイス エイリアス作業を行ったが、変更のコミットや廃棄を行ってロックを解除するのを忘れていた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこの操作を行うと、ユーザによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。

ヒント　スイッチを再起動した場合、変更は volatile ディレクトリでだけ使用でき、また廃棄される場合もあります。

管理者の権限を使用して、ロックされたデバイス エイリアス セッションを解除するには、EXEC モードで **clear device-alias session** コマンドを使用します。

```
switch# clear device-alias session
```

クリア操作のステータスを表示するには、**show device-alias status** コマンドを使用します。

```
switch# show device-alias status
Fabric Distribution: Enabled
Database:- Device Aliases 24
Status of the last CFS operation issued from this switch:
==========================================================
Operation: Clear Session <--------------------管理者によって解除されたロック
Status: Success <------------------------------ 操作の正常なステータス
```

デバイス エイリアスの配布のディセーブル化とイネーブル化

デバイス エイリアスの配布をディセーブルまたはイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# no device-alias distribute`	配布をディセーブルにします。
	`switch(config)# device-alias distribute`	配布をイネーブルにします(デフォルト)。

デバイス エイリアス配布のステータスを表示するには、**show device-alias status** コマンドを使用します。次に、配布がイネーブルな場合のデバイス エイリアスの表示例を示します。

```
switch# show device-alias status
Fabric Distribution: Enabled <-----------------------------配布がイネーブル
Database:-Device Aliases 24
Locked By:-User "Test" SWWN 20:00:00:0c:cf:f4:02:83<-ロック所有者のユーザ名とスイッチ ID
Pending Database:- Device Aliases 24
Status of the last CFS operation issued from this switch:
==========================================================
Operation: Enable Fabric Distribution
Status: Success
```

次に、配布がディセーブルな場合のデバイス エイリアスの表示例を示します。

```
switch# show device-alias status
Fabric Distribution: Disabled
Database:- Device Aliases 24
Status of the last CFS operation issued from this switch:
==========================================================
Operation: Disable Fabric Distribution
Status: Success
```

レガシー ゾーン エイリアスの設定について

次の制約事項を満たす場合、レガシー ゾーン エイリアス設定をインポートし、データを失うことなくこの機能を使用できます。

- 各ゾーン エイリアスには、メンバが 1 つだけあります。
- メンバのタイプは pWWN です。

名前または定義の競合が存在する場合、ゾーン エイリアスはインポートされません。

ヒント　設定に応じて、必要とされるゾーン エイリアスをデバイス エイリアス データベースにコピーしてください。

インポート操作が終了し、**commit** 操作を行うと、変更されたエイリアス データベースが物理ファブリック内のほかのすべてのスイッチに配布されます。ファブリック内のほかのスイッチに設定を配布したくない場合、**abort** 操作を行うと、マージの変更内容が完全に廃棄されます。

ゾーン エイリアスのインポート

特定の VSAN のゾーン エイリアスをインポートする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# device-alias import fcalias vsan vlan-id`	指定された VSAN の fcalias 情報をインポートします。

データベース マージに関するガイドライン

2 つのデバイス エイリアス データベースを結合する場合は、次の注意事項に従ってください。

- 名前が異なる 2 つのデバイス エイリアスが同一の pWWN にマッピングされていないことを確認します。
- 2 つの同一の pWWN が 2 つの異なるデバイス エイリアスにマッピングされていないことを確認します。
- 両方のデータベースのデバイス エイリアスの合計数が、Cisco MDS SAN-OS Release 3.0（x）以前が稼働しているファブリックでは 8K（8191 個のデバイス エイリアス）、Cisco MDS SAN-OS Release 3.1（x）以降が稼働しているファブリックでは 20K を超えていないことを確認します。

  両方のデータベースのデバイス エントリの合計数がサポートされる設定制限値を超えた場合、結合は失敗します。たとえば、データベース N に 6000 個のデバイス エイリアス、データベース M に 2192 個のデバイス エイリアスがあり、SAN-OS 3.0(x) 以前が稼働している場合、この結合操作は失敗します。デバイス エイリアス モードが一致していない場合も、結合操作は失敗します。

詳細は、「CFS 結合のサポート」セクション（21-6 ページ）を参照してください。

デバイス エイリアス設定の確認

デバイス エイリアス情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
`switch# show zoneset [active]`	ゾーン セット情報のデバイス エイリアスを表示します。
`switch# show device-alias database [pending | pending-diffs]`	デバイスエイリアスデータベースを表示します。
`switch# show device-alias pwwn pwwn-id |name device-name [pending]`	指定された pWWN またはエイリアスのデバイス エイリアス情報を表示します。
`switch# show flogi database [pending]`	FLOGI データベースのデバイス エイリアス情報を表示します。
`switch# show fcns database [pending]`	FCNS データベースのデバイス エイリアス情報を表示します。

次に、ゾーン セット内のデバイス エイリアス情報を表示する例を示します。

```
switch# show zoneset
zoneset name s1 vsan 1
  zone name z1 vsan 1
    pwwn 21:01:00:e0:8b:2e:80:93 [x] <---------------各 pWWN に対して表示されるデバイス
                                                     エイリアス
    pwwn 21:00:00:20:37:39:ab:5f [y]

  zone name z2 vsan 1
    pwwn 21:00:00:e0:8b:0b:66:56 [SampleName]
    pwwn 21:00:00:20:37:39:ac:0d [z]
```

次に、デバイス エイリアス データベース内の保留中の変更内容を表示する例を示します。

```
switch# show device-alias database pending
```

次に、デバイス エイリアス データベース内の特定の pWWN を表示する例を示します。

```
switch# show device-alias pwwn 21:01:00:e0:8b:2e:80:93 pending
```

次に、保留中のデバイス エイリアス データベースと有効なデバイス エイリアス データベースの相違点を表示する例を示します。

```
switch# show device-alias database pending-diff
- device-alias name Doc pwwn 21:01:02:03:00:01:01:01
+ device-alias name SampleName pwwn 21:00:00:e0:8b:0b:66:56
```

デバイス エイリアスは、使用可能な場合、**device-alias** コマンドまたはゾーン固有の **member pwwn** コマンドを使用して設定されるメンバに関係なく表示されます。

デフォルト設定

表 39-2 に、デバイス エイリアス パラメータのデフォルト設定値を示します。

表 39-2　デフォルトのデバイス エイリアス パラメータ

パラメータ	デフォルト
デバイス エイリアスの配布	イネーブル
デバイス エイリアスのモード	基本
使用中のデータベース	有効なデータベース
変更を受け入れるデータベース	保留中のデータベース
デバイスエイリアスファブリックロックの状態	最初のデバイス エイリアス作業でロックされる

CHAPTER 40

ファイバ チャネル ルーティング サービスおよびプロトコルの設定

Fabric Shortest Path First（FSPF）は、ファイバ チャネル ファブリックで使用される標準パス選択プロトコルです。FSPF 機能は、Cisco Nexus 5000 シリーズ スイッチの E モードおよび TE モードのファイバ チャネル インターフェイスでデフォルトでイネーブルです。特殊な考慮事項を必要とする設定を除き、FSPF サービスを設定する必要はありません。FSPF はファブリック内の任意の 2 つのスイッチ間の最適パスを自動的に計算します。FSPF は次の機能を提供します。

- 任意の 2 つのスイッチ間に最短で最速のパスを確立して、ファブリック全体で動的にルートを計算します。
- 特定のパスに障害が発生したときに代替パスを選択します。FSPF は複数のパスをサポートし、障害リンクを迂回する代替パスを自動的に計算します。同等な 2 つのパスが使用可能な場合は、推奨ルートが提供されます。

この章では、ファイバ チャネル ルーティング サービスおよびプロトコルの詳細について説明します。内容は次のとおりです。

- FSPF に関する情報（40-1 ページ）
- FSPF のグローバル設定（40-3 ページ）
- FSPF インターフェイスの設定（40-5 ページ）
- FSPF ルート（40-9 ページ）
- 順序どおりの配信（40-10 ページ）
- フロー統計情報の設定（40-14 ページ）
- デフォルト設定（40-16 ページ）

FSPF に関する情報

FSPF は、ファイバ チャネル ネットワーク内でのルーティング用として、T11 委員会によって現在標準化されているプロトコルです。FSPF プロトコルには、次の特性および特徴があります。

- 複数パスのルーティングをサポートします。
- パス ステータスはリンク ステート プロトコルによって決まります。
- ドメイン ID だけに基づいて、ホップ単位ルーティングを行います。
- E ポートまたは TE ポートだけで稼働し、ループのないトポロジを形成します。

- VSAN（仮想 SAN）単位で稼働します。ファブリック内の各 VSAN では、この VSAN に設定されたスイッチとの接続が保証されます。
- トポロジ データベースを使用して、ファブリック内のすべてのスイッチのリンク ステートを追跡し、各リンクにコストを対応付けます。
- トポロジが変更された場合、高速な再コンバージェンス タイムを保証します。標準ダイクストラ アルゴリズムを使用します。ただし、より強固で、効率的な差分ダイクストラ アルゴリズムを静的に、あるいは動的に選択することができます。VSAN 単位でルートが計算されるため、再コンバージェンス タイムは高速かつ効率的です。

FSPF の例

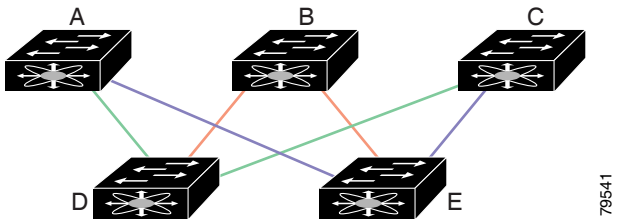
ここでは、FSPF の利点を示すトポロジおよびアプリケーション例について説明します。

（注）　FSPF 機能は任意のトポロジで使用できます。

フォールト トレラント ファブリックの例

図 40-1 に、部分的メッシュ トポロジを使用するフォールト トレラント ファブリックを示します。ファブリック内のどの部分でリンク ダウンが発生しても、各スイッチはファブリック内の他のすべてのスイッチと通信できます。同様に、どのスイッチがダウンしても、ファブリックの残りの接続は維持されます。

図 40-1　　フォールト トレラント ファブリック



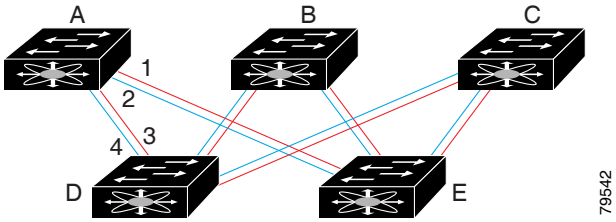
たとえば、すべてのリンク速度が等しい場合、FSPF は A ～ C 2 つの同等なパス（A-D-C（緑）と A-E-C（青））を計算します。

冗長リンクの例

図 40-1 のトポロジを改善するには、任意のスイッチ ペア間の接続をそれぞれ複製します。スイッチ ペア間には複数のリンクを設定できます。図 40-2 に、この配置例を示します。Cisco Nexus 5000 シリーズ スイッチはポート チャネルをサポートしているので、FSPF プロトコルは物理リンクのペアをそれぞれ単一の論理リンクとして認識できます。

物理リンク ペアをバンドルすることにより、データベース サイズは小さくなり、リンク アップデート頻度が減少するため、FSPF の効率が大幅に改善されます。物理リンクが集約されると、障害は単一リンクでなく、SAN ポート チャネル全体に対応付けられます。この設定により、ネットワークの復元力も向上します。SAN ポート チャネル内にリンク障害が発生してもルートが変更されないため、ルーティング ループ、トラフィックの消失、またはルート再設定によるファブリック ダウンタイムが生じるリスクが軽減されます。

図 40-2　　冗長リンクを持つフォールト トレラント ファブリック



たとえば、すべてのリンク速度が等しく、SAN ポート チャネルが存在しない場合、FSPF は A ～ C の 4 つの同等のパス（A1-E-C、A2-E-C、A3-D-C、A4-D-C）を計算します。SAN ポート チャネルが存在する場合は、このパス数は 2 つとなります。

FSPF のグローバル設定

デフォルトでは、Cisco Nexus 5000 シリーズ スイッチの FSPF はイネーブルになっています。

一部の FSPF 機能は、VSAN ごとにグローバルに設定できます。VSAN 全体に機能を設定すると、コマンドごとに VSAN 番号を指定する必要がなくなります。このグローバル設定機能を使用すると、タイプ ミスや、その他の軽微な設定エラーが発生する可能性も低減されます。

（注） FSPF はデフォルトでイネーブルになっています。通常、これらの高度な機能は設定する必要がありません。

注意 バックボーン リージョンのデフォルトは 0（ゼロ）です。この設定を変更する必要があるのは、デフォルト以外のリージョンを使用する場合だけです。バックボーン リージョンを使用して別のベンダー製品と併用する場合は、これらの製品の設定と互換性が保たれるようにこのデフォルトを変更できます。

この項では、次のトピックについて取り上げます。

- SPF 計算のホールド タイムについて（40-3 ページ）
- Link State Records の概要（40-4 ページ）
- VSAN での FSPF の設定（40-4 ページ）
- FSPF のデフォルト設定へのリセット（40-5 ページ）
- FSPF のイネーブル化またはディセーブル化（40-5 ページ）
- VSAN の FSPF カウンタのクリア（40-5 ページ）

SPF 計算のホールド タイムについて

SPF 計算のホールド タイムは、VSAN での 2 つの連続した SPF 計算間の最小時間に設定されます。これを小さい値に設定すると、VSAN 上のパスの再計算によるファブリックの変更に対して、FSPF の処理が速くなります。SPF 計算のホールド タイムが短いと、スイッチの CPU 時間は長くなります。

Link State Records の概要

ファブリックに新しいスイッチが追加されるたびに、Link State Record（LSR）が近接スイッチに送信されて、ファブリック全体にフラッディングされます。

表 40-1 に、スイッチ応答に関するデフォルト設定を示します。

表 40-1　LSR のデフォルト設定

LSR のオプション	デフォルト	説明
ACK インターバル（RxmtInterval）	5 秒	再送信するまで、スイッチが LSR からの ACK を待機する期間
リフレッシュ タイム（LSRefreshTime）	30 分	LSR リフレッシュを送信するまで、スイッチが待機する期間
最大エージング（MaxAge）	60 分	データベースから LSR を削除するまで、スイッチが待機する期間

LSR の最小着信時間は、この VSAN の LSR アップデートの受信間隔です。LSR の最小着信時間よりも前に着信した LSR アップデートは廃棄されます。

LSR 最小間隔は、このスイッチが VSAN 上の LSR アップデートを送信する頻度です。

VSAN での FSPF の設定

VSAN 全体に FSPF 機能を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fspf config vsan vsan-id`	指定された VSAN に対して FSPF グローバル コンフィギュレーション モードを開始します。
ステップ 3	`switch-config-(fspf-config)# spf static`	ダイナミック（デフォルト）差分 VSAN に対してスタティック SPF 計算を強制実行します。
ステップ 4	`switch-config-(fspf-config)# spf hold-time value`	VSAN 全体に対して、2 つのルート計算間のホールド タイムをミリ秒（msec）単位で設定します。デフォルト値は 0 です **（注）** 指定期間が短いほど、ルーティングは高速化されます。ただし、それに応じて、プロセッサ消費量が増大します。
ステップ 5	`switch-config-(fspf-config)# region region-id`	現在の VSAN に自律リージョンを設定し、リージョン ID を指定します。

FSPF のデフォルト設定へのリセット

FSPF VSAN グローバル設定を工場出荷時のデフォルト設定に戻す手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# no fspf config vsan vsan-id`	指定された VSAN の FSPF 設定を削除します。

FSPF のイネーブル化またはディセーブル化

FSPF ルーティング プロトコルをイネーブルまたはディセーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fspf enable vsan vsan-id`	指定された VSAN 内で FSPF ルーティング プロトコルをイネーブルにします。
	`switch(config)# no fspf enable vsan vsan-id`	指定された VSAN 内で FSPF ルーティング プロトコルをディセーブルにします。

VSAN の FSPF カウンタのクリア

VSAN 全体の FSPF 統計情報カウンタをクリアする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# clear fspf counters vsan vsan-id`	指定された VSAN の FSPF 統計情報カウンタをクリアします。インターフェイス参照番号を指定しない場合は、すべてのカウンタがクリアされます。

FSPF インターフェイスの設定

一部の FSPF コマンドは、インターフェイス単位で使用できます。次に示す設定手順は、特定の VSAN 内の 1 つのインターフェイスに適用されます。

この項では、次のトピックについて取り上げます。

- FSPF リンク コストの概要（40-6 ページ）
- FSPF のリンク コストの設定（40-6 ページ）
- hello タイム インターバルについて（40-6 ページ）
- hello タイム インターバルの設定（40-6 ページ）
- デッド タイム インターバルについて（40-7 ページ）
- デッド タイム インターバルの設定（40-7 ページ）
- 再送信インターバルについて（40-7 ページ）

- 再送信インターバルの設定（40-8 ページ）
- インターフェイス単位での FSPF のディセーブル化（40-8 ページ）
- インターフェイス単位での FSPF のディセーブル化（40-8 ページ）
- インターフェイスの FSPF カウンタのクリア（40-9 ページ）

FSPF リンク コストの概要

FSPF はファブリック内のすべてのスイッチのリンク ステートを追跡し、データベース内の各リンクにコストを対応付け、コストが最小なパスを選択します。インターフェイスに対応付けられたコストを管理上変更して、FSPF ルート選択を実行できます。コストは、1 ～ 65,535 の整数値で指定できます。1 Gbps のデフォルト コストは 1000 であり、2 Gbps では 500 です。

FSPF のリンク コストの設定

FSPF リンク コストを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface fc slot/port` `switch(config-if)#`	指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# fspf cost value vsan vsan-id`	指定された VSAN 内の選択されたインターフェイスにコストを設定します。

hello タイム インターバルについて

FSPF hello タイム インターバルを設定すると、リンク状態を確認するために送信される定期的な hello メッセージの間隔を指定できます。指定できる整数値は 1 ～ 65,535 秒です。

（注）　この値は、ISL の両端のポートで同じでなければなりません。

hello タイム インターバルの設定

FSPF hello タイム インターバルを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface fc slot/port` `switch(config-if)#`	指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	switch(config-if)# **fspf hello-interval** *value* **vsan** *vsan-id* switch(config-if)#	VSAN 175 のリンクのヘルスを確認するために、hello メッセージ インターバルを指定します。デフォルトは 20 秒です。

デッド タイム インターバルについて

FSPF デッド タイム インターバルを設定すると、hello メッセージを受信しなければならない最大間隔を指定できます。この期間が経過すると、ネイバーは消失したと見なされ、データベースから削除されます。指定できる整数値は 1 ～ 65,535 秒です。

（注） この値は、ISL の両端のポートで同じでなければなりません。

注意 設定されたデッド タイム インターバルが hello タイム インターバルより小さい場合は、コマンド プロンプトにエラーが報告されます。

デッド タイム インターバルの設定

FSPF デッド タイム インターバルを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configuration terminal** switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot/port* switch(config-if)#	指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **fspf dead-interval** *value* **vsan** *vsan-id* switch(config-if)#	指定された VSAN に、選択されたインターフェイスで hello メッセージを受信しなければならない最大間隔を指定します。この期間が経過すると、ネイバーは消失したと見なされます。デフォルトは 80 秒です。

再送信インターバルについて

インターフェイス上で未確認応答リンク ステート アップデートを送信するまでの期間を指定します。再送信インターバルを指定する整数値の有効範囲は、1 ～ 65,535 秒です。

（注） この値は、インターフェイスの両端のスイッチで同じでなければなりません。

再送信インターバルの設定

FSPF 再送信タイム インターバルを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface fc slot/port` `switch(config-if)#`	指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# fspf retransmit-interval value vsan vsan-id` `switch(config-if)#`	指定された VSAN の未確認応答リンク ステート アップデートの再送信タイム インターバルを指定します。デフォルトは 5 秒です。

インターフェイス単位での FSPF のディセーブル化

選択したインターフェイスで FSPF プロトコルをディセーブルにできます。デフォルトでは、FSPF はすべての E ポートおよび TE ポートでイネーブルです。このデフォルト設定をディセーブルにするには、インターフェイスをパッシブに設定します。

（注）　プロトコルを機能させるには、インターフェイスの両端で FSPF をイネーブルにする必要があります。

インターフェイス単位での FSPF のディセーブル化

選択したインターフェイスで FSPF プロトコルをディセーブルにできます。デフォルトでは、FSPF はすべての E ポートおよび TE ポートでイネーブルです。このデフォルト設定をディセーブルにするには、インターフェイスをパッシブに設定します。

特定のインターフェイスで FSPF をディセーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface fc slot/port` `switch(config-if)#`	指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# fspf passive vsan vsan-id` `switch(config-if)#`	指定された VSAN 内の特定のインターフェイスに対して FSFP プロトコルをディセーブルにします。
	`switch(config-if)# no fspf passive vsan vsan-id` `switch(config-if)#`	指定された VSAN 内の特定のインターフェイスに対して FSFP プロトコルを再度イネーブルにします。

選択したインターフェイスで FSPF プロトコルをディセーブルにできます。デフォルトでは、FSPF はすべての E ポートおよび TE ポートでイネーブルです。このデフォルト設定をディセーブルにするには、インターフェイスをパッシブに設定します。

インターフェイスの FSPF カウンタのクリア

インターフェイスの FSPF 統計情報カウンタをクリアする手順は、次のとおりです。

コマンド	目的
`switch# clear fspf counters vsan vsan-id interface fc slot/port`	指定された VSAN 内の指定インターフェイスの FSPF 統計情報カウンタをクリアします。

FSPF ルート

FSPF は、FSPF データベース内のエントリに基づいて、ファブリックを経由するトラフィックをルーティングします。これらのルートは動的に学習させるか、または静的に設定することもできます。

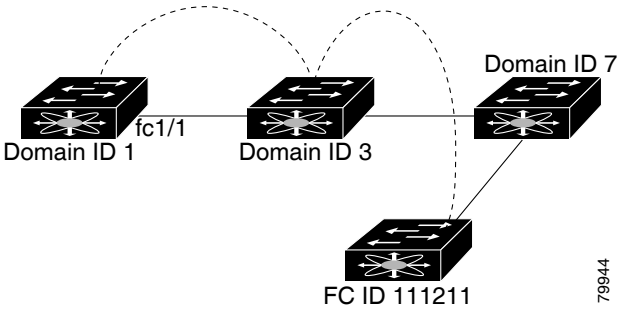
この項では、次のトピックについて取り上げます。

- ファイバ チャネルのルートについて（40-9 ページ）
- ファイバ チャネル ルートの設定（40-10 ページ）

ファイバ チャネルのルートについて

各ポートは、FC ID に基づいてフレームを転送する転送ロジックを実行します。指定されたインターフェイスおよびドメインの FC ID を使用して、ドメイン ID が 1 のスイッチに、指定されたルート（FC ID 111211 やドメイン ID 3 など）を設定できます（図 40-3を参照）。

図 40-3　　ファイバ チャネルのルート



ファイバ チャネル ルートの設定

ファイバ チャネル ルートを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configuration terminal`** `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`fcroute`** *`fcid`* **`interface fc`** *`slot/port`* **`domain`** *`domain-id`* **`vsan`** *`vsan-id`* `switch(config)#`	指定されたファイバ チャネル インターフェイスおよびドメインに対応するルートを設定します。この例では、指定されたインターフェイスに FC ID、およびネクスト ホップ スイッチに対するドメイン ID が割り当てられます。
	`switch(config)#` **`fcroute`** *`fcid`* **`interface san-port-channel`** *`port`* **`domain`** *`domain-id`* **`vsan`** *`vsan-id`* `switch(config)#`	指定された SAN ポート チャネル インターフェイスおよびドメインに対応するルートを設定します。この例では、インターフェイス san-port-channel 1 に FC ID（0x111211）、およびネクスト ホップ スイッチに対するドメイン ID が割り当てられます。
	`switch(config)#` **`fcroute`** *`fcid`* **`interface fc`** *`slot/port`* **`domain`** *`domain-id`* **`metric`** *`value`* **`vsan`** *`vsan-id`* `switch(config-if)#`	特定の FC ID およびネクスト ホップ ドメイン ID に対応するスタティック ルートを設定し、ルートのコストも割り当てます。 リモートの宛先オプションを指定しない場合、デフォルトは direct です。
	`switch(config)#` **`fcroute`** *`fcid`* **`interface fc`** *`slot/port`* **`domain`** *`domain-id`* **`metric`** *`value`* **`remote vsan`** *`vsan-id`*	RIB にスタティック ルートを追加します。このルートがアクティブ ルートであり、FIB[1] レコードに空きがある場合は、FIB にもこのルートが追加されます。 ルートのコスト（メトリック）を指定しない場合、デフォルトは 10 です。
ステップ 3	`switch(config)#` **`fcroute`** *`fcid netmask`* **`interface fc`** *`slot/port`* **`domain`** *`domain-id`* **`vsan`** *`vsan-id`* `switch(config)#`	インターフェイス（または SAN ポート チャネル）に指定されたルートのネットマスクを設定します。3 つのルート（ドメインだけに一致する 0xff0000、ドメインおよびエリアに一致する 0xffff00、およびドメイン、エリア、ポートに一致する 0xffffff）のいずれかを指定できます。

1. FIB = Forwarding Information Base（転送情報ベース）

順序どおりの配信

データ フレームに関して順序どおりの配信（IOD）を行うと、送信元が送信した順番で宛先にフレームが配信されることが保証されます。

一部のファイバ チャネル プロトコルまたはアプリケーションでは、順序外のフレーム配信を処理できません。このような場合、Cisco Nexus 5000 シリーズ スイッチはフレーム フロー内のフレーム順序を保持します。フレームのフローは SID（ソース ID）、DID（宛先 ID）、およびオプションの OX ID（送信元交換 ID）で識別されます。

IOD に対応したスイッチでは、特定の入力ポートで受信され、特定の出力ポートに送信されるすべてのフレームは、常に受信された順番で配信されます。

IOD を使用するのは、順序外のフレーム配信をサポートできない環境の場合だけにしてください。

ヒント　順序どおりの配信機能をイネーブルにすると、グレースフル シャットダウン機能は実行されません。

この項では、次のトピックについて取り上げます。

- ネットワーク フレームの順序変更について（40-11 ページ）
- SAN ポート チャネル フレームの順序変更について（40-12 ページ）
- 順序どおりの配信のイネーブル化の概要（40-12 ページ）
- 順序どおりの配信のグローバルなイネーブル化（40-13 ページ）
- VSAN の順序どおりの配信のイネーブル化（40-13 ページ）
- 順序どおりの配信のステータスの表示（40-13 ページ）
- ドロップ遅延時間の設定（40-14 ページ）
- 遅延情報の表示（40-14 ページ）

ネットワーク フレームの順序変更について

ネットワーク内でルートが変更されると、新しく選択されたパスが元のルートよりも高速になったり、輻輳が軽減されたりすることがあります。

図 40-4　　ルート変更の配信

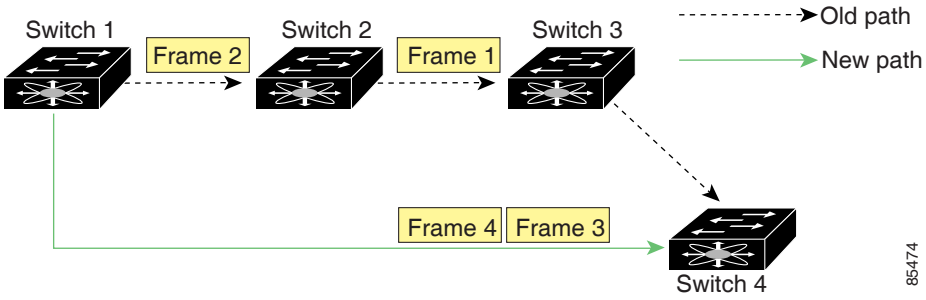


図 40-4 では、スイッチ 1 からスイッチ 4 への新しいパスの方が高速です。したがって、フレーム 3 およびフレーム 4 は、フレーム 1 およびフレーム 2 よりも先に配信されることがあります。

順序保証機能がイネーブルの場合、ネットワーク内のフレームは次のように配信されます。

- ネットワーク内のフレームは送信された順番で配信されます。
- ネットワーク遅延ドロップ期間内に順番どおりに配信できないフレームは、ネットワーク内でドロップされます。

SAN ポート チャネル フレームの順序変更について

SAN ポート チャネル内でリンクが変更されると、同じ交換または同じフローに対応するフレームが、より高速なパスに切り替わることがあります。

図 40-5　　リンクが輻輳している場合の配信

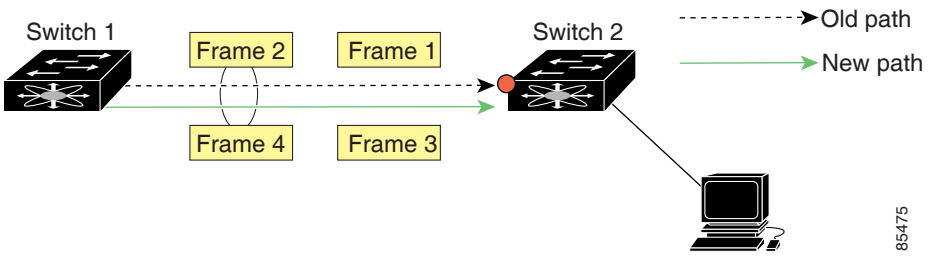


図 40-5 では、元のパス（赤い点線）のポートが輻輳しています。したがって、フレーム 3 およびフレーム 4 は、フレーム 1 およびフレーム 2 よりも先に配信されることがあります。

順序どおりの配信機能がイネーブルになっている場合、ポート チャネル リンクに変更が生じると、その SAN ポート チャネルを通過するフレームは次のように配信されます。

- 古いパスを使用するフレームが配信されてから、新しいフレームが許可されます。
- 新しいフレームは、ネットワーク遅延ドロップ期間が経過して、古いフレームがすべて消去されてから、新しいパスを通して配信されます。

古いパスを経由するフレームをネットワーク遅延ドロップ期間内に順番どおりに配信できない場合は、これらのフレームはドロップされます。「ドロップ遅延時間の設定」セクション（40-14 ページ）を参照してください。

順序どおりの配信のイネーブル化の概要

順序どおりの配信機能は、特定の VSAN またはスイッチ全体に対してイネーブルにできます。順序どおりの配信は、Cisco Nexus 5000 シリーズ スイッチでデフォルトでディセーブルです。

ヒント　この機能をイネーブルにするのは、順序に従わないフレームを処理できないデバイスがスイッチに搭載されている場合に限定してください。Cisco Nexus 5000 シリーズ スイッチ内のロードバランシング アルゴリズムを使用すると、通常のファブリック処理中に、フレームを順序どおりに配信できます。送信元 FC ID、宛先 FC ID、および交換 ID に基づくロードバランシング アルゴリズムをハードウェアで実行しても、パフォーマンスは低下しません。ただし、順序どおりの配信機能がイネーブルの場合にファブリックに障害が発生すると、ファブリック転送が意図的に中断され、順序に従わずに転送される可能性のあるフレームがファブリックから除去されるため、回復が遅れます。

順序どおりの配信のグローバルなイネーブル化

順序どおりの配信パラメータがスイッチ上のすべての VSAN で統一されるように保証するには、順序どおりの配信をグローバルにイネーブルにします。

順序どおりの配信をグローバルにイネーブルにするのは、ファブリック全体にこの機能が必要な場合だけにしてください。そうでない場合は、この機能を必要とする VSAN に対してだけ IOD をイネーブルにします。

スイッチで順序どおりの配信をイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# in-order-guarantee`	スイッチ内で順序どおりの配信をイネーブルにします。
	`switch(config)# no in-order-guarantee`	スイッチを出荷時の設定に戻し、順序どおりの配信機能をディセーブルにします。

VSAN の順序どおりの配信のイネーブル化

VSAN を新しく作成すると、グローバルな順序保証値が自動的に継承されます。新しい VSAN の順序保証をイネーブルまたはディセーブルに設定することにより、このグローバル値を変更できます。

マルチキャスト ツリーの計算に最下位ドメイン スイッチを使用する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# in-order-guarantee vsan` *vsan-id*	指定された VSAN 内で順序どおりの配信をイネーブルにします。
	`switch(config)# no in-order-guarantee vsan` *vsan-id*	スイッチを出荷時のデフォルト設定に戻し、指定された VSAN の順序どおりの配信機能をディセーブルにします。

順序どおりの配信のステータスの表示

現在の設定ステータスを表示するには、**show in-order-guarantee** コマンドを使用します。

```
switch# show in-order-guarantee
global inorder delivery configuration:guaranteed

VSAN specific settings
vsan 1 inorder delivery:guaranteed
vsan 101 inorder delivery:not guaranteed
vsan 1000 inorder delivery:guaranteed
vsan 1001 inorder delivery:guaranteed
vsan 1682 inorder delivery:guaranteed
vsan 2001 inorder delivery:guaranteed
vsan 2009 inorder delivery:guaranteed
vsan 2456 inorder delivery:guaranteed
vsan 3277 inorder delivery:guaranteed
vsan 3451 inorder delivery:guaranteed
vsan 3452 inorder delivery:guaranteed
```

ドロップ遅延時間の設定

ネットワーク、ネットワーク内の指定された VSAN、またはスイッチ全体のデフォルトの遅延時間を変更できます。

ネットワークおよびスイッチのドロップ遅延時間を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fcdroplatency network` *value*	ネットワークのネットワーク ドロップ遅延時間を設定します。有効値は 0 ～ 60000 ミリ秒です。デフォルトは 2000 ミリ秒です。 **（注）** ネットワークのドロップ遅延時間は、ネットワーク内の最長パスのすべてのスイッチ遅延の合計として計算する必要があります。
	`switch(config)# fcdroplatency network` *value* **vsan** *vsan-id*	指定された VSAN のネットワーク ドロップ遅延時間を設定します。
	`switch(config)# no fcdroplatency network` *value*	現在の fcdroplatecy ネットワーク設定を削除し、出荷時の設定に戻します。

遅延情報の表示

show fcdroplatency コマンドを使用して、設定された遅延パラメータを表示できます。次に、ネットワーク遅延情報を表示する例を示します。

```
switch# show fcdroplatency
switch latency value:500 milliseconds
global network latency value:2000 milliseconds

VSAN specific network latency settings
vsan 1 network latency:5000 milliseconds
vsan 2 network latency:2000 milliseconds
vsan 103 network latency:2000 milliseconds
vsan 460 network latency:500 milliseconds
```

フロー統計情報の設定

フロー統計情報は、集約統計情報テーブル内の入力トラフィックをカウントします。次の 2 種類の統計情報を収集できます。

- VSAN のトラフィックをカウントする集約フロー統計情報
- VSAN 内の送信元/宛先 ID ペアに対応するトラフィックをカウントするフロー統計情報。

この項では、次のトピックについて取り上げます。

- フロー統計情報について（40-15 ページ）
- 集約フロー統計情報のカウント（40-15 ページ）
- 個々のフロー統計情報のカウント（40-15 ページ）
- FIB 統計情報のクリア（40-15 ページ）
- フロー統計情報の表示（40-16 ページ）

フロー統計情報について

フロー カウンタをイネーブルにすると、集約フロー統計情報およびフロー統計情報に対して、最大 1000 エントリ をイネーブルにできます。使用されていないフロー インデックスを、各新規フローに割り当てるようにしてください。フロー インデックスの番号の間は、集約フロー統計情報とフロー統計情報間で共有します。

集約フロー統計情報のカウント

VSAN の集約フロー統計情報をカウントする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fcflow stats aggregated index` *value* `vsan` *vsan-id* `switch(config)#`	集約フロー カウンタをイネーブルにします。
	`switch(config)# no fcflow stats aggregated index` *value* `vsan` *vsan-id* `switch(config)#`	集約フロー カウンタをディセーブルにします。

個々のフロー統計情報のカウント

VSAN 内の送信元および宛先 FC ID のフロー統計情報をカウントする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fcflow stats index` *value dest-fcid source-fcid netmask* `vsan` *vsan-id* `switch(config)#`	フロー カウンタをイネーブルにします。 **（注）** ソース ID および宛先 ID は、16 進形式の FC ID（0x123aff など）で指定します。使用できるマスクは、0xff0000 または 0xffffff のどちらかです。
	`switch(config)# no fcflow stats aggregated index` *value* `vsan` *vsan-id* `switch(config)#`	フロー カウンタをディセーブルにします。

FIB 統計情報のクリア

集約フロー カウンタをクリアするには、**clear fcflow stats**コマンドを使用します。次に、集約フロー カウンタをクリアする例を示します。

```
switch# clear fcflow stats aggregated index 1
```

次に、送信元および宛先 FC ID に対応するフロー カウンタをクリアする例を示します。

```
switch# clear fcflow stats index 1
```

フロー統計情報の表示

フロー統計情報を表示するには、**show fcflow stats** コマンドを使用します。次に、集約フロー概要を表示する例を示します。

```
switch# show fcflow stats aggregated
Idx       VSAN     frames
---------- ---------- ----------
         6          1      42871
```

次に、フロー統計情報を表示する例を示します。

```
switch# show fcflow stats
```

次に、フロー インデックスの使用状況を表示する例を示します。

```
switch# show fcflow stats usage
2 flows configured
configured flow : 3,7
7
```

次に、特定の VSAN のグローバル FSPF 情報を表示する例を示します。

```
switch# show fspf vsan 1
```

次に、指定された VSAN の FSPF データベースの概要を表示する例を示します。追加のパラメータを指定しない場合、データベース内のすべての LSR が表示されます。

```
switch# show fspf database vsan 1
```

次に、FSPF インターフェイス情報を表示する例を示します。

```
switch# show fspf vsan 1 interface fc2/1
```

デフォルト設定

表 40-2 に、FSPF 機能のデフォルト設定値を示します。

表 40-2　FSPF のデフォルト設定値

パラメータ	デフォルト
FSPF	すべての E ポートおよび TE ポートでイネーブルです。
SPF 計算	ダイナミック
SPF ホールド タイム	0
バックボーン リージョン	0
ACK インターバル（RxmtInterval）	5 秒
リフレッシュ タイム（LSRefreshTime）	30 分
最大エージング（MaxAge）	60 分
hello 間隔	20 秒
デッド間隔	80 秒
配信ツリー情報	主要スイッチ（ルート ノード）から取得します。
ルーティング テーブル	FSPF は指定された宛先への等コスト パスを 16 まで格納します。

表 40-2　FSPF のデフォルト設定値（続き）

パラメータ	デフォルト
ロード バランシング	複数の等コスト パスの宛先 ID およびソース ID に基づきます。
順序どおりの配信	ディセーブル
ドロップ遅延	ディセーブル
スタティック ルート コスト	ルートのコスト（メトリック）を指定しない場合、デフォルトは 10 です。
リモート宛先スイッチ	リモート宛先スイッチを指定しない場合、デフォルトは、direct です。
マルチキャスト ルーティング	主要スイッチを使用してマルチキャスト ツリーを計算します。

CHAPTER 41

FLOGI、ネーム サーバ、FDMI、および RSCN データベースの管理

この章では、Cisco Nexus 5000 シリーズ スイッチで提供される Fabric Login（FLOGI）データベース、ネーム サーバ機能、Fabric-Device Management Interface（FDMI）、および Registered State Change Notification（RSCN）情報について説明します。内容は次のとおりです。

- ファブリック ログインに関する情報（41-1 ページ）
- ネーム サーバ プロキシ（41-2 ページ）
- FDMI（41-4 ページ）
- FDMI の表示（41-4 ページ）
- RSCN（41-5 ページ）
- デフォルト設定（41-11 ページ）

ファブリック ログインに関する情報

ファイバ チャネル ファブリックでは、ホストまたはディスクごとに FC ID が必要です。FLOGI テーブルにストレージ デバイスが表示されるどうかを確認するには、次の例のように **show flogi** コマンドを使用します。必要なデバイスが FLOGI テーブルに表示されていれば、FLOGI が正常に行われます。ホスト Host Bus Adapter（HBA）および接続ポートに直接接続されているスイッチ上の FLOGI データベースを検査します。

次に、FLOGI テーブルのストレージ デバイスを確認する例を示します。

```
switch# show flogi database
--------------------------------------------------------------------------
INTERFACE  VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------
fc2/3      1     0xb200e2  21:00:00:04:cf:27:25:2c  20:00:00:04:cf:27:25:2c
fc2/3      1     0xb200e1  21:00:00:04:cf:4c:18:61  20:00:00:04:cf:4c:18:61
fc2/3      1     0xb200d1  21:00:00:04:cf:4c:18:64  20:00:00:04:cf:4c:18:64
fc2/3      1     0xb200ce  21:00:00:04:cf:4c:16:fb  20:00:00:04:cf:4c:16:fb
fc2/3      1     0xb200cd  21:00:00:04:cf:4c:18:f7  20:00:00:04:cf:4c:18:f7
vfc3/1     2     0xb30100  10:00:00:05:30:00:49:63  20:00:00:05:30:00:49:5e
Total number of flogi = 6.
```

次に、特定のインターフェイスに接続されたストレージ デバイスを確認する例を示します。

```
switch# show flogi database interface vfc1/1
INTERFACE  VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------
```

```
vfc1/1     1     0x870000  20:00:00:1b:21:06:58:bc  10:00:00:1b:21:06:58:bc

Total number of flogi = 1.
```

次に、VSAN（仮想 SAN）1 に関連付けられたストレージ デバイスを確認する例を示します。

```
switch# show flogi database vsan 1
```

ネーム サーバ プロキシ

ネーム サーバ機能は、各 VSAN 内のすべてのホストおよびストレージ デバイスの属性を含むデータベースを維持します。ネーム サーバでは、情報を最初に登録したデバイスによるデータベース エントリの変更が認められます。

プロキシ機能は、別のデバイスによって登録されたデータベース エントリの内容を変更（更新または削除）する必要がある場合に役立ちます。

この項では、次のトピックについて取り上げます。

- ネーム サーバ プロキシの登録について（41-2 ページ）
- ネーム サーバ プロキシの登録（41-2 ページ）
- 重複 pWWN の拒否について（41-3 ページ）
- 重複 pWWN の拒否（41-3 ページ）
- ネーム サーバ データベース エントリの概要（41-3 ページ）
- ネーム サーバのデータベース エントリの表示（41-3 ページ）

ネーム サーバ プロキシの登録について

ネーム サーバ登録要求はすべて、パラメータが登録または変更されたポートと同じポートから発信されます。同一ポートから送られない場合、要求は拒否されます。

この許可を使用すると、WWN が他のノードに代わって特定のパラメータを登録できるようになります。

ネーム サーバ プロキシの登録

ネーム サーバ プロキシを登録する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configuration terminal`** `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`fcns proxy-port`** *`wwn-id`* **`vsan`** *`vsan-id`*	指定した VSAN のプロキシ ポートを設定します。

重複 pWWN の拒否について

別のデバイスの pWWN を使用した悪意のあるログインまたは偶発的なログインを回避するには、**reject-duplicate-pwwn** オプションをイネーブルにします。このオプションをディセーブルにすると、このような pWWN のファブリックへのログインが許可され、ネーム サーバ データベースにある最初のデバイスと置き換えられます。

重複 pWWN の拒否

重複 pWWN を拒否する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fcns reject-duplicate-pwwn vsan vsan-id`	pWWN がすでに存在する場合は、デバイスがファブリックにログインする際に、デバイスをログアウトします。
	`switch(config)# no fcns reject-duplicate-pwwn vsan vsan-id`	同一の pWWN を持つ新しいデバイスでネーム サーバ データベースにある最初のデバイスのエントリを上書きします（デフォルト）。

ネーム サーバ データベース エントリの概要

ネーム サーバはすべてのホストのネーム エントリを FCNS データベースに保管しています。ネーム サーバは、Nx ポートが他のホストの属性を取得するために（ネーム サーバへの）PLOGI を実行するときに、Nx ポートによる属性の登録を許可します。Nx ポートが明示的または暗黙的にログアウトする時点で、これらの属性は登録解除されます。

マルチスイッチ ファブリック構成では、各スイッチ上で稼働するネーム サーバ インスタンスが分散型データベースで情報を共有します。スイッチごとに 1 つのネーム サーバ プロセスのインスタンスが実行されます。

ネーム サーバのデータベース エントリの表示

次に、すべての VSAN のネーム サーバ データベースを表示する例を示します。

```
switch# show fcns database
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x010000    N     50:06:0b:00:00:10:a7:80                    scsi-fcp fc-gs
0x010001    N     10:00:00:05:30:00:24:63 (Cisco)            ipfc
0x010002    N     50:06:04:82:c3:a0:98:52 (Company 1)        scsi-fcp 250
0x010100    N     21:00:00:e0:8b:02:99:36 (Company A)        scsi-fcp
0x020000    N     21:00:00:e0:8b:08:4b:20 (Company A)
0x020100    N     10:00:00:05:30:00:24:23 (Cisco)         ipfc
0x020200    N     21:01:00:e0:8b:22:99:36 (Company A)        scsi-fcp
```

次に、指定された VSAN のネーム サーバ データベースおよび統計情報を表示する例を示します。

```
switch# show fcns database vsan 1
VSAN 1:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x030001    N     10:00:00:05:30:00:25:a3 (Cisco)         ipfc
0x030101    NL    10:00:00:00:77:99:60:2c (Interphase)
0x030200    N     10:00:00:49:c9:28:c7:01
0xec0001    NL    21:00:00:20:37:a6:be:14 (Seagate)       scsi-fcp

Total number of entries = 4
```

次に、すべての VSAN のネーム サーバ データベースの詳細情報を表示する例を示します。

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

次に、すべての VSAN のネーム サーバ データベースの統計情報を表示する例を示します。

```
switch# show fcns statistics
```

FDMI

Cisco Nexus 5000 シリーズ スイッチは、FC-GS-4 規格で記述されている FDMI 機能をサポートしています。FDMI を使用すると、ファイバ チャネル HBA などのデバイスをインバンド通信によって管理できます。この機能を追加することにより、既存のファイバ チャネル ネーム サーバおよび管理サーバの機能を補完します。

FDMI 機能を使用すると、独自のホスト エージェントをインストールしなくても、スイッチ ソフトウェアによって接続先 HBA およびホスト オペレーティング システムに関する次のような管理情報を抽出できます。

- 製造元、モデル、およびシリアル番号
- ノード名およびノードのシンボリック名
- ハードウェア、ドライバ、およびファームウェアのバージョン
- ホスト オペレーティング システム（OS）の名前およびバージョン番号

FDMI エントリはすべて永続ストレージに保存され、FDMI プロセスを起動した時点で取り出されます。

FDMI の表示

次に、指定された VSAN のすべての HBA の詳細情報を表示する例を示します。

```
switch# show fdmi database detail vsan 1
```

RSCN

Registered State Change Notification（RSCN）は、ファブリック内で行われた変更について各ホストに通知するためのファイバ チャネル サービスです。ホストは（SCR を通じて）ファブリック コントローラに登録することにより、この情報を受信できます。次のいずれかのイベントが発生した場合、適宜通知されます。

- ファブリックへのディスクの加入または脱退
- ネーム サーバの登録変更
- 新しいゾーンの実施
- IP アドレスの変更
- ホストの動作に影響する、その他の同様なイベント

この項では、次のトピックについて取り上げます。

- RSCN 情報について（41-5 ページ）
- RSCN 情報の表示（41-5 ページ）
- multi-pid オプションについて（41-6 ページ）
- multi-pid オプションの設定（41-6 ページ）
- ドメイン フォーマット SW-RSCN の抑制（41-6 ページ）
- RSCN 統計情報のクリア（41-7 ページ）
- RSCN タイマーの設定（41-7 ページ）
- RSCN タイマー設定の確認（41-8 ページ）
- RSCN タイマー設定の配布（41-8 ページ）

RSCN 情報について

スイッチ RSCN（SW-RSCN）は、登録されたホストおよびファブリック内の到達可能なすべてのスイッチに送信されます。

（注） スイッチは RSCN を送信して、登録済みのノードに変更が発生したことを通知します。ネーム サーバに再度クエリーを発行して新しい情報を取得するのは、各ノードの責任範囲です。スイッチが各ノードに送信する RSCN には、変更に関する詳細情報は含まれていません。

RSCN 情報の表示

次に、登録済みデバイス情報を表示する例を示します。

```
switch# show rscn scr-table vsan 1
```

（注） SCR テーブルは設定不可能です。ホストが RSCN 情報と一緒に SCR フレームを送信する場合にかぎり、入力されます。ホストが RSCN 情報を受信しない場合、**show rscn scr-table** コマンドはエントリを返しません。

multi-pid オプションについて

RSCN の **multi-pid**オプションをイネーブルに設定すると、登録済み Nx ポートに対して生成される RSCN に、影響を受けた複数のポート ID が含まれる場合があります。この場合、ゾーン分割ルールを適用してから、影響を受けた複数のポート ID が 1つの RSCN にまとめられます。このオプションをイネーブルにすることによって、RSCN の数を減らすことができます。たとえば、スイッチ 1 に 2 つのディスク（D1、D2）および 1 台のホスト（H）が接続されていると仮定します。ホスト H は、RSCN を受信するように登録済みです。D1、D2、および H は同じゾーンに属します。ディスク D1 および D2 が同時にオンラインである場合、次のどちらかの処理が適用されます。

- スイッチ 1 の **multi-pid** オプションがディセーブル：ホスト H に対して、2 つの RSCN（ディスク D1 とディスク D2 に関して 1 つずつ）が生成されます。
- スイッチ 1 の **multi-pid** オプションがイネーブル：ホスト H に対して単一の RSCN が生成されます。RSCN ペイロードには、影響を受けたポート ID が一覧表示されます（この場合は、D1 と D2 の両方）。

（注）　Nx ポートには、multi-pid RSCN ペイロードをサポートしないものがあります。その場合は、RSCN **multi-pid** オプションをディセーブルにしてください。

multi-pid オプションの設定

multi-pid オプションを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# rscn multi-pid vsan` *vsan-id*	指定された VSAN の RSCN を multi-pid フォーマットで送信します。

ドメイン フォーマット SW-RSCN の抑制

ドメイン フォーマット SW-RSCN は、ローカル スイッチ名またはローカル スイッチ管理 IP アドレスが変更されるとすぐに送信されます。この SW-RSCN は、ISL を介して、他のすべてのドメインおよびスイッチに送信されます。リモート スイッチから、ドメイン フォーマット SW-RSCN を開始したスイッチに対して GMAL コマンドおよび GIELN コマンドを発行すると、変更内容を判別できます。ドメイン フォーマット SW-RSCN によって、一部の他社製の SAN スイッチで問題が発生することがあります。詳細については、次の URL にある『*Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/interoperability/guide/intopgd.html

これらの SW-RSCN の ISL を介した送信を抑制する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# rscn suppress domain-swrscn vsan` *vsan-id*	指定された VSAN のドメイン フォーマット SW-RSCN の送信を抑制します。

（注）　ポート アドレス フォーマット RSCN またはエリア アドレス フォーマット RSCN の送信は抑制できません。

RSCN 統計情報のクリア

カウンタをクリアしたあとに、それらのカウンタを別のイベントに関して表示することができます。たとえば、特定のイベント（ONLINE または OFFLINE イベントなど）で生成された RSCN または SW-RSCN の個数を追跡できます。このような統計情報を利用して、VSAN 内で発生する各イベントへの応答を監視できます。

次に、指定された VSAN の RSCN 統計情報をクリアする例を示します。

```
switch# clear rscn statistics vsan 1
```

RSCN 統計情報をクリアした後、**show rscn statistics** コマンドを使用してクリアされたカウンタを表示できます。

```
switch# show rscn statistics vsan 1
```

RSCN タイマーの設定

RSCN は、VSAN 単位のイベント リスト キューを維持します。RSCN イベントは、生成されると、このキューに入れられます。最初の RSCN イベントがキューに入ると、VSAN 単位のタイマーが始動します。タイムアウトになると、すべてのイベントがキューから出され、結合 RSCN が登録済みユーザに送信されます。デフォルトのタイマー値の場合に、登録済みユーザに送信される結合 RSCN の数が最小になります。配置によっては、ファブリック内の変更を追跡するために、イベント タイマー値をさらに小さくする必要が生じることがあります。

（注） RSCN タイマー値は、VSAN 内のすべてのスイッチで同一にする必要があります。「RSCN タイマー設定の配布」セクション（41-8 ページ）を参照してください。

（注） ダウングレードを実行する場合は、事前に、ネットワーク内の RCSN タイマー値をデフォルト値に戻してください。デフォルト値に戻しておかないと、VSAN およびその他のデバイスを経由するリンクがディセーブルになります。

RSCN タイマーを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# rscn distribute`	RSCN タイマーの設定の配布をイネーブルにします。
ステップ 3	`switch(config)# rscn event-tov` *timeout* `vsan` *vsan-id*	指定した VSAN のイベント タイムアウト値（ミリ秒）を設定します。有効値は 0 ～ 2000 ミリ秒です。値をゼロ（0）に設定すると、タイマーはディセーブルになります。
	`switch(config)# no rscn event-tov` *timeout* `vsan` *vsan-id*	デフォルト値（ファイバ チャネル VSAN の場合、2000 ミリ秒）に戻します。
ステップ 4	`switch(config)# rscn commit vsan` *vsan-id*	配布する RSCN タイマー設定を指定された VSAN 内のスイッチにコミットします。

この例では、VSAN 12 のイベント タイムアウト値は 300 ミリ秒に設定されます。

```
switch# rscn event-tov 300 vsan 12
```

RSCN タイマー設定の確認

RSCN タイマー設定を確認するには、**show rscn event-tov vsan** コマンドを使用します。次に、VSAN 10 の RSCN 統計情報をクリアする例を示します。

```
switch# show rscn event-tov vsan 10
Event TOV : 1000 ms
```

RSCN タイマー設定の配布

各スイッチのタイムアウト値は、手動で設定されるため、異なるスイッチが別々の時間にタイムアウトになると、誤設定が生じます。つまり、ネットワーク内の異なる N ポートが別々の時間に RSCN を受信してしまうことがあります。Cisco Fabric Service（CFS）インフラストラクチャでは、RSCN タイマー設定情報をファブリック内のすべてのスイッチに自動的に配布することで、この状況を解消します。また、SW-RSCN の数も削減します。詳細は、第 21 章「CFS の使用」を参照してください。

RSCN は、配布と非配布の 2 つのモードをサポートしています。配布モードでは、RSCN は CFS を使用して、ファブリック内のすべてのスイッチに設定を配布します。非配布モードでは、影響を受けるのはローカル スイッチに対するコンフィギュレーション コマンドだけです。

（注）　すべてのコンフィギュレーション コマンドが配布されるわけではありません。配布されるのは、**rscn event-tov** ***tov*** **vsan** ***vsan*** コマンドだけです。

（注）　RSCN タイマー設定だけが配布されます。

RSCN タイマーは、初期化およびスイッチオーバーの実行時に CFS に登録されます。ハイ アベイラビリティを実現するため、RSCN タイマー配布がクラッシュし再起動する場合、またはスイッチオーバーが発生した場合には、クラッシュまたはスイッチオーバーが発生する前の状態から、通常の機能が再開されます。

この項では、次のトピックについて取り上げます。

- RSCN タイマー設定の配布のイネーブル化（41-9 ページ）
- ファブリックのロック（41-9 ページ）
- RSCN タイマー設定の変更のコミット（41-9 ページ）
- RSCN タイマー設定の変更の廃棄（41-9 ページ）
- ロック済みセッションのクリア（41-10 ページ）
- RSCN 設定の配布情報の表示（41-10 ページ）

RSCN タイマー設定の配布のイネーブル化

RSCN タイマー設定の配布をイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# rscn distribute`	RSCN タイマーの設定の配布をイネーブルにします。
	`switch(config)# no rscn distribute`	RSCN タイマーの配布をディセーブル（デフォルト）にします。

ファブリックのロック

データベースを変更するときの最初のアクションによって、保留中のデータベースが作成され、VSAN 内の機能がロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザがこの機能の設定に変更を加えることができなくなります。
- コンフィギュレーション データベースのコピーが、最初のアクティブ変更と同時に保留中のデータベースになります。

RSCN タイマー設定の変更のコミット

アクティブ データベースに加えられた変更をコミットする場合、ファブリック内のすべてのスイッチに設定がコミットされます。コミットが正常に行われると、設定の変更がファブリック全体に適用され、ロックが解除されます。

RSCN タイマー設定の変更をコミットする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# rscn commit vsan` *timeout*	RSCN タイマーの変更をコミットします。

RSCN タイマー設定の変更の廃棄

保留中のデータベースに加えられた変更を廃棄（中断）する場合、コンフィギュレーション データベースは影響を受けないまま、ロックが解除されます。

RSCN タイマー設定の変更をコミットする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# rscn abort vsan` *timeout*	RSCN タイマーの変更を廃棄し、保留中のコンフィギュレーション データベースをクリアします。

ロック済みセッションのクリア

RSCN タイマー設定を変更したが、変更をコミットまたは廃棄してロックを解除するのを忘れた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこの操作を行うと、ユーザによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。

ヒント　保留中のデータベースは揮発性ディレクトリでだけ有効で、スイッチが再起動されると廃棄されます。

管理者の特権を使用して、ロックされた RSCN セッションを解除するには、EXECモードで **clear rscn session** コマンドを使用します。次に、VSAN 10 の RSCN セッションをクリアする例を示します。

```
switch# clear rscn session vsan 10
```

RSCN 設定の配布情報の表示

次に、RSCN 設定の配布の登録ステータスを表示する例を示します。

```
switch# show cfs application name rscn

 Enabled        : Yes
 Timeout        : 5s
 Merge Capable  : Yes
 Scope          : Logical
```

（注）　結合対象のファブリックの RSCN タイマー値が異なる場合、結合は失敗します。

次に、設定のコミット時に有効な一連のコンフィギュレーション コマンドを表示する例を示します。

（注）　保留中のデータベースには、既存設定と変更された設定の両方が含まれます。

```
switch# show rscn pending
rscn event-tov 2000 ms vsan 1
rscn event-tov 2000 ms vsan 2
rscn event-tov 300 ms vsan 10
```

次に、保留中の設定とアクティブな設定の違いを表示する例を示します。

```
switch# show rscn pending-diff vsan 10
- rscn event-tov 2000 ms vsan 10
+ rscn event-tov 300 ms vsan 10
```

デフォルト設定

表 41-1 に、RSCN のデフォルト設定値を示します。

表 41-1　デフォルトの RSCN 設定値

パラメータ	デフォルト
RSCN タイマー値	2000 ミリ秒（ファイバ チャネル VSAN）
RSCN タイマー設定の配布	ディセーブル

CHAPTER 42

SCSI ターゲットの検出

この章では、Cisco Nexus 5000 シリーズ スイッチに組み込まれた Small Computer System Interface（SCSI）Logical Unit Number（LUN）検出機能について説明します。内容は次のとおりです。

- SCSI LUN 検出に関する情報（42-1 ページ）
- SCSI LUN 情報の表示（42-3 ページ）

SCSI LUN 検出に関する情報

SCSI ターゲットにはディスク、テープ、およびその他のストレージ デバイスが含まれます。これらのターゲットは、ネーム サーバに LUN を登録しません。

ネーム サーバには、次の理由により、LUN 情報が必要となります。

- ネットワーク管理システム（Network Management System）がアクセスできるように、LUN ストレージ デバイス情報を表示するため。
- デバイスのキャパシティ、シリアル番号、およびデバイス ID 情報を表示するため。
- ネーム サーバにイニシエータおよびターゲット機能を登録するため。

SCSI LUN 検出機能には、ローカル ドメイン コントローラ ファイバ チャネル アドレスが使用されます。この機能はローカル ドメイン コントローラをソース FC ID として使用し、SCSI デバイス上で SCSI INQUIRY、REPORT LUNS、および READ CAPACITY コマンドを実行します。

SCSI LUN 検出機能は、CLI（コマンドライン インターフェイス）または SNMP（簡易ネットワーク管理プロトコル）を通して、オンデマンドで開始されます。近接スイッチが Cisco Nexus 5000 シリーズに属する場合、この情報は近接スイッチとも同期されます。

この項では、次のトピックについて取り上げます。

- SCSI LUN 検出の開始について（42-1 ページ）
- SCSI LUN 検出の開始（42-2 ページ）
- カスタマイズ検出の開始について（42-2 ページ）
- カスタマイズ検出の開始（42-2 ページ）

SCSI LUN 検出の開始について

SCSI LUN 検出はオンデマンドで実行されます。

ネーム サーバ データベース内の Nx ポートのうち、FC4 Type = SCSI_FCP として登録されたものだけが検出されます。

SCSI LUN 検出の開始

SCSI LUN 検出を開始する手順は、次のとおりです。

コマンド	目的
switch# **discover scsi-target** {**custom-list** | **local** | **remote** | **vsan** *vsan-id* **fcid** *fc-id*} **os** {**aix** | **all** | **hpux** | **linux** | **solaris** | **windows**} [**lun** | **target**]	指定されたオペレーティング システム（OS）の SCSI ターゲットを検出します。

次に、すべてのオペレーティング システム（OS）のローカル SCSI ターゲットを検出する例を示します。

```
switch# discover scsi-target local os all
discovery started
```

次に、AIX OS に割り当てられたリモート SCSI ターゲットを検出する例を示します。

```
switch# discover scsi-target remote os aix
discovery started
```

次に、VSAN（仮想 SAN）1 および FC ID 0x9c03d6 に対応する SCSI ターゲットを検出する例を示します。

```
switch# discover scsi-target vsan 1 fcid 0x9c03d6
discover scsi-target vsan 1 fcid 0x9c03d6
VSAN:    1 FCID: 0x9c03d6 PWWN: 00:00:00:00:00:00:00:00
  PRLI RSP: 0x01 SPARM: 0x0012
  SCSI TYPE: 0 NLUNS: 1
  Vendor: Company 4 Model: ST318203FC    Rev: 0004
  Other: 00:00:02:32:8b:00:50:0a
```

次に、Linux OS に割り当てられたカスタマイズ リストから SCSI ターゲットを検出する例を示します。

```
switch# discover scsi-target custom-list os linux
discovery started
```

カスタマイズ検出の開始について

カスタマイズ検出は、検出を開始するように選択的に設定された VSAN とドメインのペア リストによって行われます。この検出を開始するには、**custom-list** オプションを使用します。ドメイン ID は 0 ～ 255 の数値（10 進数）、または 0x0 ～ 0xFF の数値（16 進数）です。

カスタマイズ検出の開始

カスタマイズ検出を開始する手順は、次のとおりです。

コマンド	目的
switch# **discover custom-list add vsan** *vsan-id* **domain** *domain-id*	指定されたエントリをカスタム リストに追加します。
switch# **discover custom-list delete vsan** *vsan-id* **domain** *domain-id*	指定されたドメイン ID をカスタム リストから削除します。

SCSI LUN 情報の表示

検出結果を表示するには、**show scsi-target** および **show fcns database** コマンドを使用します。

次に、検出されたターゲットを表示する例を示します。

```
switch# show scsi-target status
discovery completed
```

（注）　このコマンドを完了するには、数分間かかることがあります（特に、ファブリックが大規模である場合や、複数のデバイスの応答速度が遅い場合）。

次に、FCNS データベースを表示する例を示します。

```
switch# show fcns database
```

次に、SCSI ターゲット ディスクを表示する例を示します。

```
switch# show scsi-target disk
```

次に、すべてのオペレーティング システムの検出済み LUN を表示する例を示します。

```
switch# show scsi-target lun os all
```

次に、各オペレーティング システム（Windows、AIX、Solaris、Linux、または HPUX）に割り当てられたポート WWN を表示する例を示します。

```
switch# show scsi-target pwwn
```

CHAPTER 43

拡張ファイバ チャネル機能および概念

この章では、Cisco Nexus 5000 シリーズ スイッチに備わっている拡張ファイバ チャネル機能について説明します。内容は次のとおりです。

- ファイバ チャネルのタイムアウト値（43-1 ページ）
- World Wide Name（43-5 ページ）
- HBA に対する FC ID の割り当て（43-7 ページ）
- スイッチの相互運用性（43-9 ページ）
- デフォルト設定（43-16 ページ）

ファイバ チャネルのタイムアウト値

ファイバ チャネル プロトコルに関連するスイッチのタイマー値を変更するには、次の Time Out Value（TOV; タイムアウト値）を設定します。

- Distributed Services TOV（D_S_TOV）：有効範囲は 5,000 ～ 10,000 ミリ秒です。デフォルトは 5,000 ミリ秒です。
- Error Detect TOV（E_D_TOV）：有効範囲は 1,000 ～ 10,000 ミリ秒です。デフォルトは 2,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。
- Resource Allocation TOV（R_A_TOV）：有効範囲は 5,000 ～ 10,000 ミリ秒です。デフォルトは 10,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。

（注） Fabric Stability TOV（F_S_TOV）定数は設定できません。

この項では、次のトピックについて取り上げます。

- すべての VSAN に対するタイマーの設定（43-2 ページ）
- VSAN 単位のタイマー設定（43-2 ページ）
- fctimer の配布について（43-3 ページ）
- fctimer の配布のイネーブル化とディセーブル化（43-3 ページ）
- fctimer 設定変更のコミット（43-3 ページ）
- fctimer 設定変更の廃棄（43-4 ページ）
- ファブリックのロックの上書き（43-4 ページ）
- データベース マージの注意事項（43-4 ページ）
- 設定された fctimer 値の確認（43-5 ページ）

すべての VSAN に対するタイマーの設定

ファイバ チャネル プロトコルに関連するスイッチのタイマー値を変更できます。

注意 D_S_TOV、E_D_TOV、および R_A_TOV 値をグローバルに変更するには、スイッチのすべての VSAN（仮想 SAN）を中断する必要があります。

（注） タイマー値を変更するときに VSAN を指定しない場合は、変更された値がスイッチ内のすべての VSAN に適用されます。

すべての VSAN にファイバ チャネル タイマーを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configure terminal`** `switch(config)`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`fctimer R_A_TOV`** *`timeout`*	すべての VSAN の R_A_TOV タイムアウト値を設定します。単位はミリ秒です。 このタイプの設定は、すべての VSAN が一時停止されていないかぎり、許可されません。

VSAN 単位のタイマー設定

指定された VSAN に fctimer を発行して、ファイバ チャネルなどの特殊なリンクを含む VSAN に別の TOV 値を設定することもできます。VSAN ごとに異なる E_D_TOV、R_A_TOV、および D_S_TOV 値を設定できます。アクティブ VSAN のタイマー値を変更すると、VSAN は一時停止されてからアクティブになります。

（注） この設定はファブリック内のすべてのスイッチに伝播させる必要があります。ファブリック内のすべてのスイッチに同じ値を設定してください。

VSAN 単位の FC タイマーを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configuration terminal`** `switch(config)`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config#)#` **`fctimer D_S_TOV`** *`timeout`* **`vsan`** *`vsan-id`*	指定された VSAN の D_S_TOV タイムアウト値（ミリ秒）を設定します。VSAN が一時的に停止します。必要に応じて、このコマンドを終了することもできます。

次に、VSAN 2 のタイマー値を設定する例を示します。

```
switch(config#)# fctimer D_S_TOV 6000 vsan 2
Warning: The vsan will be temporarily suspended when updating the timer value This
configuration would impact whole fabric.Do you want to continue? (y/n) y
Since this configuration is not propagated to other switches, please configure the same value
in all the switches
```

fctimer の配布について

ファブリック内のすべての Cisco SAN スイッチに対して、VSAN 単位での fctimer のファブリック配布をイネーブルにできます。fctimer の設定を実行して、配布をイネーブルにすると、ファブリック内のすべてのスイッチにその設定が配布されます。

スイッチの配布をイネーブルにしたあとで最初のコンフィギュレーション コマンドを入力すると、ファブリック全体のロックを自動的に取得します。fctimer アプリケーションは、有効データベースと保留データベース モデルを使用し、使用中のコンフィギュレーションに基づいてコマンドを格納またはコミットします。

CFS アプリケーションの詳細については、第 21 章「CFS の使用」を参照してください。

fctimer の配布のイネーブル化とディセーブル化

fctimer のファブリック配布をイネーブルまたはディセーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fctimer distribute`	ファブリック内のすべてのスイッチに対する fctimer 設定の配布をイネーブルにします。ファブリックのロックを取得して、その後の設定変更をすべて保留データベースに格納します。
	`switch(config)# no fctimer distribute`	ファブリック内のすべてのスイッチに対する fctimer 設定の配布をディセーブル（デフォルト）にします。

fctimer 設定変更のコミット

fctimer の設定変更をコミットすると、有効データベースは保留データベースの設定変更によって上書きされ、ファブリック内のすべてのスイッチが同じ設定を受け取ります。セッション機能を実行せずに fctimer の設定変更をコミットすると、fctimer 設定は物理ファブリック内のすべてのスイッチに配布されます。

fctimer の設定変更をコミットする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fctimer commit`	ファブリック内のすべてのスイッチに対して fctimer の設定変更を配布し、ロックを解除します。保留データベースに対する変更を有効データベースに上書きします。

fctimer 設定変更の廃棄

設定変更を加えたあと、変更内容をコミットする代わりに廃棄すると、この変更内容を廃棄できます。いずれの場合でも、ロックは解除されます。

fctimer の設定変更を廃棄する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fctimer abort`	保留データベースの fctimer の設定変更を廃棄して、ファブリックのロックを解除します。

ファブリックのロックの上書き

ユーザが fctimer を設定して、変更のコミットや廃棄を行ってロックを解除するのを忘れていた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこの操作を行うと、ユーザによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。

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

管理者特権を使用して、ロックされた fctimer セッションを解除するには、**clear fctimer session** コマンドを使用します。

```
switch# clear fctimer session
```

データベース マージの注意事項

2 つのファブリックを結合する場合は、次の注意事項に従ってください。

- 次の結合条件を確認します。
  - fctimer 値を配布する結合プロトコルが実行されない。ファブリックを結合する場合、fctimer 値を手動で結合する必要があります。
  - VSAN 単位の fctimer 設定は物理ファブリック内で配布される。
  - fctimer 設定は、変更された fctimer 値を持つ VSAN が含まれるスイッチだけに適用される。
  - グローバルな fctimer 値は配布されない。
- 配布がイネーブルになっている場合は、グローバル タイマーの値を設定しないでください。

（注）　保留できる fctimer 設定操作の回数は 15 回以内です。15 回を超えて設定操作を行う場合には、保留設定をコミットするか、中止する必要があります。

詳細については、「CFS 結合のサポート」セクション（21-6 ページ）を参照してください。

設定された fctimer 値の確認

設定された fctimer 値を表示するには、**show fctimer** コマンドを使用します。次の例では、設定されたグローバル TOV が表示されています。

```
switch# show fctimer
F_S_TOV   D_S_TOV   E_D_TOV   R_A_TOV
---------------------------------------
5000 ms   5000 ms   2000 ms   10000 ms
```

（注）　**show fctimer** コマンドの出力には、（設定されていない場合でも）F_S_TOV 定数が表示されます。

次の例では、VSAN 10 の設定済み TOV が表示されています。

```
switch# show fctimer vsan 10
vsan no.  F_S_TOV   D_S_TOV   E_D_TOV   R_A_TOV
-------------------------------------------------
10        5000 ms   5000 ms   3000 ms   10000 ms
```

World Wide Name

スイッチの World Wide Name（WWN）は、イーサネット MAC アドレスと同等です。MAC アドレスと同様に、デバイスごとに WWN を一意に対応付ける必要があります。主要スイッチを選択するとき、およびドメイン ID を割り当てるときは、WWN を使用します。

Cisco Nexus 5000 シリーズ スイッチは、3 つの Network Address Authority（NAA）アドレス フォーマットをサポートします（表 43-1を参照）。

表 43-1　　標準化された NAA WWN フォーマット

NAA アドレス	NAA タイプ	WWN フォーマット	
IEEE 48 ビット アドレス	タイプ 1 = 0001b	000 0000 0000b	48 ビット MAC アドレス
IEEE 拡張	タイプ 2 = 0010b	ローカルに割り当て	48 ビット MAC アドレス
IEEE 登録	タイプ 5 = 0101b	IEEE 企業 ID：24 ビット	VSID：36 ビット

注意　WWN の変更は、管理者または、スイッチの操作に精通した担当者が実行してください。

この項では、次のトピックについて取り上げます。

- WWN 情報の確認（43-6 ページ）
- リンク初期化時の WWN の使用方法（43-6 ページ）
- セカンダリ MAC アドレスの設定（43-6 ページ）

WWN 情報の確認

WWN 設定のステータスを表示するには、**show wwn** コマンドを使用します。次に、すべての WWN のステータスを表示する例を示します。

```
switch# show wwn status
Type    Configured     Available    Resvd.Alarm State
----    ----------  --------------  ------  -----------
   1           64        48 ( 75%)      16    NONE
 2,5       524288    442368 ( 84%)   73728    NONE
```

次に、ブロック ID 51 の情報を表示する例を示します。

```
switch# show wwn status block-id 51
WWNs in this block: 21:00:ac:16:5e:52:00:03 to 21:ff:ac:16:5e:52:00:03
Num. of WWNs:: Configured: 256 Allocated:    0 Available: 256
Block Allocation Status: FREE
```

次に、特定のスイッチにおける WWN を表示する例を示します。

```
switch# show wwn switch
Switch WWN is 20:00:ac:16:5e:52:00:00
```

リンク初期化時の WWN の使用方法

Exchange Link Protocol（ELP）および Exchange Fabric Protocol（EFP）は、リンク初期化の際に WWN を使用します。ELP と EFP はどちらも、デフォルトでは、リンク初期化時に VSAN WWN を使用します。ただし、ELP の使用方法はピア スイッチの使用方法に応じて変わります。

- ピア スイッチの ELP がスイッチの WWN を使用する場合、ローカル スイッチもスイッチの WWN を使用します。
- ピア スイッチの ELP が VSAN の WWN を使用する場合、ローカル スイッチも VSAN の WWN を使用します。

セカンダリ MAC アドレスの設定

セカンダリ MAC アドレスを割り当てる手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# wwn secondary-mac` *wwn-id* `range` *value*	セカンダリ MAC アドレスを設定します。このコマンドは元に戻せません。

次に、セカンダリ MAC アドレスを設定する例を示します。

```
switch(config)# wwn secondary-mac 00:99:55:77:55:55 range 64
This command CANNOT be undone.
Please enter the BASE MAC ADDRESS again: 00:99:55:77:55:55
Please enter the mac address RANGE again: 64
From now on WWN allocation would be based on new MACs.
Are you sure? (yes/no) no
You entered: no. Secondary MAC NOT programmed
```

HBA に対する FC ID の割り当て

ファイバ チャネル標準では、任意のスイッチの F ポートに接続された N ポートに、一意の FC ID を割り当てる必要があります。使用する FC ID 番号を節約するために、Cisco Nexus 5000 シリーズ スイッチでは特殊な割り当て方式を使用しています。

一部の Host Bus Adapter（HBA）は、ドメインとエリアが同じ FC ID を持つターゲットを検出しません。スイッチ ソフトウェアは、この動作が発生しないテスト済みの企業 ID のリストを保持しています。これらの HBA には単一の FC ID が割り当てられます。HBA が同じドメインおよびエリア内のターゲットを検出できる場合、完全なエリアが割り当てられます。

多数のポートを持つスイッチのスケーラビリティを高めるため、スイッチ ソフトウェアは、同じドメインおよびエリア内のターゲットを検出できる HBA のリストを維持しています。個々の HBA は、ファブリック ログイン時に pWWN で使用される、それぞれの企業 ID（別名、組織固有識別子または OUI）で識別されます。リストされている企業 ID を持つ N ポートには完全なエリアが割り当てられ、それ以外には単一の FC ID が割り当てられます。割り当てられる FC ID のタイプ（エリア全体または単一）に関係なく、FC ID エントリは永続的です。

この項では、次のトピックについて取り上げます。

- デフォルトの企業 ID リスト（43-7 ページ）
- 企業 ID の設定の確認（43-8 ページ）

デフォルトの企業 ID リスト

すべての Cisco Nexus 5000 シリーズ スイッチには、エリア割り当てが必要な企業 ID のデフォルト リストが含まれています。この企業 ID を使用すると、設定する永続的 FC ID エントリの数が少なくなります。これらのエントリは、CLI を使用して設定または変更できます。

注意　永続的エントリは、企業 ID の設定よりも優先されます。HBA がターゲットを検出しない場合は、HBA とターゲットが同じスイッチに接続され、FC ID のエリアが同じであることを確認してから、次の手順を実行します。

1.HBA に接続されているポートをシャットダウンします。
2.永続的 FC ID エントリをクリアします。
3.ポート WWN から企業 ID を取得します。
4.エリア割り当てを必要とするリストに企業 ID を追加します。
5.ポートをアップにします。

企業 ID のリストには、次の特性があります。

- 永続的 FC ID の設定は常に企業 ID リストよりも優先されます。エリアを受け取るように企業 ID が設定されている場合でも、永続的 FC ID の設定によって単一の FC ID が割り当てられます。
- 後続のリリースに追加される新規の企業 ID は、既存の企業 ID に自動的に追加されます。
- 企業 ID のリストは、実行コンフィギュレーションおよび保存されたコンフィギュレーションの一部として保存されます。

- 企業 ID のリストが使用されるのは、fcinterop の FC ID 割り当て方式が auto モードの場合だけです。変更されないかぎり、interop の FC ID 割り当ては、デフォルトで auto に設定されています。

ヒント　fcinterop の FC ID 割り当て方式を auto に設定し、企業 ID リストと永続的 FC ID 設定を使用して、FC ID のデバイス割り当てを行うことをお勧めします。

FC ID の割り当てを変更するには、**fcinterop FCID allocation auto** コマンドを使用し、現在割り当てられているモードを表示するには、**show running-config** コマンドを使用します。

- **write erase** を入力すると、リストは該当するリリースに付属している企業 ID のデフォルト リストを継承します。

企業 ID を割り当てる手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fcid-allocation area company-id value`	デフォルト リストに新しい企業 ID を追加します。
	`switch(config)# no fcid-allocation area company-id value`	デフォルト リストから企業 ID を削除します。

次に、デフォルト リストに新しい企業 ID を追加する例を示します。

```
switch(config)# fcid-allocation area company-id 0x003223
```

企業 ID の設定の確認

設定された企業 ID を表示するには、**show fcid-allocation area** コマンドを入力します。最初にデフォルト エントリが表示され、次にユーザによって追加されたエントリが表示されます。エントリがデフォルト リストの一部で、あとで削除された場合でも、エントリは表示されます。

次に、デフォルトおよび設定された企業 ID のリストを表示する例を示します。

```
switch# show fcid-allocation area
FCID area allocation company id info:
    00:50:2E <-------------------- デフォルト エントリ
    00:50:8B
    00:60:B0
    00:A0:B8
    00:E0:69
    00:30:AE + <------------------ ユーザが追加したエントリ
    00:32:23 +

    00:E0:8B * <------------------ (元のデフォルト リストから)明示的に削除されたエントリ
Total company ids: 7
+ - ユーザーが設定した追加の企業 ID
* - デフォルト リストから明示的に削除した企業 ID
```

削除済みエントリの印が付いていない企業 ID のリストを組み合わせると、特定のリリースに付属するデフォルト エントリを暗黙的に導き出すことができます。

また、**show fcid-allocation company-id-from-wwn** コマンドを使用すると、特定の WWN の企業 ID を表示または取得することもできます。一部の WWN 形式では、企業 ID がサポートされていません。この場合、FC ID の永続的エントリを設定する必要があります。

次に、指定の WWN の企業 ID を表示する例を示します。

```
switch# show fcid-allocation company-id-from-wwn 20:00:00:05:30:00:21:60
Extracted Company ID: 0x000530
```

スイッチの相互運用性

相互運用性を使用すると、複数ベンダーによる製品の間で相互に通信することができます。ファイバ チャネル標準規格では、ベンダーに対して共通の外部ファイバ チャネル インターフェイスを使用することを推奨しています。

同じ方法で標準規格に準拠していないベンダーもあるため、相互運用モードが必要になります。ここでは、これらのモードの基本的な概念について簡単に説明します。

各ベンダーには標準モード、および同等の相互運用モードがあります。相互運用モードでは拡張機能または独自の機能が無効になり、標準に準拠した実装が可能になります。

（注）　Cisco Nexus 5000 シリーズ スイッチでの相互運用性の設定方法に関する詳細は、『*Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*』を参照してください。

この項では、次のトピックについて取り上げます。

- Interop モードについて（43-9 ページ）
- interop モード 1 の設定（43-11 ページ）
- 相互運用ステータスの確認（43-12 ページ）

Interop モードについて

Cisco NX-OS ソフトウェアは、次の 4 つの interop モードをサポートしています。

- モード 1：標準ベースの interop モード。ファブリック内の他のベンダー製品もすべて interop モードになっている必要があります。
- モード 2：Brocade ネイティブ モード（Core PID 0）
- モード 3：Brocade ネイティブ モード（コア PID 1）
- モード 4：McData ネイティブ モード

interop モード 2、3、および 4 の設定方法については、次の URL にある『*Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/interoperability/guide/intopgd.html

表 43-2 に、相互運用モードをイネーブルにした場合のスイッチ動作の変更点を示します。これらは、interop モードの Cisco Nexus 5000 シリーズ スウィッチに固有の変更点です。

表 43-2　相互運用モードがイネーブルの場合のスイッチ動作の変更点

スイッチ機能	相互運用モードがイネーブルの場合の変更点
ドメイン ID	一部のベンダーは、ファブリック内の 239 のドメインを完全には使用できません。 ドメイン ID は 97 ～ 127 の範囲に制限されます。これは、McData の公称制限をこの範囲内に収めるためです。ドメイン ID は Static または Preferred に設定できます。それぞれの動作は次のとおりです。 • Static：シスコ スイッチは 1 つのドメイン ID だけを受け入れ、そのドメイン ID を取得できない場合には、ファブリックから隔離します。 • Preferred：スイッチが要求したドメイン ID を取得できない場合、割り当てられた任意のドメインを受け入れます。
タイマー	ISL（スイッチ間リンク）を確立するときにファイバ チャネル タイマー値が E ポートで交換されるので、すべてのスイッチでこれらのタイマーをすべて同じにする必要があります。タイマーには、F_S_TOV、D_S_TOV、E_D_TOV、および R_A_TOV があります。
F_S_TOV	Fabric Stability TOV タイマーが正確に一致するかどうかを確認してください。
D_S_TOV	Distributed Services TOV タイマーが正確に一致するかどうかを確認してください。
E_D_TOV	Error Detect TOV タイマーが正確に一致するかどうかを確認してください。
R_A_TOV	Resource Allocation TOV タイマーが正確に一致するかどうかを確認してください。
トランキング	2 つの異なるベンダー製のスイッチ間では、トランキングはサポートされません。この機能はポート単位、またはスイッチ単位でディセーブルに設定できます。
デフォルト ゾーン	ゾーンのデフォルトの許可動作（すべてのノードから他のすべてのノードを認識可能）または拒否動作（明示的にゾーンに配置されていないすべてのノードが隔離される）は変更できます。
ゾーン分割属性	ゾーンを pWWN に制限したり、その他の独自のゾーン分割方式（物理ポート番号）を除去することができます。 **（注）** Brocade スイッチでは、**cfgsave** コマンドを使用して、ファブリック全体のゾーン分割設定を保存します。このコマンドは、同じファブリックに属する Cisco Nexus 5000 シリーズ スイッチには影響しません。Cisco Nexus 5000 シリーズの各スイッチに、明示的に設定を保存する必要があります。
ゾーンの伝播	一部のベンダーは、他のスイッチに完全なゾーン設定を受け渡さないで、アクティブ ゾーン セットだけを受け渡します。 ファブリック内の他のスイッチにアクティブ ゾーンセットまたはゾーン設定が正しく伝播されたかどうかを確認してください。
VSAN	interop モードは、指定された VSAN にだけ有効です。 **（注）** interop モードは、FICON 対応の VSAN でイネーブルにできません。

表 43-2　相互運用モードがイネーブルの場合のスイッチ動作の変更点（続き）

スイッチ機能	相互運用モードがイネーブルの場合の変更点
TE ポートおよび SAN ポート チャネル	シスコ スイッチと Cisco SAN 以外のスイッチを接続する場合は、TE ポートおよび SAN ポート チャネルを使用できません。Cisco SAN 以外のスイッチに接続できるのは、E ポートだけです。interop モードの場合でも、TE ポートおよび SAN ポート チャネルを使用すると、シスコ スイッチをほかの Cisco SAN スイッチに接続することができます。
FSPF	interop モードにしても、ファブリック内のフレームのルーティングは変更されません。スイッチは引き続き src-id、dst-id、および ox-id を使用して、複数の ISL リンク間でロード バランスします。
ドメインの中断再設定	これは、スイッチ全体に影響するイベントです。Brocade および McData では、ドメイン ID を変更するときにスイッチ全体をオフライン モードにしたり、再起動したりする必要があります。
ドメインの非中断再設定	これは、関連する VSAN に限定されるイベントです。Cisco Nexus 5000 シリーズ スイッチには、スイッチ全体ではなく、関連する VSAN のドメイン マネージャ プロセスだけを再起動する機能が組み込まれています。
ネーム サーバ	すべてのベンダーのネーム サーバ データベースに正しい値が格納されているかを確認してください。

interop モード 1 の設定

Cisco Nexus 5000 シリーズ スイッチでは、interop モード 1 の中断または非中断をイネーブルにできます。

（注） Brocade スイッチから Cisco Nexus 5000 シリーズ スイッチまたは McData スイッチに接続する前に、Brocade の **msplmgmtdeactivate** コマンドを明示的に実行する必要があります。このコマンドは Brocade 独自のフレームを使用して、Cisco Nexus 5000 シリーズ スイッチまたは McData スイッチが認識しないプラットフォーム情報を交換します。これらのフレームを拒否すると、一般的な E ポートが隔離されます。

Cisco Nexus 5000 シリーズの任意のスイッチに interop モード 1 を設定する手順は、次のとおりです。

ステップ 1　他ベンダー製スイッチに接続する E ポートの VSAN を相互運用モードにします。

```
switch# configuration terminal
switch(config)# vsan database
switch(config-vsan-db)# vsan 1 interop 1
switch(config-vsan-db)# exit
switch(config)#
```

ステップ 2　97（0x61）～ 127（0x7F）の範囲でドメイン ID を割り当てます。

（注） これは、McData スイッチに適用される制限です。

```
switch(config)# fcdomain domain 100 preferred vsan 1
```

Cisco Nexus 5000 シリーズ スイッチの場合、デフォルトでは、主要スイッチから ID が要求されます。Preferred オプションを使用した場合、Cisco Nexus 5000 シリーズ スイッチは固有の ID を要求しますが、主要スイッチから別の ID が割り当てられた場合もファブリックに加入します。Static オプションを使用した場合、要求された ID を主要スイッチが承認して、これを割り当てないかぎり、Cisco Nexus 5000 シリーズ スイッチはファブリックに参加しません。

（注） ドメイン ID を変更すると、N ポートに割り当てられた FC ID も変更されます。

ステップ 3 FC タイマーを変更します（システム デフォルトから変更された場合）。

（注） Cisco Nexus 5000 シリーズ、Brocade、および McData の FC Error Detect（ED_TOV）と Resource Allocation（RA_TOV）タイマーは、デフォルトで同じ値です。これらの値は、必要に応じて変更できます。RA_TOV のデフォルト値は 10 秒、ED_TOV のデフォルト値は 2 秒です。FC-SW2 標準に基づく場合、これらの値は、ファブリック内の各スイッチで一致している必要があります。

```
switch(config)# fctimer e_d_tov ?
  <1000-100000>  E_D_TOV in milliseconds(1000-100000)
switch(config)# fctimer r_a_tov ?
  <5000-100000>  R_A_TOV in milliseconds(5000-100000)
```

ステップ 4 ドメインを変更するときに、変更された VSAN のドメイン マネージャ機能の再起動が必要な場合と、不要な場合があります。

- **disruptive** オプションを使用して、ファブリックを強制的に再設定する場合は次のようになります。

  ```
  switch(config)# fcdomain restart disruptive vsan 1
  ```

  または

- ファブリックを強制的に再設定しない場合は次のようになります。

  ```
  switch(config# fcdomain restart vsan 1
  ```

相互運用ステータスの確認

ここでは、ファブリックが起動していて、相互運用モードで稼働していることを確認するためのコマンドについて説明します。

Cisco Nexus 5000 シリーズの任意のスイッチで相互運用性コマンドを入力した場合のステータスを確認する手順は、次のとおりです。

ステップ 1 ソフトウェア バージョンを確認します。

```
switch# show version
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2007, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software may be covered under the GNU Public
License or the GNU Lesser General Public License.A copy of
```

```
each such license is available at
http://www.gnu.org/licenses/gpl.html and
http://www.gnu.org/licenses/lgpl.html

Software
  BIOS:      version
  kickstart: version 4.0(0) [build 4.0(0.308)] [gdb]
  system:    version 4.0(0) [build 4.0(0.308)] [gdb]

  BIOS compile time:
  kickstart image file is: bootflash:///nuova-or-kickstart-nsg.0.1.0.001.bin
  kickstart compile time:  10/12/2020 25:00:00 [02/22/2008 13:05:46]
  system image file is:    bootflash:/nuova-or-system-nsg.0.1.0.001.bin
  system compile time:     10/22/2007 14:00:00 [02/22/2008 14:19:45]

ハードウェア
  cisco Nexus5020 Chassis ("40x10GE/Supervisor")
  Intel(R) Celeron(R) M CPU   with 2074100 kB of memory.
  Processor Board ID FOX1009009B

  bootflash:  987136 kB

switch   kernel uptime is 0 days 20 hours 6 minute(s) 55 second(s)

  Last reset
    Reason: Unknown
    System version:
    [Service]:
```

ステップ 2　インターフェイスの状態が使用中の設定に必要な状態になっているかどうかを確認します。

```
switch# show int brief
--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                          Mode  Speed  Channel
                         Mode                                  (Gbps)
--------------------------------------------------------------------------------
fc3/1      1      E      on      trunking         swl    TE      2    --
fc3/2      1      auto   on      sfpAbsent        --     --           --
fc3/3      1      E      on      trunking         swl    TE      2    --
fc3/4      1      auto   on      sfpAbsent        --     --           --
fc3/5      1      auto   auto    notConnected     swl    --           --
fc3/6      1      auto   on      sfpAbsent        --     --           --
fc3/7      1      auto   auto    sfpAbsent        --     --           --
fc3/8      1      auto   auto    sfpAbsent        --     --           --
```

ステップ 3　目的のコンフィギュレーションが稼働しているかどうかを確認します。

```
switch# show run
Building Configuration...

 interface fc2/1
no shutdown

 interface fc2/2
no shutdown

 interface fc2/3
 interface fc2/4

<省略>

interface mgmt0
```

```
ip address 6.1.1.96 255.255.255.0
switchport encap default
no shutdown

vsan database
vsan 1 interop

boot system bootflash:/nx5000-system-23e.bin
boot kickstart bootflash:/nx5000-kickstart-23e.bin
callhome

fcdomain domain 100 preferred vsan 1

ip route 6.1.1.0 255.255.255.0 6.1.1.1
ip routing
line console
  databits 5
  speed 110
logging linecard
ssh key rsa 512 force
ssh server enable
switchname MDS9509
username admin password 5 $1$Li8/fBYX$SNc72.xt4nTXpSnR9OUFB/ role network-admin
```

ステップ 4　相互運用性モードがアクティブであるかどうかを確認します。

```
switch# show vsan 1
vsan 1 information
         name:VSAN0001  state:active
         interoperability mode:yes <--------------------モードを確認
         loadbalancing:src-id/dst-id/oxid
         operational state:up
```

ステップ 5　ドメイン ID を確認します。

```
switch# show fcdomain vsan 1
The local switch is a Subordinated Switch.

Local switch run time information:
        State: Stable
        Local switch WWN:    20:01:00:05:30:00:51:1f
        Running fabric name: 10:00:00:60:69:22:32:91
        Running priority: 128
        Current domain ID: 0x64(100) <---------------ドメイン ID を確認

Local switch configuration information:
        State: Enabled
        Auto-reconfiguration: Disabled
        Contiguous-allocation: Disabled
        Configured fabric name: 41:6e:64:69:61:6d:6f:21
        Configured priority: 128
        Configured domain ID: 0x64(100) (preferred)

Principal switch run time information:
        Running priority: 2

Interface               Role          RCF-reject
----------------    -------------    ------------
fc2/1               Downstream       Disabled
fc2/2               Downstream       Disabled
fc2/4               Upstream         Disabled
----------------    -------------    ------------
```

ステップ 6　ローカル主要スイッチのステータスを確認します。

```
switch# show fcdomain domain-list vsan 1

Number of domains: 5
Domain ID              WWN
---------    -----------------------
 0x61(97)    10:00:00:60:69:50:0c:fe
 0x62(98)    20:01:00:05:30:00:47:9f
 0x63(99)    10:00:00:60:69:c0:0c:1d
0x64(100)    20:01:00:05:30:00:51:1f [Local]
0x65(101)    10:00:00:60:69:22:32:91 [Principal]
---------    -----------------------
```

ステップ 7　スイッチのネクスト ホップおよび宛先を確認します。

```
switch# show fspf internal route vsan 1

FSPF Unicast Routes
---------------------------
 VSAN Number  Dest Domain   Route Cost    Next hops
---------------------------------------------
           1     0x61(97)          500      fc2/2
           1     0x62(98)         1000      fc2/1
                                           fc2/2
           1     0x63(99)          500      fc2/1
           1    0x65(101)         1000      fc2/4
```

ステップ 8　ネーム サーバ情報を確認します。

```
switch# show fcns data vsan 1
VSAN 1:
-----------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR) FC4-TYPE:FEATURE
-----------------------------------------------------------------
0x610400    N     10:00:00:00:c9:24:3d:90 (Emulex)     scsi-fcp
0x6105dc    NL    21:00:00:20:37:28:31:6d (Seagate)    scsi-fcp
0x6105e0    NL    21:00:00:20:37:28:24:7b (Seagate)    scsi-fcp
0x6105e1    NL    21:00:00:20:37:28:22:ea (Seagate)    scsi-fcp
0x6105e2    NL    21:00:00:20:37:28:2e:65 (Seagate)    scsi-fcp
0x6105e4    NL    21:00:00:20:37:28:26:0d (Seagate)    scsi-fcp
0x630400    N     10:00:00:00:c9:24:3f:75 (Emulex)     scsi-fcp
0x630500    N     50:06:01:60:88:02:90:cb              scsi-fcp
0x6514e2    NL    21:00:00:20:37:a7:ca:b7 (Seagate)    scsi-fcp
0x6514e4    NL    21:00:00:20:37:a7:c7:e0 (Seagate)    scsi-fcp
0x6514e8    NL    21:00:00:20:37:a7:c7:df (Seagate)    scsi-fcp
0x651500    N     10:00:00:e0:69:f0:43:9f (JNI)

Total number of entries = 12
```

（注）　シスコ スイッチ ネーム サーバにはローカル エントリおよびリモート エントリが表示され、エントリはタイムアウトしません。

デフォルト設定

表 43-3 に、この章で説明した機能のデフォルト設定値を示します。

表 43-3　拡張機能のデフォルト設定値

パラメータ	デフォルト
CIM サーバ	ディセーブル
CIM サーバ セキュリティ プロトコル	HTTP
D_S_TOV	5,000 ミリ秒
E_D_TOV	2,000 ミリ秒
R_A_TOV	10,000 ミリ秒
fctrace を呼び出すタイムアウト時間	5 秒
fcping 機能によって送信されるフレーム数	5 フレーム
リモート キャプチャ接続プロトコル	TCP
リモート キャプチャ接続モード	Passive
ローカル キャプチャ フレーム制限	10 フレーム
FC ID の割り当てモード	auto モード
ループ モニタリング	ディセーブル
interop モード	ディセーブル

CHAPTER 44

FC-SP および DHCHAP の設定

Fibre Channel Security Protocol（FC-SP）機能は、スイッチとスイッチ間およびホストとスイッチ間で認証を実行して、企業全体のファブリックに関するセキュリティ問題を解決します。Diffie-Hellman Challenge Handshake Authentication Protocol（DHCHAP）は、Cisco Nexus 5000 シリーズ スイッチとその他のデバイス間で認証を行う FC-SP プロトコルです。DHCHAP は、CHAP プロトコルと Diffie-Hellman 交換を組み合わせて構成されています。

この章は、次の項で構成されています。

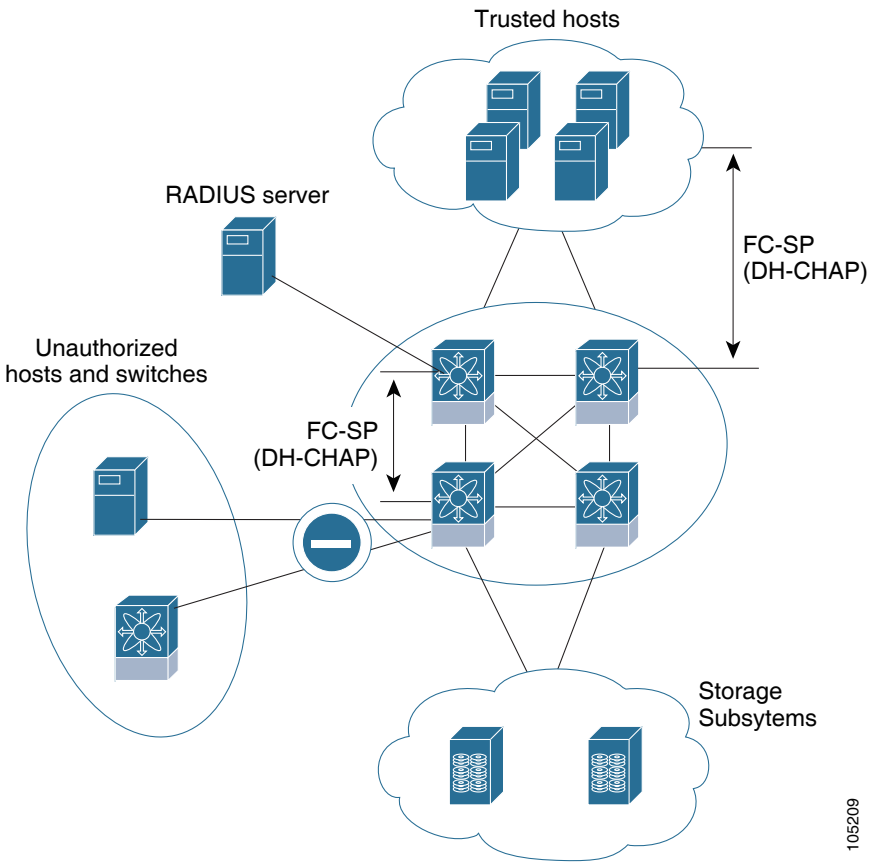
- ファブリック認証に関する情報（44-1 ページ）
- DHCHAP（44-2 ページ）
- 設定例（44-10 ページ）
- デフォルト設定（44-11 ページ）

ファブリック認証に関する情報

Cisco Nexus 5000 シリーズ の全スイッチで、1 台のスイッチから他のスイッチへ、またはスイッチからホストへ、ファブリック規模の認証を実行できます。これらのスイッチおよびホスト認証は、各ファブリックでローカルまたはリモートで実行できます。ストレージ アイランドを企業全体のファブリックに統合して、移行すると、新しいセキュリティ問題が発生します。ストレージ アイランドを保護する方法が、企業全体のファブリックで必ずしも保証されなくなります。たとえば、スイッチが地理的に分散しているキャンパス環境では、他のユーザが故意に、またはユーザ自身が誤って、互換性のないスイッチに故意に相互接続すると、ISL（スイッチ間リンク）分離やリンク切断が発生することがあります。

Cisco Nexus 5000 シリーズ スイッチでは、物理セキュリティに対処する認証機能をサポートしています（図 44-1 を参照）。

図 44-1　　スイッチおよびホストの認証



（注）　ホスト スイッチ認証には、適切なファームウェアおよびドライバを備えたファイバ チャネル Host Bus Adapter（HBA）が必要です。

DHCHAP

DHCHAP は、スイッチに接続しているデバイスを認証する認証プロトコルです。ファイバ チャネル認証を使用すると、信頼できるデバイスだけをファブリックに追加できるので、不正なデバイスのスイッチへのアクセスを防止できます。

（注）　この章では、FC-SP および DHCHAP という用語を共通の意味で使用しています。

DHCHAP は、必須のパスワードに基づくキー交換による認証プロトコルであり、スイッチ間およびホスト スイッチ間の認証をサポートします。DHCHAP はハッシュ アルゴリズムおよび DH グループをネゴシエートしてから、認証を実行します。また、MD5 および SHA-1 アルゴリズムベース認証をサポートします。

ローカル パスワード データベースを使用する DHCHAP 認証の設定手順は、次のとおりです。

ステップ 1　DHCHAP をイネーブルにします。

ステップ 2　DHCHAP 認証モードを識別して設定します。

ステップ 3　ハッシュ アルゴリズムおよび DH グループを設定します。

ステップ 4　ローカル スイッチおよびファブリックの他のスイッチの DHCHAP パスワードを設定します。

ステップ 5　再認証の DHCHAP タイムアウト値を設定します。

ステップ 6　DHCHAP の設定を確認します。

この項では、次のトピックについて取り上げます。

- ファイバ チャネル機能と DHCHAP の互換性（44-3 ページ）
- DHCHAP のイネーブル化の概要（44-4 ページ）
- DHCHAP のイネーブル化（44-4 ページ）
- DHCHAP 認証モードの概要（44-4 ページ）
- DHCHAP モードの設定（44-5 ページ）
- DHCHAP ハッシュ アルゴリズムの概要（44-6 ページ）
- DHCHAP ハッシュ アルゴリズムの設定（44-6 ページ）
- DHCHAP グループ設定の概要（44-6 ページ）
- DHCHAP グループの設定（44-6 ページ）
- DHCHAP パスワードの概要（44-7 ページ）
- ローカル スイッチの DHCHAP パスワードの設定（44-7 ページ）
- リモート デバイスのパスワード設定の概要（44-8 ページ）
- リモート デバイスの DHCHAP パスワードの設定（44-8 ページ）
- DHCHAP タイムアウト値の概要（44-8 ページ）
- DHCHAP タイムアウト値の設定（44-9 ページ）
- DHCHAP AAA 認証の設定（44-9 ページ）
- プロトコル セキュリティ情報の表示（44-9 ページ）

ファイバ チャネル機能と DHCHAP の互換性

ここでは、DHCHAP 機能を既存の Cisco NX-OS 機能と一緒に設定した場合の影響について説明します。

- SAN ポートチャネル インターフェイス：SAN ポートチャネルに属しているポートに対して DHCHAP がイネーブルの場合、DHCHAP 認証はポートチャネル レベルではなく、物理インターフェイス レベルで実行されます。
- ポート セキュリティまたはファブリック バインディング：ファブリック バインディング ポリシーは、DHCHAP によって認証される ID に基づいて実行されます。
- VSAN：DHCHAP 認証は、VSAN 単位では実行されません。

DHCHAP のイネーブル化の概要

デフォルトでは、DHCHAP 機能はすべての Cisco Nexus 5000 シリーズ スイッチでディセーブルです。

ファブリック認証用のコンフィギュレーション コマンドおよび確認コマンドにアクセスするには、DHCHAP 機能をイネーブルにする必要があります。この機能をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

DHCHAP のイネーブル化

Cisco Nexus 5000 シリーズ スイッチ用の DHCHAP をイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fcsp enable`	このスイッチ上で DHCHAP をイネーブルにします。
	`switch(config)# no fcsp enable`	このスイッチ上で DHCHAP をディセーブル（デフォルト）にします。

DHCHAP 認証モードの概要

各インターフェイスの DHCHAP 認証ステータスは、DHCHAP ポート モードの設定によって変化します。

スイッチ内で DHCHAP 機能がイネーブルの場合には、各ファイバ チャネル インターフェイスまたは FCIP インターフェイスを次の 4 つの DHCHAP ポート モードのいずれかに設定できます。

- On：接続元デバイスが DHCHAP 認証をサポートしている場合、スイッチ初期化中に認証シーケンスが実行されます。接続元デバイスが DHCHAP 認証をサポートしていない場合には、リンクが分離状態になります。
- auto-Active：接続元デバイスが DHCHAP 認証をサポートしている場合、スイッチ初期化中に認証シーケンスが実行されます。接続元デバイスが DHCHAP 認証をサポートしていない場合には、ソフトウェアにより、初期化シーケンスの残りが実行されます。
- auto-Passive（デフォルト）：スイッチは DHCHAP 認証を開始しませんが、接続元デバイスが DHCHAP 認証を開始すれば、DHCHAP 認証に参加します。
- Off：スイッチは DHCHAP 認証をサポートしません。このモードでポートに認証メッセージが送信された場合、開始元スイッチにエラー メッセージが戻されます。

（注） DHCHAP ポート モードを off モード以外のモードに変更すると、再認証が実行されます。

表 44-1 で、さまざまなモードに設定した 2 台のシスコ スイッチ間での認証について説明します。

表 44-1　2 台の MDS スイッチ間の DHCHAP 認証ステータス

<table>
<tr><th rowspan="2">スイッチ番号DHCHAP モード</th><th colspan="4">スイッチ 1 の DHCHAP モード</th></tr>
<tr><th>on</th><th>auto-active</th><th>auto-passive</th><th>off</th></tr>
<tr><td>on</td><td rowspan="3">FC-SP 認証が実行されます。</td><td rowspan="3">FC-SP 認証が実行されます。</td><td rowspan="2">FC-SP 認証が実行されます。</td><td>リンクがダウンになります。</td></tr>
<tr><td>auto-Active</td><td rowspan="2">FC-SP 認証は*実行されません。*</td></tr>
<tr><td>auto-Passive</td><td>FC-SP 認証は*実行されません。*</td></tr>
<tr><td>off</td><td>リンクがダウンになります。</td><td colspan="3">FC-SP 認証は*実行されません。*</td></tr>
</table>

DHCHAP モードの設定

特定のインターフェイスの DHCHAP モードを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configuration terminal`**	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`interface fc`** *`slot/port - slot/port`* `switch(config-if)#`	インターフェイスの範囲を選択し、インターフェイス コンフィギュレーション モードに入ります。
ステップ 3	`switch(config-if)#` **`fcsp on`**	選択したインターフェイスの DHCHAP モードを on ステートに設定します。
	`switch(config-if)#` **`no fcsp on`**	これら 3 つのインターフェイスを出荷時デフォルトの auto-passive に戻します。
ステップ 4	`switch(config-if)#` **`fcsp auto-active 0`**	選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。0 は、ポートが再認証を実行しないことを表します。 **（注）** 再許可インターバル設定は、デフォルトの動作と同じです。
	`switch(config-if)#` **`fcsp auto-active`** *`timeout-period`*	選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。タイムアウト期間の値（分）では、最初の認証後の再認証の頻度を設定します。
	`switch(config-if)#` **`fcsp auto-active`**	選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。再認証はディセーブルになります（デフォルト）。 **（注）** 再許可インターバル設定は、0 に設定した場合と同じです。

DHCHAP ハッシュ アルゴリズムの概要

Cisco SAN スイッチは、DHCHAP 認証のためのデフォルトのハッシュ アルゴリズムのプライオリティ リストとして、最初に MD5、次に SHA-1 をサポートします。

ヒント ハッシュ アルゴリズムの設定を変更する場合は、ファブリック上の全スイッチに対して設定をグローバルに変更してください。

注意 RADIUS および TACACS+ プロトコルは、CHAP 認証で常に MD5 を使用します。SHA-1 をハッシュ アルゴリズムとして使用すると、DHCHAP 認証用に RADIUS および TACACS+ がイネーブルになっていても、これらの AAA プロトコルが使用できなくなる可能性があります。

DHCHAP ハッシュ アルゴリズムの設定

ハッシュ アルゴリズムを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fcsp dhchap hash [md5] [sha1]`	MD5 または SHA-1 ハッシュ アルゴリズムを使用するように設定します。
	`switch(config)# no fcsp dhchap hash sha1`	出荷時デフォルトのハッシュ アルゴリズム プライオリティ リスト（最初に MD5、次に SHA-1）に戻します。

DHCHAP グループ設定の概要

すべての Cisco Nexus 5000 シリーズ スイッチは、規格 0（DH 交換を実行しないヌルの DH グループ）、1、2、3、または 4 で指定されたすべての DHCHAP グループをサポートします。

ヒント DH グループの設定を変更する場合は、ファブリック内のすべてのスイッチの設定をグローバルに変更してください。

DHCHAP グループの設定

DH グループの設定を変更する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fcsp dhchap dhgroup [0 | 1 | 2 | 3 | 4]`	DH グループを設定された順序で使用するようにプライオリティ リスト化します。
	`switch(config)# no fcsp dhchap dhgroup [0 | 1 | 2 | 3 | 4]`	DHCHAP の出荷時デフォルトの順序（0、4、1、2、3）に戻します。

DHCHAP パスワードの概要

DHCHAP 認証を実行する方向ごとに、接続デバイス間の共有シークレット パスワードが必要です。このパスワードを使用するために、次の 3 つの設定例のいずれかを使用してDHCHAP に参加するファブリック内のすべてのスイッチのパスワードを管理します。

- 設定例 1: ファブリック内の全スイッチに同じパスワードを使用します。これは最も単純な設定例です。新しいスイッチを追加する場合、このファブリック内では同じパスワードを使用してそのスイッチを認証します。したがってこれは、ファブリック内のいずれかのスイッチに外部から不正アクセスが試みられた場合に最も脆弱な設定例です。
- 設定例 2: スイッチごとに異なるパスワードを使用して、ファブリック内のスイッチごとにパスワード リストを保持します。新しいスイッチを追加する場合は、新規パスワード リストを作成して、この新規リストを使用してすべてのスイッチを更新します。いずれかのスイッチにアクセスすると、このファブリック上のすべてのスイッチに関するパスワード リストが生成されます。
- 設定例 3: ファブリック内のスイッチごとに、異なるパスワードを使用します。新しいスイッチを追加する場合は、ファブリック内の各スイッチに対応する複数の新規パスワードを生成して、各スイッチに設定する必要があります。いずれかのスイッチが被害にあっても、他のスイッチのパスワードは引き続き保護されます。この設定例では、ユーザ側で大量のパスワード メンテナンス作業が必要になります。

（注） パスワードはすべて 64 文字以内の英数字に制限されます。パスワードは変更できますが、削除はできません。

ヒント スイッチが 6 台以上のファブリックでは、RADIUS または TACACS+ の使用をお勧めします。ローカル パスワード データベースを使用する必要がある場合には、設定例 3 を使用し、Cisco MDS 9000 ファミリ Fabric Manager を使用して、パスワード データベースを管理します。

ローカル スイッチの DHCHAP パスワードの設定

ローカル スイッチの DHCHAP パスワードを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fcsp dhchap password [0 | 7] password [wwn wwn-id]`	ローカル スイッチのクリアテキスト パスワードを設定します。

次に、指定した WWN を持つデバイスに使用されるローカル スイッチのクリアテキスト パスワードを設定する例を示します。

```
switch(config)# fcsp dhchap password 0 mypassword 30:11:bb:cc:dd:33:11:22
```

次に、指定した WWN を持つデバイスに使用されるローカル スイッチのクリアテキスト パスワードを削除する例を示します。

```
switch(config)# no fcsp dhchap password 0 mypassword 30:11:bb:cc:dd:33:11:22
```

次に、ローカル スイッチの暗号化パスワードを設定する例を示します。

```
switch(config)# fcsp dhchap password 7 sfsfdf
```

リモート デバイスのパスワード設定の概要

ファブリック内の他のデバイスのパスワードを、ローカル認証データベースに設定できます。他のデバイスは、スイッチ WWN やデバイス WWN といったデバイス名で表されます。パスワードは 64 文字に制限され、クリア テキスト（0）または暗号化テキスト（7）で指定できます。

（注）　スイッチ WWN は、物理スイッチを識別します。この WWN はスイッチの認証に使用されます。また、VSAN ノード WWN とは異なります。

リモート デバイスの DHCHAP パスワードの設定

ファブリック内の他のスイッチのリモート DHCHAP パスワードをローカル側で設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fcsp dhchap devicename` *switch-wwn* `password` *password*	スイッチ WWN デバイス名で表される、ファブリック上の他のスイッチのパスワードを設定します。
	`switch(config)# no fcsp dhchap devicename` *switch-wwn* `password` *password*	ローカル認証データベースから、このスイッチのパスワード エントリを削除します。

次に、スイッチ WWN デバイス名で表される、ファブリック内の他のスイッチのクリアテキストパスワードを設定する例を示します。

```
switch(config)# fcsp dhchap devicename 00:11:55:66:00:aa:bb:cc password 0 NewPassword
```

次に、スイッチ WWN デバイス名で表される、ファブリック内の他のスイッチの暗号化パスワードを設定する例を示します。

```
switch(config)# fcsp dhchap devicename 00:11:22:33:55:aa:bb:cc password 7 asdflkjh
```

DHCHAP タイムアウト値の概要

DHCHAP プロトコル交換を実行するとき、Cisco Nexus 5000 シリーズ スイッチが指定時間内に DHCHAP メッセージを受信しない場合、認証は失敗したと見なされます。この（認証が失敗したと見なされるまでの）時間は、20 ～ 1000 秒の範囲で設定できます。デフォルトは 30 秒です。

タイムアウト値を変更する場合には、次の要因について考慮してください。

- 既存の RADIUS および TACACS+ タイムアウト値。
- ファブリック内のすべてのスイッチに同じ値を設定する必要もあります。

DHCHAP タイムアウト値の設定

DHCHAP タイムアウト値を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fcsp timeout timeout`	再認証タイムアウトを指定された値に設定します。単位は秒です。
	`switch(config)# no fcsp timeout timeout`	出荷時デフォルトの 30 秒に戻します。

DHCHAP AAA 認証の設定

AAA 認証で RADIUS または TACACS+ サーバ グループを使用するように設定できます。AAA 認証を設定しない場合、デフォルトでローカル認証が使用されます。

AAA 認証を設定する手順については、「AAA の設定」セクション（16-6 ページ）を参照してください。

プロトコル セキュリティ情報の表示

ローカル データベースの設定を表示するには、**show fcsp** コマンドを使用します。

次に、指定されたインターフェイスに関する DHCHAP 設定を表示する例を示します。

```
switch# show fcsp interface fc2/4

fc2/4:
        fcsp authentication mode:SEC_MODE_ON
        Status: Successfully authenticated
```

次に、指定されたインターフェイスに関する DHCHAP 統計情報を表示する例を示します。

```
switch# show fcsp interface fc2/4 statistics
```

次に、指定されたインターフェイスに接続されたデバイスの FC-SP WWN を表示する例を示します。

```
switch# show fcsp interface fc2/1 wwn
```

次に、スイッチに設定済みのハッシュ アルゴリズムおよび DHCHAP グループを表示する例を示します。

```
switch# show fcsp dhchap
```

次に、DHCHAP ローカル パスワード データベースを表示する例を示します。

```
switch# show fcsp dhchap database
```

ヒント　RADIUS サーバおよび TACACS+ サーバにスイッチ情報を設定する場合、デバイス WWN の ASCII 表記を使用してください。

設定例

ここでは、図 44-2 に示した例を設定する手順を示します。

図 44-2　DHCHAP 認証の例

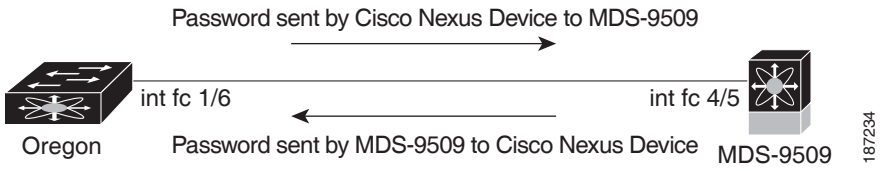


図 44-2 に表示されているように認証設定を設定する手順は、次のとおりです。

ステップ 1　ファブリック内の Cisco Nexus 5000 シリーズ スイッチのデバイス名を取得します。ファブリック内の Cisco Nexus 5000 シリーズ スイッチは、スイッチ WWN によって識別されます。

```
switch# show wwn switch
Switch WWN is 20:00:00:05:30:00:54:de
```

ステップ 2　このスイッチで DHCHAP を明示的にイネーブルにします。

（注）　DHCHAP をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

```
switch(config)# fcsp enable
```

ステップ 3　このスイッチのクリア テキスト パスワードを設定します。このパスワードは、接続先デバイスで使用されます。

```
switch(config)# fcsp dhchap password rtp9216
```

ステップ 4　スイッチ WWN デバイス名で表される、ファブリック上の他のスイッチのパスワードを設定します。

```
switch(config)# fcsp dhchap devicename 20:00:00:05:30:00:38:5e password rtp9509
```

ステップ 5　目的のファイバ チャネル インターフェイスの DHCHAP モードをイネーブルにします。

（注）　DHCHAP ポート モードを off モード以外のモードに変更すると、再認証が実行されます。

```
switch(config)# interface fc2/4
switch(config-if)# fcsp on
```

ステップ 6　DHCHAP ローカル パスワード データベースを表示して、このスイッチに設定されたプロトコル セキュリティ情報を確認します。

```
switch# show fcsp dhchap database
DHCHAP Local Password:
        Non-device specific password:*******
Other Devices' Passwords:
        Password for device with WWN:20:00:00:05:30:00:38:5e is *******
```

ステップ 7　ファイバ チャネル インターフェイスの DHCHAP 設定を表示します。

```
switch# show fcsp interface fc2/4
fc2/4
        fcsp authentication mode:SEC_MODE_ON
        Status:Successfully authenticated
```

ステップ 8　接続先の MDS 9509 スイッチでこれらの手順を繰り返します。

```
MDS-9509# show wwn switch
Switch WWN is 20:00:00:05:30:00:38:5e
MDS-9509(config)# fcsp enable
MDS-9509(config)# fcsp dhchap password rtp9509
MDS-9509(config)# fcsp dhchap devicename 20:00:00:05:30:00:54:de password rtp9216
MDS-9509(config)# interface fc 4/5
MDS-9509(config-if)# fcsp on
MDS-9509# show fcsp dhchap database
DHCHAP Local Password:
        Non-device specific password:*******
Other Devices' Passwords:
        Password for device with WWN:20:00:00:05:30:00:54:de is *******
MDS-9509# show fcsp interface fc2/4
Fc2/4
        fcsp authentication mode:SEC_MODE_ON
        Status:Successfully authenticated
```

これで、図 44-2 に示す設定例の DHCHAP 認証のイネーブル化と設定の作業が終わります。

デフォルト設定

表 44-2 に、スイッチのすべてのファブリック セキュリティ機能のデフォルト設定値を示します。

表 44-2　デフォルトのファブリック セキュリティ設定値

パラメータ	デフォルト
DHCHAP 機能	Disabled
DHCHAP ハッシュ アルゴリズム	最初に MD5、次に SHA-1 のプライオリティ リストで DHCHAP 認証を実行
DHCHAP 認証モード	auto-passive
DHCHAP グループのデフォルトの交換プライオリティ	0、4、1、2、3 の順
DHCHAP タイムアウト値	30 秒

CHAPTER 45

ポート セキュリティの設定

Cisco Nexus 5000 シリーズ スイッチには、侵入の試みを拒否して管理者に報告するポート セキュリティ機能が組み込まれています。

（注） ポート セキュリティは、仮想ファイバ チャネル ポートと物理ファイバ チャネル ポートでサポートされます。

この章は、次の項で構成されています。

- ポート セキュリティについて（45-1 ページ）
- ポート セキュリティの設定（45-3 ページ）
- ポート セキュリティのイネーブル化（45-6 ページ）
- ポート セキュリティのアクティベーション（45-6 ページ）
- 自動学習（45-8 ページ）
- ポート セキュリティの手動設定（45-11 ページ）
- ポート セキュリティ設定の配信（45-13 ページ）
- データベース結合に関する注意事項（45-16 ページ）
- データベースの相互作用（45-16 ページ）
- ポート セキュリティ設定の表示（45-20 ページ）
- デフォルト設定（45-21 ページ）

ポート セキュリティについて

通常、SAN 内のすべてのファイバ チャネル デバイスを任意の SAN スイッチ ポートに接続して、ゾーン メンバーシップに基づいて SAN サービスにアクセスできます。ポート セキュリティ機能は、次の方法で Cisco Nexus 5000 シリーズ スイッチのスイッチ ポートへの不正アクセスを防止します。

- 不正なファイバ チャネル デバイス（N ポート）およびスイッチ（xE ポート）からのログイン要求は拒否されます。
- 侵入に関するすべての試みは、システム メッセージを通して SAN 管理者に報告されます。

- 設定配信は CFS インフラストラクチャを使用し、CFS 対応スイッチに制限されています。配信はデフォルトでディセーブルになっています。
- ポート セキュリティ ポリシーを設定するには、ストレージ プロトコル サービス ライセンスが必要です。詳細は、第 4 章「ライセンスの管理」を参照してください。

この項では、次のトピックについて取り上げます。

- ポート セキュリティの実行（45-2 ページ）
- 自動学習の概要（45-2 ページ）
- ポート セキュリティのアクティベーション（45-3 ページ）

ポート セキュリティの実行

ポート セキュリティを実行するには、デバイスおよびスイッチ ポート インターフェイス（これらを通じて各デバイスまたはスイッチが接続される）を設定し、設定をアクティブにします。

- デバイスごとに N ポート接続を指定するには、Port World Wide Name（pWWN）または Node World Wide Name（nWWN）を使用します。
- スイッチごとに xE ポート接続を指定するには、Switch World Wide Name（sWWN）を使用します。

N および xE ポートをそれぞれ設定して、単一ポートまたはポート範囲に限定できます。

ポート セキュリティ ポリシーはポートがアクティブになるたび、およびポートを起動しようとした場合に実行されます。

ポート セキュリティ機能は 2 つのデータベースを使用して、設定の変更を受け入れ、実装します。

- コンフィギュレーション データベース：すべての設定の変更がコンフィギュレーション データベースに保存されます。
- アクティブ データベース：ファブリックが現在実行しているデータベース。ポート セキュリティ機能を実行するには、スイッチに接続されているすべてのデバイスがポート セキュリティ アクティブ データベースに格納されている必要があります。ソフトウェアはこのアクティブ データベースを使用して、認証を行います。

自動学習の概要

指定期間内にポート セキュリティ設定を自動的に学習するように、スイッチを設定できます。この機能を使用すると、任意の Cisco Nexus 5000 シリーズ スイッチで、接続先のデバイスおよびスイッチについて自動的に学習できます。ポート セキュリティ機能を初めてアクティブにするときに、この機能を使用してください。ポートごとに手動で設定する面倒な作業が軽減されます。自動学習は、VSAN 単位で設定する必要があります。この機能をイネーブルにすると、ポート アクセスを設定していない場合でも、スイッチに接続可能なデバイスおよびスイッチが自動学習されます。

自動学習がイネーブルのときは、まだスイッチにログインしていないデバイスまたはインターフェイスに関する学習だけ実行されます。自動学習がまだイネーブルなときにポートをシャットダウンすると、そのポートに関する学習エントリが消去されます。

学習は、既存の設定済みのポート セキュリティ ポリシーを上書きしません。たとえば、インターフェイスが特定の pWWN を許可するように設定されている場合、自動学習がエントリを追加して、そのインターフェイス上の他の pWWN を許可することはありません。他のすべての pWWN は、自動学習モードであってもブロックされます。

シャットダウン状態のポートについては、学習エントリは作成されません。

ポート セキュリティ機能をアクティブにすると、自動学習も自動的にイネーブルになります。

（注）　ポート セキュリティをアクティブにする前に自動学習をイネーブルにする場合、自動学習をディセーブルにするまでポート セキュリティをアクティブにできません。

ポート セキュリティのアクティベーション

デフォルトでは、ポート セキュリティ機能が Cisco Nexus 5000 シリーズ スイッチでアクティブにされていません。

ポート セキュリティ機能をアクティブにすると、次のようになります。

- 自動学習も自動的にイネーブルになります。つまり、
  - この時点から、まだスイッチにログインしていないデバイスまたはインターフェイスに対してだけ自動学習が行われます。
  - 自動学習をディセーブルにするまで、データベースをアクティブにできません。
- すでにログインしているすべてのデバイスは学習され、アクティブ データベースに追加されます。
- 設定済みデータベースのすべてのエントリがアクティブ データベースにコピーされます。

データベースをアクティブにすると、以降のデバイスのログインは、自動学習されたエントリを除き、アクティブ化されたポートによってバインドされた WWN ペアの対象になります。自動学習されたエントリがアクティブになる前に、自動学習をディセーブルにする必要があります。

ポート セキュリティ機能をアクティブにすると、自動学習も自動的にイネーブルになります。ポート セキュリティ機能をアクティブにし、自動学習をディセーブルにすることもできます。

ヒント　ポートがログインを拒否されて停止している場合、その後でログインを許可するようにデータベースを設定しても、ポートは自動的に起動しません。明示的に **no shutdown** CLI コマンドを入力して、そのポートをオンラインに戻す必要があります。

ポート セキュリティの設定

ポート セキュリティを設定する手順は、使用する機能によって異なります。CFS 配信を使用している場合、自動学習の動作が異なります。

この項では、次のトピックについて取り上げます。

- 自動学習と CFS 配信を使用する場合のポート セキュリティの設定（45-4 ページ）
- 自動学習を使用し、CFS を使用しない場合のポート セキュリティの設定（45-4 ページ）
- 手動データベース設定を使用する場合のポート セキュリティの設定（45-5 ページ）

自動学習と CFS 配信を使用する場合のポート セキュリティの設定

自動学習と CFS 配信を使用する場合にポート セキュリティを設定するには、次の手順に従ってください。

ステップ 1　ポート セキュリティをイネーブルにします。

「ポート セキュリティのイネーブル化」セクション（45-6 ページ）を参照してください。

ステップ 2　CFS 配信をイネーブルにします。

「配信のイネーブル化」セクション（45-13 ページ）を参照してください。

ステップ 3　各 VSAN で、ポート セキュリティをアクティブにします。

デフォルトで自動学習が有効になります。「ポート セキュリティのアクティブ化」セクション（45-6 ページ）を参照してください。

ステップ 4　CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。

「変更のコミット」セクション（45-14 ページ）を参照してください。すべてのスイッチで、ポート セキュリティがアクティブになり、自動学習がイネーブルになります。

ステップ 5　すべてのスイッチとすべてのホストが自動的に学習されるまで待ちます。

ステップ 6　各 VSAN で、自動学習をディセーブルにします。

「自動学習のディセーブル化」セクション（45-9 ページ）を参照してください。

ステップ 7　CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。

「変更のコミット」セクション（45-14 ページ）を参照してください。すべてのスイッチから自動学習されたエントリが、すべてのスイッチへ配信されるスタティックなアクティブ データベースに集約されます。

ステップ 8　各 VSAN のコンフィギュレーション データベースにアクティブ データベースをコピーします。

「ポート セキュリティ データベースのコピー」セクション（45-19 ページ）を参照してください。

ステップ 9　CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。

「変更のコミット」セクション（45-14 ページ）を参照してください。これで、ファブリック内のすべてのスイッチのコンフィギュレーション データベースが同一になります。

ステップ 10　ファブリック オプションを使用して、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

これで、ファブリック内のすべてのスイッチのスタートアップ コンフィギュレーションにポート セキュリティ コンフィギュレーション データベースが保存されます。

自動学習を使用し、CFS を使用しない場合のポート セキュリティの設定

自動学習を使用し、CFS を使用しない場合にポート セキュリティを設定するには、次の手順に従ってください。

ステップ 1　ポート セキュリティをイネーブルにします。

「ポート セキュリティのイネーブル化」セクション（45-6 ページ）を参照してください。

ステップ 2　各 VSAN で、ポート セキュリティをアクティブにします。デフォルトで自動学習が有効になります。

「ポート セキュリティのアクティブ化」セクション（45-6 ページ）を参照してください。

ステップ 3　すべてのスイッチとすべてのホストが自動的に学習されるまで待ちます。

ステップ 4　各 VSAN で、自動学習をディセーブルにします。

「自動学習のディセーブル化」セクション（45-9 ページ）を参照してください。

ステップ 5　各 VSAN のコンフィギュレーション データベースにアクティブ データベースをコピーします。

「ポート セキュリティ データベースのコピー」セクション（45-19 ページ）を参照してください。

ステップ 6　実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。これにより、ポート セキュリティ コンフィギュレーション データベースがスタートアップ コンフィギュレーションに保存されます。

ステップ 7　ファブリック内のすべてのスイッチについて、ステップ 1 ～ステップ 6 を繰り返します。

手動データベース設定を使用する場合のポート セキュリティの設定

手動でポート セキュリティ データベースを設定する場合にポート セキュリティを設定するには、次の手順に従ってください。

ステップ 1　ポート セキュリティをイネーブルにします。

「ポート セキュリティのイネーブル化」セクション（45-6 ページ）を参照してください。

ステップ 2　各 VSAN のコンフィギュレーション データベースにすべてのポート セキュリティ エントリを手動で設定します。

「手動データベース設定を使用する場合のポート セキュリティの設定」セクション（45-5 ページ）を参照してください。

ステップ 3　各 VSAN で、ポート セキュリティをアクティブにします。デフォルトで自動学習が有効になります。

「自動学習のディセーブル化」セクション（45-9 ページ）を参照してください。

ステップ 4　各 VSAN で、自動学習をディセーブルにします。

「自動学習のディセーブル化」セクション（45-9 ページ）を参照してください。

ステップ 5　実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。これにより、ポート セキュリティ コンフィギュレーション データベースがスタートアップ コンフィギュレーションに保存されます。

ステップ 6　ファブリック内のすべてのスイッチについて、ステップ 1 ～ステップ 5 を繰り返します。

ポート セキュリティのイネーブル化

デフォルトでは、ポート セキュリティ機能が Cisco Nexus 5000 シリーズ スイッチでディセーブルです。

ポート セキュリティをイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# port-security enable`	スイッチ上でポート セキュリティをイネーブルにします。
	`switch(config)# no port-security enable`	スイッチ上でポート セキュリティをディセーブル（デフォルト）にします。

ポート セキュリティのアクティベーション

この項では、次のトピックについて取り上げます。

- ポート セキュリティのアクティブ化（45-6 ページ）
- データベースのアクティベーションの拒否（45-6 ページ）
- ポート セキュリティのアクティベーションの強制（45-7 ページ）
- データベースのリアクティベーション（45-7 ページ）

ポート セキュリティのアクティブ化

ポート セキュリティをアクティブにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# port-security activate vsan` *vsan-id*	指定された VSAN のポート セキュリティ データベースをアクティブにし、自動的に自動学習をイネーブルにします。
	`switch(config)# port-security activate vsan` *vsan-id* `no-auto-learn`	指定された VSAN のポート セキュリティ データベースをアクティブにし、自動学習をディセーブルにします。
	`switch(config)# no port-security activate vsan` *vsan-id*	指定された VSAN のポート セキュリティ データベースを無効にし、自動的に自動学習をディセーブルにします。

データベースのアクティベーションの拒否

次の場合は、データベースをアクティブ化しようとしても、拒否されます。

- 存在しないエントリや矛盾するエントリがコンフィギュレーション データベースにあるが、アクティブ データベースにはない場合。
- アクティベーションの前に、自動学習機能がイネーブルに設定されていた場合。この状態のデータベースを再アクティブ化するには、自動学習をディセーブルにします。

- 各ポート チャネル メンバに正確なセキュリティが設定されていない場合。
- 設定済みデータベースが空であり、アクティブ データベースが空でない場合。

上記のような矛盾が 1 つ以上発生したためにデータベース アクティベーションが拒否された場合は、ポート セキュリティ アクティベーションを強制して継続することができます。

ポート セキュリティのアクティベーションの強制

ポート セキュリティ アクティベーション要求が拒否された場合は、アクティベーションを強制できます。

（注） アクティベーションを強制すると、既存のデバイスがアクティブ データベースに違反したときに既存のデバイスがログアウトされます。

存在しないエントリや矛盾するエントリを表示するには、EXEC モードで **port-security database diff active vsan** コマンドを使用します。

ポート セキュリティ データベースを強制的にアクティブにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configuration terminal`** `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`port-security activate vsan`** *`vsan-id`* **`force`**	矛盾がある場合でも、指定された VSAN のポート セキュリティ データベースを強制的にアクティブにします。

データベースのリアクティベーション

ヒント **自動学習がイネーブルの場合**、force オプションを使用しないと、自動学習をディセーブルにするまでデータベースをアクティブにできません。

ポート セキュリティ データベースを再度アクティブにする手順は、次のとおりです。

ステップ 1 自動学習をディセーブルにします。

ステップ 2 設定済みデータベースにアクティブ データベースをコピーします。

ヒント アクティブ データベースが空の場合は、この手順を実行できません。

ステップ 3 コンフィギュレーション データベースに必要な変更を加えます。

ステップ 4 データベースをアクティブにします

ポート セキュリティ データベースを再度アクティブにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configuration terminal`** `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`no port-security auto-learn vsan`** *`vsan-id`*	自動学習をディセーブルにし、スイッチにアクセスする新規デバイスをスイッチが学習しないように設定します。この時点までに学習されたデバイスに基づいて、データベースの内容を処理します。
ステップ 3	`switch(config)#` **`exit`** `switch#` **`port-security database copy vsan`** *`vsan-id`*	アクティブ データベースから設定済みデータベースにコピーします。
ステップ 4	`switch#` **`configuration terminal`** `switch(config)#` **`port-security activate vsan`** *`vsan-id`*	指定された VSAN のポート セキュリティ データベースをアクティブにし、自動的に自動学習をイネーブルにします。

自動学習

この項では、次のトピックについて取り上げます。

- 自動学習のイネーブル化について（45-8 ページ）
- 自動学習のイネーブル化（45-9 ページ）
- 自動学習のディセーブル化（45-9 ページ）
- 自動学習デバイスの許可（45-9 ページ）
- 許可される場合（45-10 ページ）

自動学習のイネーブル化について

自動学習設定の状態は、ポート セキュリティ機能の状態によって異なります。

- ポート セキュリティ機能がアクティブでない場合、自動学習はデフォルトでディセーブルです。
- ポート セキュリティ機能がアクティブである場合、自動学習はデフォルトでイネーブルです（このオプションを明示的にディセーブルにしていない場合）。

ヒント　VSAN 上で自動学習がイネーブルの場合、**force** オプションを使用して、この VSAN のデータベースだけをアクティブにできます。

自動学習のイネーブル化

自動学習をイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# port-security auto-learn vsan` *vsan-id*	自動学習をイネーブルにして、VSAN 1 へのアクセスが許可されたすべてのデバイスについて、スイッチが学習できるようにします。これらのデバイスは、ポート セキュリティ アクティブ データベースに記録されます。

自動学習のディセーブル化

自動学習をディセーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# no port-security auto-learn vsan` *vsan-id*	自動学習をディセーブルにし、スイッチにアクセスする新規デバイスをスイッチが学習しないように設定します。この時点までに学習されたデバイスに基づいて、データベースの内容を処理します。

自動学習デバイスの許可

表 45-1 に、デバイス要求に対して接続が許可される条件をまとめます。

表 45-1　許可される自動学習デバイス要求

状態	デバイス（pWWN、nWWN、sWWN）	接続先	許可
1	1 つまたは複数のスイッチ ポートに設定されている場合	設定済みスイッチ ポート	許可
2		他のすべてのスイッチ ポート	拒否
3	設定されていない場合	設定されていないスイッチ ポート	許可される条件: 自動学習が有効
4			拒否される条件: 自動学習が無効
5	設定されている場合、または設定されていない場合	任意のデバイスを接続許可するスイッチ ポート	許可
6		スイッチ上の任意のポート	許可
7	設定されていない場合任意のスイッチ ポートにログインするように設定されている場合	その他のデバイスが設定されたポート	拒否

許可される場合

ポート セキュリティ機能がアクティブで、アクティブ データベースに次の条件が指定されていることが前提です。

- pWWN(P1)には、インターフェイス fc2/1(F1)からアクセスできます。
- pWWN(P2)には、インターフェイス fc2/2(F1)からアクセスできます。
- nWWN(N1)には、インターフェイス fc2/2(F2)からアクセスできます。
- インターフェイス vfc3/1(F3)からは、任意の WWN にアクセスできます。
- nWWN(N3)には、任意のインターフェイスからアクセスできる。
- pWWN(P3)には、インターフェイス fc2/4(F4)からアクセスできます。
- sWWN(S1)には、インターフェイス fc3/1 ～ 3(F10 ～ F13)からアクセスできます。
- pWWN(P10)には、インターフェイス vfc4/1(F11)からアクセスできます。

表 45-2 に、このアクティブ データベースに対するポート セキュリティ許可の結果をまとめます。ここに示す条件は、表 45-1 の条件を参照しています。

表 45-2　各シナリオの許可結果

デバイス接続要求	許可	状態	理由
P1、N2、F1	許可	1	競合しません。
P2、N2、F1	許可	1	競合しません。
P3、N2、F1	拒否	2	F1 が P1/P2 にバインドされています。
P1、N3、F1	許可	6	N3 に関するワイルドカード一致です。
P1、N1、F3	許可	5	F3 に関するワイルドカード一致です。
P1、N4、F5	拒否	2	P1 が F1 にバインドされています。
P5、N1、F5	拒否	2	N1 は F2 でだけ許可されます。
P3、N3、F4	許可	1	競合しません。
S1、F10	許可	1	競合しません。
S2、F11	拒否	7	P10 が F11 にバインドされています。
P4、N4、F5(自動学習が有効)	許可	3	競合しません。
P4、N4、F5(自動学習が無効)	拒否	4	一致しません。
S3、F5(自動学習が有効)	許可	3	競合しません。
S3、F5(自動学習が無効)	拒否	4	一致しません。
P1、N1、F6(自動学習が有効)	拒否	2	P1 が F1 にバインドされています。
P5、N5、F1(自動学習が有効)	拒否	7	P1 と P2 だけが F1 にバインドされています。
S3、F4(自動学習が有効)	拒否	7	P3 と F4 がペアになります。

表 45-2　各シナリオの許可結果（続き）

デバイス接続要求	許可	状態	理由
S1、F3（自動学習が有効）	許可	5	競合しません。
P5、N3、F3	許可	6	F3 および N3 に関するワイルドカード (*) 一致です。
P7、N3、F9	許可	6	N3 に関するワイルドカード (*) が一致しています。

ポート セキュリティの手動設定

Cisco Nexus 5000 シリーズ スイッチにポート セキュリティを設定する手順は、次のとおりです。

ステップ 1　保護する必要があるポートの WWN を識別します。

「許可済みのポート ペアの追加」セクション（45-12 ページ）を参照してください。

ステップ 2　許可された nWWN または pWWN に対して fWWN を保護します。

ステップ 3　ポート セキュリティ データベースをアクティブにします。

ステップ 4　設定を確認します。

この項では、次のトピックについて取り上げます。

- WWN の識別に関する注意事項（45-11 ページ）
- 許可済みのポート ペアの追加（45-12 ページ）

WWN の識別に関する注意事項

ポート セキュリティを手動で設定する場合は、次に従い行ってください。

- インターフェイスまたは fWWN でスイッチ ポートを識別します。
- pWWN または nWWN でデバイスを識別します。
- N ポートが SAN スイッチ ポート F にログインできる場合、その N ポートは指定された F ポートを介してだけログインできます。
- N ポートの nWWN が F ポート WWN にバインドされている場合、N ポートのすべての pWWN は暗黙的に F ポートとペアになります。
- TE ポート チェックは、VSAN トランク ポートの許可 VSAN リスト内の VSAN ごとに実行されます。
- 同じ SAN ポートチャネル内のすべてのポートチャネル xE ポートに、同じ WWN セットを設定する必要があります。
- E ポートのセキュリティは、E ポートのポート VSAN に実装されます。この場合、sWWN を使用して許可チェックを保護します。

- アクティブ化されたコンフィギュレーション データベースは、アクティブ データベースに影響を与えることなく変更できます。
- 実行コンフィギュレーションを保存することにより、コンフィギュレーション データベースおよびアクティブ データベース内のアクティブ化されたエントリを保存します。アクティブ データベース内の学習済みエントリは保存されません。

許可済みのポート ペアの追加

バインドする必要がある WWN ペアを識別したら、これらのペアをポート セキュリティ データベースに追加します。

ヒント　リモート スイッチのバインドは、ローカル スイッチで指定できます。リモート インターフェイスを指定する場合、fWWN または sWWN インターフェイスの組み合わせを使用できます。

ポート セキュリティに関して許可済みのポート ペアを追加する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configuration terminal** switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **port-security database vsan** *vsan-id* switch(config-port-security)#	指定された VSAN に対してポート セキュリティ データベース モードを開始します。
	switch(config)# **no port-security database vsan** *vsan-id* switch(config)#	指定された VSAN からポート セキュリティ コンフィギュレーション データベースを削除します。
ステップ 3	switch(config-port-security)# **swwn** *swwn-id* **interface san-port-channel 5**	SAN ポート チャネル 5 を介した場合だけログインするように、指定された sWWN を設定します。
ステップ 4	switch(config-port-security)# **any-wwn interface fc** *slot/port* **- fc** *slot/port*	指定されたインターフェイスを介してログインするようにすべての WWN を設定します。

次に、VSAN 2 に対してポート セキュリティ データベース モードを開始する例を示します。

```
switch(config)# port-security database vsan 2
```

次に、SAN ポート チャネル 5 を介した場合だけログインするように、指定された sWWN を設定する例を示します。

```
switch(config-port-security)# swwn 20:01:33:11:00:2a:4a:66 interface san-port-channel 5
```

次に、指定されたスイッチの指定されたインターフェイスを介してログインするように、指定された pWWN を設定する例を示します。

```
switch(config-port-security)# pwwn 20:11:33:11:00:2a:4a:66 swwn 20:00:00:0c:85:90:3e:80
interface fc 3/2
```

次に、任意のスイッチの指定されたインターフェイスを介してログインするようにすべての WWN を設定する例を示します。

```
switch(config-port-security)# any-wwn interface fc slot/port
```

ポート セキュリティ設定の配信

ポート セキュリティ機能は Cisco Fabric Services（CFS）インフラストラクチャを使用して効率的なデータベース管理を実現し、VSAN 内のファブリック全体にシングル ポイントの設定を提供します。また、ファブリック全体でポート セキュリティ ポリシーを実行します（第 21 章「CFS の使用」を参照）。

ここでは、次の内容について説明します。

- 配信のイネーブル化（45-13 ページ）
- ファブリックのロック（45-14 ページ）
- 変更のコミット（45-14 ページ）
- 変更の廃棄（45-14 ページ）
- アクティベーション設定と自動学習設定の配信（45-14 ページ）

配信のイネーブル化

配信モードで実行されたすべての設定は保留中の（一時的な）データベースに保存されます。設定を変更する場合、設定に対して保留中のデータベースの変更をコミットまたは廃棄する必要があります。その間、ファブリックはロックされた状態になります。保留中のデータベースへの変更は、変更をコミットするまで設定に反映されません。

（注） CFS 配信がイネーブルの場合、ポートのアクティベーションまたは非アクティベーションおよび自動学習のイネーブル化またはディセーブル化は、CFS コミットを発行するまで有効になりません。常に CFS コミットとこれらの処理のいずれかを使用して、正しい設定を確認してください。「アクティベーション設定と自動学習設定の配信」セクション（45-14 ページ）を参照してください。

たとえば、ポート セキュリティをアクティブにし、自動学習をディセーブルにし、最後に保留状態のデータベースに変更をコミットすると、**port-security activate vsan** *vsan-id* **no-auto-learn** コマンドを入力した場合と同じ結果になります。

ヒント ポート セキュリティをアクティブにし、自動学習をイネーブルにしたあとに、コミットを実行することを推奨します。

ポート セキュリティ データベースを再度アクティブにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# port-security distribute`	配信をイネーブルにします。
	`switch(config)# no port-security distribute`	配信をディセーブルにします。

ファブリックのロック

既存の設定を変更するときの最初のアクションが実行されると、保留中のデータベースが作成され、VSAN 内の機能がロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザがこの機能の設定に変更を加えることができなくなります。
- コンフィギュレーション データベースのコピーが保留中のデータベースになります。

変更のコミット

設定に加えられた変更をコミットする場合、保留中のデータベースの設定が他のスイッチに配信されます。コミットが正常に行われると、設定の変更がファブリック全体に適用され、ロックが解除されます。

指定された VSAN のポート セキュリティ設定の変更をコミットする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configuration terminal`** `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`port-security commit vsan`** *`vsan-id`*	指定された VSAN のポート セキュリティの変更をコミットします。

変更の廃棄

保留中のデータベースに加えられた変更を廃棄（中断）する場合、設定は影響されないまま、ロックが解除されます。

指定された VSAN のポート セキュリティ設定の変更を廃棄する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configuration terminal`** `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)#` **`port-security abort vsan`** *`vsan-id`*	指定された VSAN のポート セキュリティの変更を廃棄し、保留中のコンフィギュレーション データベースをクリアします。

アクティベーション設定と自動学習設定の配信

配信モードのアクティベーション設定および自動学習設定は、保留中のデータベースの変更をコミットするときに実行する処理として記憶されます。

学習済みエントリは一時的なもので、ログインを許可するか否かを決定するロールを持ちません。そのため、学習済みエントリは配信に参加しません。学習をディセーブルにし、保留中のデータベースの変更をコミットする場合、学習済みエントリはアクティブ データベース内のスタティック エントリになり、ファブリック内のすべてのスイッチに配信されます。コミット後、すべてのスイッチのアクティブ データベースが同一になり、学習をディセーブルにできます。

保留中のデータベースに複数のアクティベーションおよび自動学習設定が含まれる場合、変更をコミットすると、アクティベーションおよび自動学習の変更が統合され、動作が変化する場合があります（表 45-3を参照）。

表 45-3　配信モードのアクティベーション設定および自動学習設定のシナリオ

シナリオ	アクションs	配信がオフの場合	配信がオンの場合
コンフィギュレーション データベースに A および B が存在し、アクティベーションが行われておらず、デバイス C および D がログインされています。	**1.** ポート セキュリティ データベースをアクティブにし、自動学習をイネーブルにします。	コンフィギュレーション データベース = {A、B} アクティブ データベース = {A、B、C[1]、D*}	コンフィギュレーション データベース = {A、B} アクティブ データベース = {ヌル} 保留中のデータベース = {A、B + アクティベーション（イネーブル）}
	2. 新規のエントリ E がコンフィギュレーション データベースに追加されました。	コンフィギュレーション データベース = {A、B、E} アクティブ データベース = {A、B、C*、D*}	コンフィギュレーション データベース = {A、B} アクティブ データベース = {ヌル} 保留中のデータベース = {A、B、E + アクティベーション（イネーブル）}
	3. コミットを行います。	N/A	コンフィギュレーション データベース = {A、B、E} アクティブ データベース = {A、B、E、C*、D*} 保留中のデータベース = 空の状態
コンフィギュレーション データベースに A および B が存在し、アクティベーションが行われておらず、デバイス C および D がログインされています。	**1.** ポート セキュリティ データベースをアクティブにし、自動学習をイネーブルにします。	コンフィギュレーション データベース = {A、B} アクティブ データベース = {A、B、C*、D*}	コンフィギュレーション データベース = {A、B} アクティブ データベース = {ヌル} 保留中のデータベース = {A、B + アクティベーション（イネーブル）}
	2. 学習をディセーブルにします。	コンフィギュレーション データベース = {A、B} アクティブ データベース = {A、B、C、D}	コンフィギュレーション データベース = {A、B} アクティブ データベース = {ヌル} 保留中のデータベース = {A、B + アクティベーション（イネーブル）+ 学習（ディセーブル）}
	3. コミットを行います。	N/A	コンフィギュレーション データベース = {A、B} アクティブ データベース = {A、B}、デバイス C および D がログアウトされます。これは、自動学習をディセーブルにした場合のアクティベーションと同じです。 保留中のデータベース = 空の状態

1. *（アスタリスク）は学習されたエントリを意味します。

データベース結合に関する注意事項

データベースのマージとは、コンフィギュレーション データベースとアクティブ データベース内のスタティック（学習されていない）エントリの統合を指します。概念の詳細については、「CFS 結合のサポート」セクション（21-6 ページ）を参照してください。

2 つのファブリック間のデータベースをマージする場合は、次のことに気をつけて行ってください。

- アクティベーション ステータスと自動学習ステータスが両方のファブリックで同じであることを確認します。
- 両方のデータベースの各 VSANの 設定を合わせた数が 2000 を超えていないことを確認します。

注意　この 2 つの条件に従わない場合は、マージに失敗します。次の 配信がデータベースとファブリック内のアクティベーション ステートを強制的に同期化します。

データベースの相互作用

表 45-4 に、アクティブ データベースとコンフィギュレーション データベース間の相違、および相互作用を示します。

表 45-4　アクティブおよびコンフィギュレーション ポート セキュリティ データベース

アクティブ データベース	コンフィギュレーション データベース
読み取り専用。	読み取りと書き込み。
設定を保存すると、アクティブなエントリだけが保存されます。学習済みエントリは保存されません。	設定を保存すると、コンフィギュレーション データベース内のすべてのエントリが保存されます。
アクティブ化すると、VSAN にログイン済みのすべてのデバイスも学習され、アクティブ データベースに追加されます。	アクティブ化されたコンフィギュレーション データベースは、アクティブ データベースに影響を与えることなく変更できます。
アクティブ データベースを設定済みデータベースで上書きするには、ポート セキュリティ データベースをアクティブ化します。強制的にアクティブにすると、アクティブ データベースの設定済みエントリに違反が生じることがあります。	コンフィギュレーション データベースをアクティブ データベースで上書きできます。

（注）　**port-security database copy vsan** コマンドを使用すると、コンフィギュレーション データベースをアクティブ データベースで上書きできます。アクティブ データベースとコンフィギュレーション データベースとの相違を表示するには、EXEC モードで **port-security database diff active vsan** コマンドを使用します。

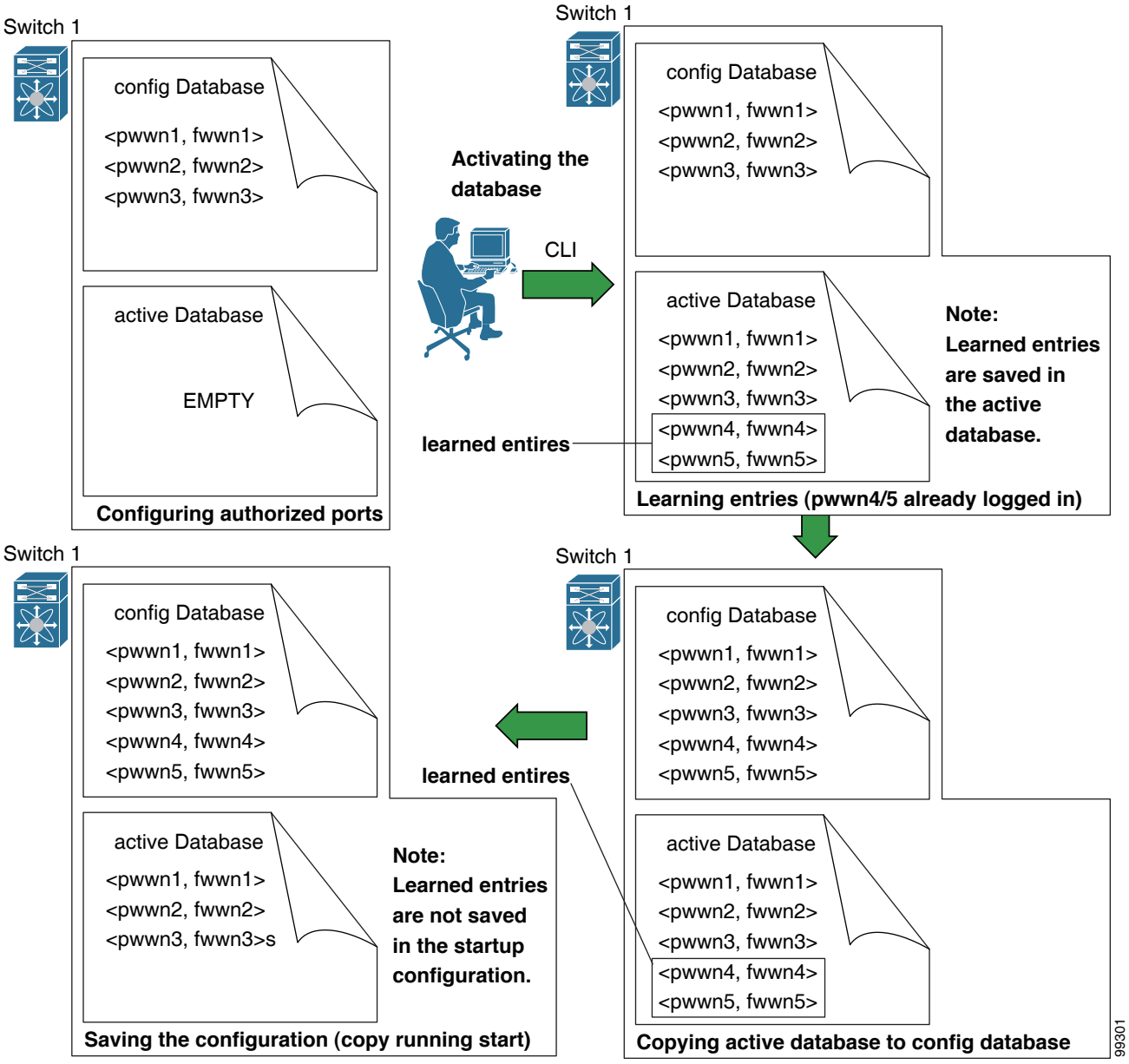
この項では、次のトピックについて取り上げます。

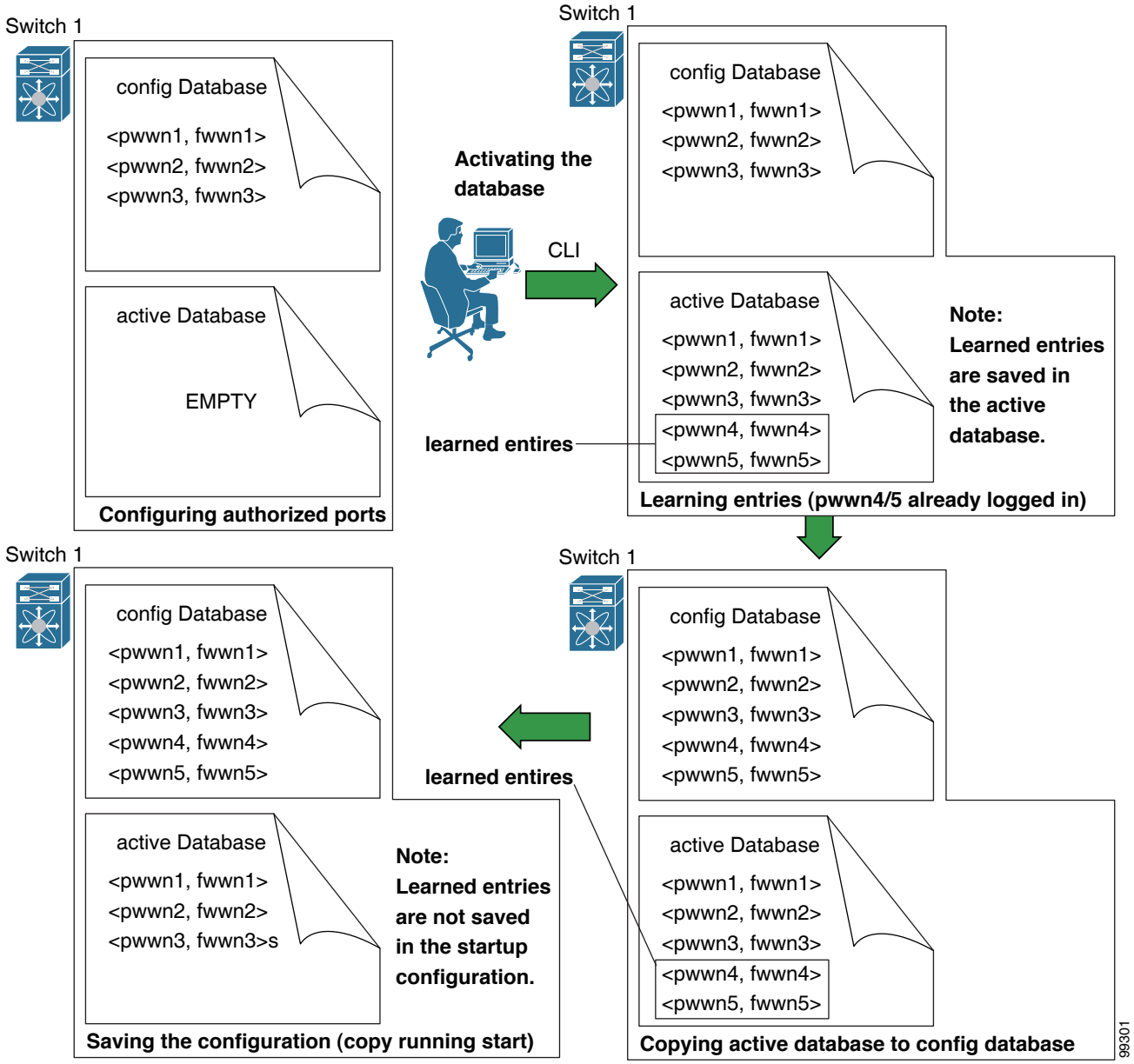
- データベースのシナリオ（45-17 ページ）
- ポート セキュリティ データベースのコピー（45-19 ページ）
- ポート セキュリティ データベースの削除（45-19 ページ）
- ポート セキュリティ データベースのクリア（45-19 ページ）

データベースのシナリオ

図 45-1 の各シナリオでは、ポート セキュリティ設定に基づくアクティブ データベースとコンフィギュレーション データベースのステータスを示します。

図 45-1　　ポート セキュリティ データベースのシナリオ




Switch 1
config Database
<pwwn1, fwwn1>
<pwwn2, fwwn2>
<pwwn3, fwwn3>
active Database
EMPTY
Configuring authorized ports
Activating the database
CLI
Switch 1
config Database
<pwwn1, fwwn1>
<pwwn2, fwwn2>
<pwwn3, fwwn3>
active Database
<pwwn1, fwwn1>
<pwwn2, fwwn2>
<pwwn3, fwwn3>
<pwwn4, fwwn4>
<pwwn5, fwwn5>
learned entires
Note:
Learned entries are saved in the active database.
Learning entries (pwwn4/5 already logged in)
Switch 1
config Database
<pwwn1, fwwn1>
<pwwn2, fwwn2>
<pwwn3, fwwn3>
<pwwn4, fwwn4>
<pwwn5, fwwn5>
active Database
<pwwn1, fwwn1>
<pwwn2, fwwn2>
<pwwn3, fwwn3>
<pwwn4, fwwn4>
<pwwn5, fwwn5>
Copying active database to config database
learned entires
Switch 1
config Database
<pwwn1, fwwn1>
<pwwn2, fwwn2>
<pwwn3, fwwn3>
<pwwn4, fwwn4>
<pwwn5, fwwn5>
active Database
<pwwn1, fwwn1>
<pwwn2, fwwn2>
<pwwn3, fwwn3>s
Note:
Learned entries are not saved in the startup configuration.
Saving the configuration (copy running start)
99301

ポート セキュリティ データベースのコピー

ヒント 自動学習をディセーブルにしてから、アクティブ データベースをコンフィギュレーション データベースにコピーすることをお勧めします。このアクションにより、コンフィギュレーション データベースがアクティブ データベースと確実に同期化されます。配信がイネーブルの場合、このコマンドによってコンフィギュレーション データベースの一時的なコピーが作成され、結果としてファブリックがロックされます。ファブリックをロックする場合、すべてのスイッチのコンフィギュレーション データベースに変更をコミットする必要があります。

アクティブ データベースから設定済みデータベースにコピーするには、**port-security database copy vsan** コマンドを使用します。アクティブ データベースが空の場合、このコマンドは受け付けられません。

```
switch# port-security database copy vsan 1
```

アクティブ データベースとコンフィギュレーション データベースとの相違を表示するには、**port-security database diff active vsan** コマンドを使用します。このコマンドは、矛盾を解決する場合に使用できます。

```
switch# port-security database diff active vsan 1
```

コンフィギュレーション データベースとアクティブ データベースとの違いに関する情報を表示するには、**port-security database diff config vsan** コマンドを使用します。

```
switch# port-security database diff config vsan 1
```

ポート セキュリティ データベースの削除

ヒント 配信がイネーブルの場合、削除によってデータベースのコピーが作成されます。実際にデータベースを削除するには、明示的に **port-security commit** コマンドを入力する必要があります。

指定された VSAN の設定済みデータベースを削除するには、コンフィギュレーション モードで **no port-security database vsan** コマンドを使用します。

```
switch(config)# no port-security database vsan 1
```

ポート セキュリティ データベースのクリア

指定された VSAN のポート セキュリティ データベースから既存の統計情報をすべてクリアするには、**clear port-security statistics vsan** コマンドを使用します。

```
switch# clear port-security statistics vsan 1
```

VSAN 内の指定されたインターフェイスに関するアクティブ データベース内の学習済みエントリをすべてクリアするには、**clear port-security database auto-learn interface** コマンドを使用します。

```
switch# clear port-security database auto-learn interface fc2/1 vsan 1
```

VSAN 全体に関するアクティブ データベース内の学習済みエントリをすべてクリアするには、**clear port-security database auto-learn vsan** コマンドを使用します。

```
switch# clear port-security database auto-learn vsan 1
```

（注）**clear port-security database auto-learn** および **clear port-security statistics** コマンドはローカルスイッチだけに関連するので、ロックを取得しません。また、学習済みエントリはスイッチにだけローカルで、配信に参加しません。

VSAN 内で、任意のスイッチから VSAN の保留中のセッションをクリアするには、**port-security clear vsan** コマンドを使用します。

```
switch# clear port-security session vsan 5
```

ポート セキュリティ設定の表示

show port-security database コマンドを実行すると、設定されたポート セキュリティ情報が表示されます。**show port-security** コマンドで fWWN や VSAN、またはインターフェイスや VSAN を指定すると、アクティブなポート セキュリティの出力を表示することもできます。

各ポートのアクセス情報は個別に表示されます。fWWN または interface オプションを指定すると、(その時点で)アクティブ データベース内で指定された fWWN またはインターフェイスとペアになっているすべてのデバイスが表示されます。

次に、ポート セキュリティ コンフィギュレーション データベースを表示する例を示します。

```
switch# show port-security database
```

次に、VSAN 1 のポート セキュリティ コンフィギュレーション データベースを表示する例を示します。

```
switch# show port-security database vsan 1
```

次に、アクティブなデータベースを表示する例を示します。

```
switch# show port-security database active
```

次に、一時的なコンフィギュレーション データベースとコンフィギュレーション データベースの相違を表示する例を示します。

```
switch# show port-security pending-diff vsan 1
```

次に、VSAN 1 内の設定済み fWWN ポート セキュリティを表示する例を示します。

```
switch# show port-security database fwwn 20:01:00:05:30:00:95:de vsan 1
20:00:00:0c:88:00:4a:e2(swwn)
```

次に、ポート セキュリティ統計情報を表示する例を示します。

```
switch# show port-security statistics
```

次に、アクティブ データベースのステータスおよび自動学習設定を確認する例を示します。

```
switch# show port-security status
```

デフォルト設定

表 45-5 に、スイッチのすべてのポート セキュリティ機能のデフォルト設定値を示します。

表 45-5　セキュリティのデフォルト設定値

パラメータ	デフォルト
Auto-learn	ポート セキュリティがイネーブルの場合は、イネーブル。
Port security	ディセーブル
Distribution	ディセーブル **（注）** 配信をイネーブルにすると、スイッチ上のすべての VSAN の配信がイネーブルになります。

CHAPTER 46

ファブリック バインディングの設定

この章では、Cisco Nexus 5000 シリーズ スイッチに組み込まれたファブリック バインディング機能について説明します。内容は次のとおりです。

- ファブリック バインディングについて（46-1 ページ）
- ファブリック バインディングの設定（46-3 ページ）
- ファブリック バインディング情報の確認（46-7 ページ）
- デフォルト設定（46-7 ページ）

ファブリック バインディングについて

ファブリック バインディング機能を使用すると、ファブリック内で指定されたスイッチ間でだけ、ISL（スイッチ間リンク）をイネーブルにできます。ファブリック バインディングは、VSAN 単位で設定します。

この機能を使用すると、不正なスイッチがファブリックに参加したり、現在のファブリック処理が中断されることがなくなります。Exchange Fabric Membership Data（EFMD）プロトコルが使用されて、許可スイッチ リストがファブリック内のすべてのスイッチで同一になります。

この項では、次のトピックについて取り上げます。

- ライセンス要件（46-1 ページ）
- ポート セキュリティとファブリック バインディングの比較（46-2 ページ）
- ファブリック バインディングの実行（46-2 ページ）

ライセンス要件

ファブリック バインディングを使用するには、ストレージ プロトコル サービス ライセンスが必要です。詳細については、第 4 章「ライセンスの管理」を参照してください。

ポート セキュリティとファブリック バインディングの比較

ポート セキュリティとファブリック バインディングは、相互補完するように設定可能な、2 つの独立した機能です。表 46-1 では、2 つの機能を比較します。

表 46-1　ファブリック バインディングとポート セキュリティの比較

ファブリック バインディング	ポート セキュリティ
一連の sWWN および永続的ドメイン ID を使用します。	pWWN/nWWN または fWWN/sWWN を使用します。
スイッチ レベルでファブリックをバインドします。	インターフェイス レベルでデバイスをバインドします。
ファブリック バインディング データベースに格納された設定済み sWWN にだけ、ファブリックへの参加を許可します。	設定済みの一連のファイバ チャネル デバイスを SAN ポートに論理的に接続できます。WWN またはインターフェイス番号で識別されるスイッチ ポートは、同様に WWN で識別されるファイバ チャネル デバイス（ホストまたは別のスイッチ）に接続されます。これらの 2 つのデバイスをバインドすると、これらの 2 つのポートがグループ（リスト）にロックされます。
VSAN 単位でアクティブ化する必要があります。	VSAN 単位でアクティブ化する必要があります。
ピア スイッチが接続されている物理ポートに関係なく、ファブリックに接続可能な特定のユーザ定義のスイッチを許可します。	別のデバイスを接続できる特定のユーザ定義の物理ポートを許可します。
ログインしているスイッチについて学習しません。	学習モードがイネーブルの場合、ログインしているスイッチまたはデバイスについて学習します。
CFS によって配信できず、ファブリック内の各スイッチで手動で設定する必要があります。	CFS によって配信できます。

ポート レベルの xE ポート検査は、次のとおりです。

- スイッチ ログインは、指定された VSAN にポート セキュリティ バインディングとファブリック バインディングの両方を使用します。
- バインディング検査は、ポート VSAN で次のように実行されます。
  - ポート VSAN での E ポート セキュリティ バインディング検査
  - 許可された各 VSAN での TE ポート セキュリティ バインディング検査

ポート セキュリティはファブリック バインディングを補完する関係にありますが、これらの機能は互いに独立していて、個別にイネーブルまたはディセーブルにできます。

ファブリック バインディングの実行

ファブリック バインディングを実行するには、Switch World Wide Name（sWWN）を設定して、スイッチごとに xE ポート接続を指定します。ファブリック バインディング ポリシーは、ポートがアクティブになるたび、およびポートを起動しようとした場合に実行されます。ファイバ チャネル VSAN では、ファブリック バインディング機能を実行するには、すべての sWWN をスイッチに接続し、ファブリック バインディング アクティブ データベースに格納する必要があります。

ファブリック バインディングの設定

ファブリック バインディング機能を使用すると、ファブリック バインディング設定で指定されたスイッチ間でだけ、ISL をイネーブルにできます。ファブリック バインディングは、VSAN 単位で設定します。

この項では、次のトピックについて取り上げます。

- ファブリック バインディングの設定（46-3 ページ）
- ファブリック バインディングのイネーブル化（46-3 ページ）
- スイッチの WWN リストの概要（46-4 ページ）
- スイッチの WWN リストの設定（46-4 ページ）
- ファブリック バインディングのアクティベーションおよび非アクティベーション（46-5 ページ）
- ファブリック バインディングのアクティベーション（46-5 ページ）
- ファブリック バインディングの強制的なアクティベーション（46-5 ページ）
- ファブリック バインディング設定のコピー（46-6 ページ）
- ファブリック バインディング統計情報のクリア（46-6 ページ）
- ファブリック バインディング データベースの削除（46-6 ページ）

ファブリック バインディングの設定

ファブリック内の各スイッチにファブリック バインディングを設定する手順は、次のとおりです。

ステップ 1　ファブリック設定機能をイネーブルにします。

ステップ 2　ファブリックにアクセス可能なデバイスに sWWN のリスト、および対応するドメイン ID を設定します。

ステップ 3　ファブリック バインディング データベースをアクティブにします。

ステップ 4　ファブリック バインディング アクティブ データベースをファブリック バインディングコンフィギュレーション データベースにコピーします。

ステップ 5　ファブリック バインディング設定を保存します。

ステップ 6　ファブリック バインディング設定を確認します。

ファブリック バインディングのイネーブル化

ファブリック バインディングに参加するファブリック内のスイッチごとに、ファブリック バインディング機能をイネーブルにする必要があります。デフォルトでは、この機能は Cisco Nexus 5000 シリーズ スイッチにおいてディセーブルです。ファブリック バインディング機能に関する設定および確認コマンドを使用できるのは、スイッチ上でファブリック バインディングがイネーブルな場合だけです。この設定をディセーブルにした場合、関連するすべての設定は自動的に廃棄されます。

参加しているスイッチ上でファブリック バインディングをイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fabric-binding enable**	現在のスイッチ上でファブリック バインディングをイネーブルにします。
	switch(config)# **no fabric-binding enable**	現在のスイッチ上でファブリック バインディングをディセーブル(デフォルト)にします。

ファブリック バインディング対応スイッチのファブリック バインディング機能のステータスを確認するには、**show fabric-binding status** コマンドを入力します。

```
switch# show fabric-binding status
VSAN 1:Activated database
VSAN 4:No Active database
```

スイッチの WWN リストの概要

ユーザ指定のファブリック バインディング リストには、ファブリック内の sWWN のリストが含まれています。リストにない sWWN、または許可リストで指定されているドメイン ID と異なるドメイン ID を使用する sWWN がファブリックへの参加を試みると、スイッチとファブリック間の ISL が VSAN 内で自動的に隔離され、スイッチはファブリックへの参加を拒否されます。

スイッチの WWN リストの設定

ファイバ チャネル VSAN 用の sWWN とオプションのドメイン ID のリストを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configuration terminal** switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fabric-binding database vsan** *vsan-id* switch(config-fabric-binding)#	指定された VSAN のファブリック バインディング サブモードを開始します。
	switch(config)# **no fabric-binding database vsan** *vsan-id*	指定された VSAN のファブリック バインディング データベースを削除します。
ステップ 3	switch(config-fabric-binding)# **swwn** *swwn-id* **domain** *domain-id*	設定されたデータベース リストに、特定のドメイン ID 用の別のスイッチの sWWN を追加します。
	switch(config-fabric-binding)# **no swwn** *swwn-id* **domain** *domain-id*	設定されたデータベース リストから、スイッチの sWWN およびドメイン ID を削除します。

次に、ドメイン ID 3 の設定済みのデータベース リストにほかのスイッチの sWWN を設定する例を示します。

```
switch(config)# fabric-binding database vsan 10
switch(config-fabric-binding)# swwn 21:00:05:30:23:1a:11:03 domain 3
```

ファブリック バインディングのアクティベーションおよび非アクティベーション

ファブリック バインディング機能では、コンフィギュレーション データベース（config database）およびアクティブ データベースが維持されます。config database は、実行された設定を収集する読み取りと書き込みのデータベースです。これらの設定を実行するには、データベースをアクティブにする必要があります。データベースがアクティブになると、アクティブ データベースが config database の内容で上書きされます。アクティブ データベースは、ログインを試みる各スイッチをチェックする読み取り専用データベースです。

デフォルトでは、ファブリック バインディング機能は非アクティブです。コンフィギュレーション データベース内の既存のエントリがファブリックの現在の状態と矛盾する場合は、スイッチでファブリック バインディング データベースをアクティブにできません。たとえば、ログイン済みのスイッチの 1 つが config database によってログインを拒否される場合があります。これらの状態を強制的に上書きできます。

（注）　アクティベーションのあと、現在アクティブなデータベースに違反するログイン済みのスイッチは、ログアウトされ、ファブリック バインディング制限によってログインが拒否されたすべてのスイッチは再初期化されます。

ファブリック バインディングのアクティベーション

ファブリック バインディング機能をアクティブにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# fabric-binding activate vsan` *vsan-id*	指定された VSAN のファブリック バインディング データベースをアクティブにします。
	`switch(config)# no fabric-binding activate vsan` *vsan-id*	指定された VSAN のファブリック バインディング データベースを非アクティブにします。

ファブリック バインディングの強制的なアクティベーション

上記のような矛盾が 1 つまたは複数発生したためにデータベースのアクティベーションが拒否された場合は、force オプションを使用してアクティベーションを継続できます。

ファブリック バインディング データベースを強制的にアクティブにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal` `switch(config)#`	コンフィギュレーション モードに入ります。

	コマンド	目的
ステップ 2	switch(config)# **fabric-binding activate vsan** *vsan-id* **force**	指定された VSAN のファブリック バインディング データベースを、設定が許可されない場合でも、強制的にアクティブにします。
	switch(config)# **no fabric-binding activate vsan** *vsan-id* **force**	元の設定状態、または（状態が設定されていない場合は）出荷時の設定に戻します。

ファブリック バインディング設定のコピー

ファブリック バインディング設定をコピーすると、コンフィギュレーション データベースが実行コンフィギュレーションに保存されます。

次のコマンドを使用して、コンフィギュレーション データベースにコピーできます。

- アクティブ データベースからコンフィギュレーション データベースにコピーするには、**fabric-binding database copy vsan** コマンドを使用します。設定されたデータベースが空の場合、このコマンドは受け付けられません。

  switch# **fabric-binding database copy vsan 1**

- アクティブ データベースとコンフィギュレーション データベース間の違いを表示するには、**fabric-binding database diff active vsan** コマンドを使用します。このコマンドは、矛盾を解決する場合に使用できます。

  switch# **fabric-binding database diff active vsan 1**

- コンフィギュレーション データベースとアクティブ データベース間の違いに関する情報を表示するには、**fabric-binding database diff config vsan** コマンドを使用します。

  switch# **fabric-binding database diff config vsan 1**

- 再起動後にファブリック バインディングのコンフィギュレーション データベースを使用できるように、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存するには、**copy running-config startup-config** コマンドを使用します。

  switch# **copy running-config startup-config**

ファブリック バインディング統計情報のクリア

指定された VSAN のファブリック バインディング データベースから既存の統計情報をすべてクリアするには、**clear fabric-binding statistics** コマンドを使用します。

switch# **clear fabric-binding statistics vsan 1**

ファブリック バインディング データベースの削除

指定された VSAN の設定済みデータベースを削除するには、コンフィギュレーション モードで **no fabric-binding** コマンドを使用します。

switch(config)# **no fabric-binding database vsan 10**

ファブリック バインディング情報の確認

ファブリック バインディング情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
switch# **show fabric-binding database** [**active**]	設定されたファブリック バインディング データベースを表示します。キーワード active を含めて、アクティブなファブリック バインディング データベースだけを表示します。
switch# **show fabric-binding database** [**active**] [**vsan** *vsan-id*]	指定された VSAN の設定済みファブリック バインディング データベースを表示します。
switch# **show fabric-binding statistics**	ファブリック バインディング データベースの統計情報を表示します。
switch# **show fabric-binding status**	すべての VSAN のファブリック バインディング ステータスを表示します。
switch# **show fabric-binding violations**	ファブリック バインディング違反を表示します。
switch# **show fabric-binding efmd** [**vsan** *vsan-id*]	指定された VSAN の設定済みファブリック バインディング データベースを表示します。

次に、VSAN 4 のアクティブ ファブリック バインディング情報を表示する例を示します。

```
switch# show fabric-binding database active vsan 4
```

次に、ファブリック バインディング違反を表示する例を示します。

```
switch# show fabric-binding violations
-------------------------------------------------------------------------------
VSAN Switch WWN [domain]     Last-Time             [Repeat count] Reason
-------------------------------------------------------------------------------
2    20:00:00:05:30:00:4a:1e [0xeb] Nov 25 05:46:14 2003   [2]    Domain mismatch
3    20:00:00:05:30:00:4a:1e [*] Nov 25 05:44:58 2003      [2]    sWWN not found
4    20:00:00:05:30:00:4a:1e [*] Nov 25 05:46:25 2003      [1]    Database mismatch
```

（注） VSAN 3 では、sWWN がリストで見つかりませんでした。VSAN 2 では、sWWN がリストで見つかりましたが、ドメイン ID が一致しませんでした。

次に、VSAN 4 の EFMD 統計情報を表示する例を示します。

```
switch# show fabric-binding efmd statistics vsan 4
```

デフォルト設定

表 46-2 に、ファブリック バインディング機能のデフォルト設定を示します。

表 46-2　ファブリック バインディングのデフォルト設定

パラメータ	デフォルト
ファブリック バインディング	ディセーブル

CHAPTER 47

FCS の設定

この章では、Cisco Nexus 5000 シリーズ スイッチに組み込まれた Fabric Configuration Server（FCS）機能について説明します。内容は次のとおりです。

- FCS について（47-1 ページ）
- FCS 名の指定（47-3 ページ）
- FCS 情報の表示（47-4 ページ）
- デフォルト設定（47-4 ページ）

FCS について

Fabric Configuration Server（FCS）を使用すると、トポロジ属性を検出したり、ファブリック要素の設定情報リポジトリを維持したりすることができます。通常、管理アプリケーションは N ポートを通してスイッチの FCS に接続されます。FCS は次のオブジェクトに基づいて、ファブリック全体を表示します。

- Interconnect Element（IE）オブジェクト：ファブリック内の各スイッチは IE オブジェクトに対応しています。ファブリックは 1 つまたは複数の IE オブジェクトで構成されます。
- ポート オブジェクト：IE の各物理ポートはポート オブジェクトに対応しています。ポート オブジェクトにはスイッチ ポート（xE および F ポート）および接続された N ポートが含まれます。
- プラットフォーム オブジェクト：一連のノードをプラットフォーム オブジェクトとして定義して、管理可能な単一のエンティティにできます。これらのノードはファブリックに接続されたエンドデバイス（ホスト システム、ストレージ サブシステム）です。プラットフォーム オブジェクトは、ファブリックのエッジ スイッチ上にあります。

各オブジェクトには、それぞれ独自の属性および値のセットがあります。一部の属性にはヌル値も定義できます。

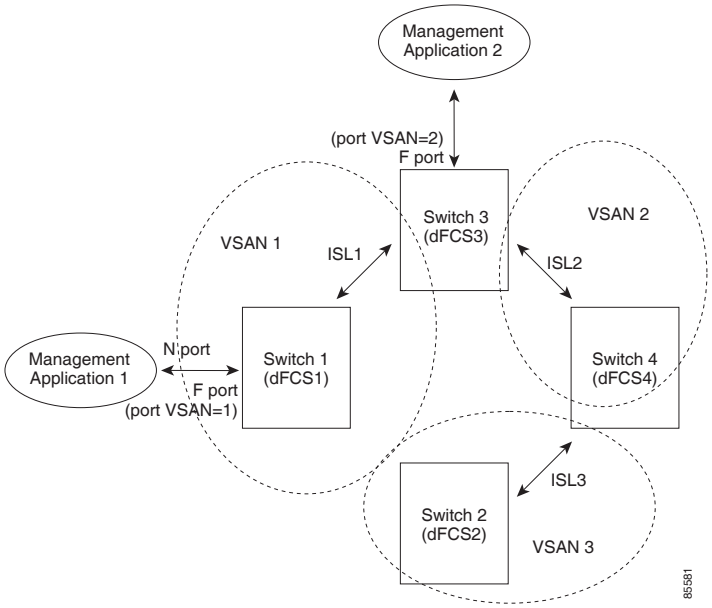
Cisco Nexus 5000 シリーズ スイッチ環境では、ファブリックは複数の VSAN で構成される場合があります。VSAN ごとに FCS インスタンスが 1 つ存在します。

FCS は仮想デバイスの検出をサポートします。**fcs virtual-device-add** コマンドを FCS コンフィギュレーション サブモードで入力すると、特定の VSAN またはすべての VSAN の仮想デバイスを検出できます。

スイッチに管理アプリケーションが接続されている場合、スイッチの FCS に転送されるすべてのフレームは、スイッチ ポート（F ポート）のポート VSAN に属します。管理アプリケーションの表示対象はこの VSAN に限定されます。ただし、このスイッチが属する他の VSAN に関する情報は、SNMP または CLI を使用して取得できます。

図 47-1 では、管理アプリケーション 1（M1）は、ポート VSAN ID が 1 の F ポートを介して接続され、管理アプリケーション 2（M2）はポート VSAN ID が 2 の F ポートを介して接続されています。M1 はスイッチ S1 および S3 の FCS 情報を、M2 はスイッチ S3 および S4 の FCS 情報をそれぞれ問い合せることができます。スイッチ S2 の情報はどちらにも提供されません。FCS は、VSAN で表示可能なこれらのスイッチ上でだけ動作します。S3 は VSAN 1 にも属していますが、M2 は VSAN 2 にだけ FCS 要求を送信できます。

図 47-1　　VSAN 環境における FCS



FCS の特性

FCS には次の特性があります。

- 次のようなネットワーク管理をサポートしています。
  - N ポート管理アプリケーションはファブリック要素に関する情報を問い合せて、取得できます。
  - SNMP マネージャは FCS 管理情報ベース（MIB）を使用して、ファブリック トポロジ情報の検出を開始して、取得できます。
- 標準 F および E ポートだけでなく、TE ポートもサポートします。
- プラットフォームに登録された論理名および管理アドレスを持つ一連のノードを維持できます。FCS はすべての登録情報のバックアップをセカンダリ ストレージに維持し、変更があるたびに更新します。再起動またはスイッチオーバーが発生すると、FCS はセカンダリ ストレージ情報を取得し、データベースを再構築します。
- SNMP マネージャは FCS に、ファブリック内のすべての IE、ポート、およびプラットフォームについて問い合わせることができます。

FCS 名の指定

一意の名前の確認をファブリック全体(グローバル)に行うのか、または登録されたプラットフォームにローカル(デフォルト)に行うのかを指定できます。

（注）　このコマンドのグローバル設定は、ファブリック内のすべてのスイッチが Cisco MDS 9000 ファミリまたは Cisco Nexus 5000 シリーズ のスイッチである場合にかぎり実行してください。

プラットフォーム名のグローバル チェックをイネーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configuration terminal** switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcs plat-check-global vsan** *vsan-id*	プラットフォーム名のグローバル チェックをイネーブルにします。
	switch(config)# **no fcs plat-check-global vsan** *vsan-id*	プラットフォーム名のグローバル チェックをディセーブル(デフォルト)にします。

プラットフォーム属性を登録する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configuration terminal** switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcs register** switch(config-fcs-register)#	FCS 登録サブモードを開始します。
ステップ 3	switch(config-fcs-register)# **platform name SamplePlatform vsan** *vsan-id* switch(config-fcs-register-attrib)#	FCS 登録属性サブモードを開始します。
	switch(config-fcs-register)# **no platform name SamplePlatform vsan** *vsan-id* switch(config-fcs-register)#	登録されたプラットフォームを削除します。
ステップ 4	switch(config-fcs-register-attrib)# **mgmt-addr 1.1.1.1**	プラットフォーム管理 IPv4 アドレスを設定します。
	switch(config-fcs-register-attrib)# **no mgmt-addr 1.1.1.1**	プラットフォーム管理 IPv4 アドレスを削除します。
	switch(config-fcs-register-attrib)# **mgmt-addr 2001:0DB8:800:200C::417A**	プラットフォーム管理 IPv6 アドレスを設定します。
	switch(config-fcs-register-attrib)# **no mgmt-addr 2001:0DB8:800:200C::417A**	プラットフォーム管理 IPv6 アドレスを削除します。
ステップ 5	switch(config-fcs-register-attrib)# **nwwn 11:22:33:44:55:66:77:88**	プラットフォーム ノード名を設定します。
	switch(config-fcs-register-attrib)# **no nwwn 11:22:33:44:55:66:77:88**	プラットフォーム ノード名を削除します。
ステップ 6	switch(config-fcs-register-attrib)# **type 5**	定義済みプラットフォーム タイプ fc-gs-3 を設定します。
	switch(config-fcs-register-attrib)# **no type 5**	設定済みのタイプを削除し、スイッチを出荷時の設定(不明なタイプ)に戻します。

	コマンド	目的
ステップ 7	`switch(config-fcs-register-attrib)# exit`	FCS 登録属性サブモードを終了します。
ステップ 8	`switch(config-fcs-register)# exit` `switch(config)#`	FCS 登録サブモードを終了します。

FCS 情報の表示

WWN 設定のステータスを表示するには、**show fcs** コマンドを使用します

次に、FCS ローカル データベースを表示する例を示します。

```
switch# show fcs database
```

次に、VSAN 1 のすべての IE のリストを表示する例を示します。

```
switch# show fcs ie vsan 1
```

次に、特定のプラットフォームに関する情報を表示する例を示します。

```
switch# show fcs platform name SamplePlatform vsan 1
```

次に、特定の pWWN のポート情報を表示する例を示します。

```
switch# show fcs port pwwn 20:51:00:05:30:00:16:de vsan 24
```

デフォルト設定

表 47-1 に、FCSの デフォルト設定値を示します。

表 47-1　FCS のデフォルト設定値

パラメータ	デフォルト
プラットフォーム名のグローバル チェック	ディセーブル
プラットフォームの ノード タイプ	不明

CHAPTER 48

ポート トラッキングの設定

Cisco Nexus 5000 シリーズ スイッチは、物理ファイバ チャネル インターフェイス（仮想ファイバ チャネル インターフェイスではなく）でのポート トラッキング機能を提供します。この機能はリンクの動作ステートに関する情報を利用して、エッジ デバイスを接続するリンクの障害を引き起こします。この処理では、間接障害が直接障害に変換されるため、冗長リンクへの復旧処理が迅速化されます。ポート トラッキング機能がイネーブルになっている場合、この機能はリンク障害時に設定されたリンクをダウンにし、トラフィックを別の冗長リンクに強制的にリダイレクトします。

この章は、次の項で構成されています。

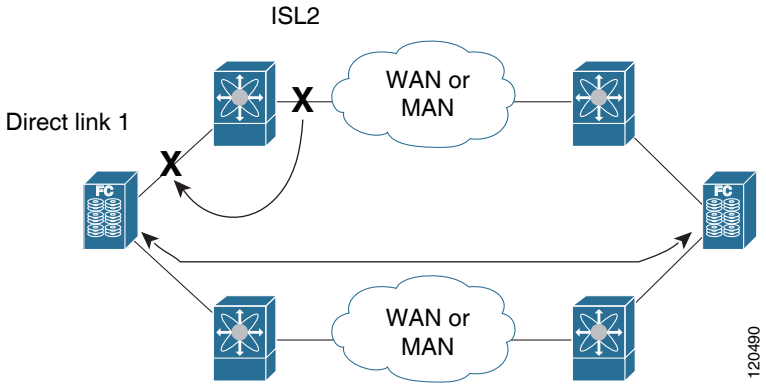
- ポート トラッキングに関する情報（48-1 ページ）
- ポート トラッキングの設定（48-2 ページ）
- ポート トラッキング情報の表示（48-7 ページ）
- ポート トラッキングのデフォルト設定値（48-7 ページ）

ポート トラッキングに関する情報

一般的に、ホストはスイッチに直接接続されているリンク（直接リンク）上でのリンク障害からすぐに復旧できます。しかし、キープアライブ メカニズムを備えた WAN や MAN ファブリック内のスイッチ間で発生する間接的なリンク障害からの復旧は、タイムアウト値（TOV）や Registered State Change Notification（RSCN）情報などの複数の要因に左右されます（「ファイバ チャネルのタイムアウト値」セクション（43-1 ページ）および「RSCN 情報について」セクション（41-5 ページ）を参照）。

図 48-1 で、ホストに対する直接リンク 1 に障害が発生した場合、ただちに復旧可能です。ただし、2 つのスイッチ間の ISL 2 に障害が発生した場合、復旧は TOV や RSCN などに左右されます。

図 48-1　　ポート トラッキングによるトラフィックの復旧



ポート トラッキング機能は、トポロジの変化を引き起こし、接続デバイスを接続しているリンクをダウンさせる障害を監視し、検出します。この機能をイネーブルにして、リンク対象ポートとトラッキング対象ポートを明示的に設定すると、スイッチ ソフトウェアはトラッキング対象ポートを監視します。リンク ステートの変化を検出した場合、スイッチ ソフトウェアはリンク対象ポートの動作ステートを変更します。

この章では次の用語を使用します。

- トラッキング対象ポート：動作ステートが継続的に監視されるポート。トラッキング対象ポートの動作ステートを使用して、1 つまたは複数のポートの動作ステートを変更します。トラッキング対象ポートは、ファイバ チャネル、VSAN（仮想 SAN）、SAN ポート チャネル、またはギガビット イーサネットのポートです。一般的に、E および TE ポート モードのポートは F ポートにもなります。
- リンク対象ポート：トラッキング対象ポートの動作ステートに基づいて動作ステートが変更されるポート。リンク対象ポートは、物理ファイバ チャネル ポートだけです。

ポート トラッキングには、次の機能があります。

- トラッキング対象ポートがダウンすると、アプリケーションはリンク対象ポートをダウンさせます。追跡されたポートが障害から復旧して再度アップになると、リンクされたポートも自動的にアップになります（特に別の設定がないかぎり）。
- トラッキング対象ポートがアップしても、リンク対象ポートを強制的にダウンしたままにできます。この場合、必要に応じてリンク対象ポートを明示的にアップする必要があります。

ポート トラッキングの設定

ポート トラッキングを設定する際、次の点に注意してください。

- トラッキング対象ポートとリンク対象ポートが同じシスコ スイッチ上に存在することを確認します。
- トラッキング対象ポートがダウンしたときに、リンク対象ポートが自動的にダウンすることを確認します。
- 再帰依存を回避するためにリンク対象ポートに再度トラッキングしないでください（たとえば、ポート fc2/2 からポート fc2/4 にトラッキングし、さらにポート fc2/2 に戻す）。

この項では、次のトピックについて取り上げます。

- ポート トラッキングのイネーブル化(48-3 ページ)
- リンク対象ポートの設定の概要(48-3 ページ)
- トラッキング対象ポートの動作バインディング(48-4 ページ)
- 複数ポートのトラッキングの概要(48-4 ページ)
- 複数ポートのトラッキング(48-5 ページ)
- VSAN 内のポートのモニタリングの概要(48-5 ページ)
- VSAN 内のポートのモニタリングの概要(48-6 ページ)
- 強制シャットダウンの概要(48-6 ページ)
- トラッキング対象ポートの強制シャットダウン(48-6 ページ)

ポート トラッキングのイネーブル化

デフォルトでは、ポート トラッキング機能は Cisco Nexus 5000 シリーズ スイッチでディセーブルです。この機能をイネーブルにすると、ポート トラッキングはスイッチ全体でグローバルにイネーブルになります。

ポート トラッキングを設定するには、ポート トラッキング機能をイネーブルにして、トラッキング対象ポートに対応するリンク対象ポートを設定します。

ポート トラッキングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# port-track enable`	ポート トラッキングをイネーブルにします。
	`switch(config)# no port-track enable`	現在適用されているポート トラッキング設定を削除し、ポート トラッキングをディセーブルにします。

リンク対象ポートの設定の概要

ポートをリンクするには、次の 2 通りの方法があります。

- リンク対象ポートからトラッキング対象ポートへの動作バインディングを設定します(デフォルト)。
- リンク対象ポートを強制的にダウンしたままにします(トラッキング対象ポートがリンク障害から回復した場合も同様)。

トラッキング対象ポートの動作バインディング

最初のトラッキング対象ポートを設定すると、動作バインディングは自動的に有効になります。この方法を使用すると、複数のポートを監視したり、1 つの VSAN 内のポートを監視したりできます。

トラッキング対象ポートの動作バインディングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface fc slot/port`	リンク対象ポートでインターフェイス コンフィギュレーション モードを開始します。これで、トラッキング対象ポートを設定できるようになります。 **（注）** 図 48-1 で、このリンクは直接リンク（1）で示されます。
ステップ 3	`switch(config-if)# port-track interface fc slot/port | san-port-channel port`	トラッキング対象ポートを指定します。トラッキング対象ポートがダウンすると、リンク対象ポートもダウンします。 **（注）** 図 48-1 で、このリンクは ISL（2）で示されます。
	`switch(config-if)# no port-track interface fc slot/port | san-port-channel port`	インターフェイスに現在適用されているポート トラッキング設定を削除します。

次に、特定のインターフェイスでポート トラッキングをイネーブルにする例を示します。

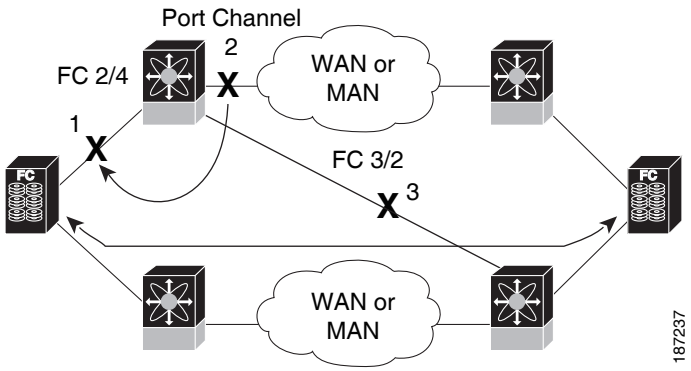
```
switch# configure
switch(config)# interface fc 2/4
switch(config-if)# port-track interface san-port-channel 2
```

複数ポートのトラッキングの概要

複数のトラッキング対象ポートの動作ステートに基づいて、リンク対象ポートの動作ステートを制御できます。複数のトラッキング対象ポートが 1 つのリンク対象ポートに対応付けられている場合、対応付けられたトラッキング対象ポートがすべてダウンしたときにかぎり、リンク対象ポートの動作ステートはダウンに設定されます。トラッキング対象ポートが 1 つでもアップしている場合、リンク対象ポートはアップしたままになります。

図 48-2 で、直接リンク 1 がダウンするのは、ISL 2 と 3 の両方に障害が発生した場合だけです。ISL 2 または 3 が動作しているかぎり、直接リンク 1 はダウンしません。

図 48-2　　ポート トラッキングによるトラフィックの復旧



複数ポートのトラッキング

複数のポートをトラッキングするには、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface fc slot/port`	指定されたインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。これで、トラッキング対象ポートを設定できるようになります。 **（注）**　図 48-2 で、このリンクは直接リンク（1）で示されます。
ステップ 3	`switch(config-if)# port-track interface interface fc slot/port | san-port-channel port`	指定されたインターフェイスのあるリンク対象ポートをトラッキングします。トラッキング対象ポートがダウンすると、リンク対象ポートもダウンします。 **（注）**　図 48-2 で、このリンクは ISL（2）で示されます。

次に、複数のインターフェイスでポート トラッキングをイネーブルにする例を示します。

```
switch# configure
switch(config)# interface fc 2/3
switch(config-if)# port-track interface fc 2/3
switch(config-if)# port-track interface san-port-channel 2
```

VSAN 内のポートのモニタリングの概要

トラッキング対象ポート上のすべての動作 VSAN から VSAN をリンク対象ポートに対応付けるには、必要な VSAN を指定します。このため、トラッキング対象ポートの詳細な設定が可能になります。トラッキング対象ポートが TE ポートの場合、ポートの動作ステートがダウンにならずに、ポート上の動作 VSAN がダイナミックに変わる場合があります。この場合、リンク対象ポートのポート VSAN は、トラッキング対象ポート上の動作 VSAN 上で監視できます。

この機能を設定すると、トラッキング対象ポート上で VSAN がアップしている場合にだけリンク対象ポートがアップします。

ヒント　指定する VSAN は、リンク対象ポートのポート VSAN と同じである必要はありません。

VSAN 内のポートのモニタリングの概要

特定の VSAN でトラッキング対象ポートをモニタする手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot/port*	指定されたインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。これで、トラッキング対象ポートを設定できるようになります。
ステップ 3	switch(config-if)# **port-track interface san-port-channel 1 vsan 2**	VSAN 2 で SAN ポート チャネルのトラッキングをイネーブルにします。
	switch(config-if)# **no port-track interface san-port-channel 1 vsan 2**	リンク対象ポートに対する VSAN の対応付けを削除します。SAN ポート チャネル リンクは有効なままです。

強制シャットダウンの概要

トラッキング対象ポートで頻繁にフラップが発生する場合、動作バインディング機能を使用するトラッキング ポートは頻繁にトポロジを変えることがあります。この場合、頻繁なフラップの原因が解決されるまで、ポートをダウンしたままにできます。フラップが発生するポートをダウン状態のままにしておくと、プライマリのトラッキング対象ポートの問題が解決されるまで、トラフィックは冗長パスを流れるよう強制されます。問題が解決されて、トラッキング対象ポートが再びアップした場合には、インターフェイスを明示的にイネーブルにできます。

ヒント　この機能を設定すると、トラッキング対象ポートが再びアップになっても、リンク対象ポートはシャットダウン状態のままになります。トラッキング対象ポートがアップして安定したら、(このインターフェイスを管理上アップして) リンク対象ポートの強制シャットダウン状態を明示的に解除する必要があります。

トラッキング対象ポートの強制シャットダウン

トラッキング対象ポートを強制的にシャットダウンするには、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot/port*	指定されたインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。これで、トラッキング対象ポートを設定できるようになります。
ステップ 3	switch(config-if)# **port-track force-shut**	トラッキング対象ポートを強制的にシャットダウンします。
	switch(config-if)# **no port-track force-shut**	トラッキング対象ポートのポート シャットダウン設定を解除します。

ポート トラッキング情報の表示

スイッチの現在のポート トラッキング設定を表示するには、**show** コマンドを使用します。

次に、特定のインターフェイスのトラッキング対象ポートの設定を表示する例を示します。

```
switch# show interface fc2/1
fc2/1 is down (Administratively down)
    Hardware is Fibre Channel, FCOT is short wave laser w/o OFC (SN)
    Port WWN is 20:01:00:05:30:00:0d:de
    Admin port mode is FX
    Port vsan is 1
    Receive data field Size is 2112
    Beacon is turned off
  Port tracked with interface fc2/2 (down)
    Port tracked with interface san-port-channel 1 vsan 2 (down)
5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
...
```

次に、SAN ポート チャネルのトラッキング対象ポートの設定を表示する例を示します。

```
switch# show interface san-port-channel 1
port-channel 1 is down (No operational members)
    Hardware is Fibre Channel
    Port WWN is 24:01:00:05:30:00:0d:de
    Admin port mode is auto, trunk mode is on
    Port vsan is 2
    Linked to 1 port(s)
   Port linked to interface fc2/1
...
```

次に、ポート トラッキング モードを表示する例を示します。

```
switch# show interface fc 2/4

fc2/4 is up
    Hardware is Fibre Channel, FCOT is short wave laser
...
    Transmit B2B Credit is 64
    Receive B2B Credit is 16
    Receive data field Size is 2112
    Beacon is turned off
  Port track mode is force_shut <--トラッキング対象ポートがアップになってもこのポート
                                  はダウンのまま
```

ポート トラッキングのデフォルト設定値

表 48-1 に、ポート トラッキング パラメータのデフォルト設定値を示します。

表 48-1　ポート トラッキング パラメータのデフォルト設定値

パラメータ	デフォルト
ポート トラッキング	ディセーブル
動作バインディング	イネーブル（ポート トラッキングと同時）

CHAPTER 49

SPAN の設定

スイッチド ポート アナライザ（SPAN）機能（ポート ミラーリングまたはポート モニタリングとも呼ばれる）は、ネットワーク アナライザによる分析のためにネットワーク トラフィックを選択します。ネットワーク アナライザは、Cisco SwitchProbe、ファイバ チャネル アナライザ、またはその他のリモート モニタリング（RMON）プローブです。

この章は、次の項で構成されています。

- SPAN 送信元（49-1 ページ）
- SPAN 宛先（49-2 ページ）
- SPAN の設定（49-3 ページ）

SPAN 送信元

SPAN 送信元とは、トラフィックをモニタリングできるインターフェイスを表します。Cisco Nexus 5000 シリーズ スイッチは、SPAN 送信元として、イーサネット、ファイバ チャネル、仮想ファイバ チャネル、ポート チャネル、SAN ポート チャネル、VLAN（仮想 LAN）および VSAN（仮想 SAN）をサポートします。VLAN または VSAN では、指定された VLAN または VSAN でサポートされているすべてのインターフェイスが SPAN 送信元として含まれます。イーサネット、ファイバ チャネル、および仮想ファイバ チャネルの送信元インターフェイスで、入力方向、出力方向、または両方向の SPAN トラフィックを選択できます。

- 入力送信元（Rx）：この送信元ポートを介してスイッチに入るトラフィックは、SPAN 宛先ポートにコピーされます。
- 出力送信元（Tx）：この送信元ポートを介してスイッチから出るトラフィックは、SPAN 宛先ポートにコピーされます。

送信元ポートの特性

送信元ポート（モニタリング対象ポートとも呼ばれる）は、ネットワーク トラフィック分析のためにモニタリングするスイッチド インターフェイスです。スイッチは、任意の数の入力送信元ポート（スイッチで使用できる最大数のポート）と任意の数のソース VLAN または VSAN をサポートします。

送信元ポートの特性は、次のとおりです。

- イーサネット、ファイバ チャネル、仮想ファイバ チャネル、ポート チャネル、SAN ポート チャネル、VLAN、および VSAN のいずれのポート タイプでも可能です。

- 複数の SPAN セッションではモニタリングできません。
- 宛先ポートには設定できません。
- モニタする方向（入力、出力、または両方）を指定して、各送信元ポートを設定できます。VLAN、VSAN、ポート チャネル、および SAN ポート チャネルの送信元の場合、モニタ方向は入力だけであり、グループ内のすべての物理ポートに適用されます。Rx と Tx のオプションは、VLAN または VSAN の SPAN セッションでは使用できません。
- 送信元ポートは、同じ VLAN または VSAN か、別の VLAN または VSAN に設定できます。
- VLAN または VSAN の SPAN 送信元では、ソース VLAN または VSAN のすべてのアクティブ ポートが送信元ポートとして含まれます。
- スイッチは最大 2 つの出力 SPAN 送信元ポートをサポートします。

SPAN 宛先

SPAN 宛先とは、送信元ポートをモニタリングするインターフェイスを表します。Cisco Nexus 5000 シリーズ スイッチは、SPAN 宛先として、イーサネット インターフェイスとファイバ チャネル インターフェイスをサポートします。

送信元 SPAN	宛先 SPAN
イーサネット	イーサネット
ファイバ チャネル	ファイバ チャネル
ファイバ チャネル	イーサネット（FCoE）
仮想ファイバ チャネル	ファイバ チャネル
仮想ファイバ チャネル	イーサネット（FCoE）

宛先ポートの特性

各ローカル SPAN セッション には、送信元ポート、VLAN、または VSAN からトラフィックのコピーを受信する宛先ポート（モニタ ポートとも呼ばれる）がある必要があります。宛先ポートの特性は、次のとおりです。

- あらゆる物理ポート、イーサネット、イーサネット（FCoE）、またはファイバ チャネルとして使用できます。仮想ファイバ チャネル ポートは、宛先ポートに指定できません。
- ソース ポートにはなれません。
- ポート チャネルまたは SAN ポート チャネル グループにはできません。
- SPAN セッションがアクティブなときは、スパニングツリーに参加しません。
- 任意の SPAN セッションのソース VLAN に属する場合、送信元リストから除外され、モニタリングされません。
- すべてのモニタリング対象送信元ポートの送受信トラフィックのコピーを受信します。宛先ポートがオーバーサブスクライブ型の場合、輻輳が発生する可能性があります。輻輳が発生すると、1 つまたは複数の送信元ポートでのトラフィック転送に影響を及ぼす可能性があります。

SPAN の設定

送信元ポートからスイッチの指定された宛先ポートにパケットをコピーするように、SPAN セッションを設定できます。この項では、次のトピックについて取り上げます。

- SPAN セッションの作成および削除（49-3 ページ）
- 宛先ポートの設定（49-4 ページ）
- 送信元ポートの設定（49-5 ページ）
- 送信元ポート チャネル、VLAN、または VSAN の設定（49-6 ページ）
- SPAN セッションの説明の設定（49-7 ページ）
- SPAN セッションの一時停止またはアクティベーション（49-7 ページ）
- SPAN 情報の表示（49-8 ページ）

SPAN セッションの作成および削除

モニタ コマンドを使用してセッション番号を割り当てることによって、SPAN セッションを作成できます。セッションがすでに存在する場合、そのセッションに設定が追加されます。

SPAN セッションを作成する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch#` **`configure terminal`**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)#` **`monitor session`** *`session-number`*	モニタ コンフィギュレーション モードを開始します。既存のセッション設定に新しいセッション設定が追加されます。 *session-number* は 1 ～ 18 です。最大 18 セッションを設定できます。ただし、同時にアクティブにできるのは 2 つのセッションのみです。 2 つを超える SPAN セッションを設定すると、最初の 2 つのセッションがアクティブになります。起動中にアクティブなセッションの順序が逆になり、最後の 2 つのセッションがアクティブになります。たとえば、セッション 1 ～ 10 を設定して、1 と 2 がアクティブな場合、リブート後はセッション 9 と 10 がアクティブになります。確定した動作を可能にするには、**monitor session** *session-number* **shut** コマンドを使用して、セッション 3 ～ 10 を明示的に一時停止します。

次に、SPAN セッションを作成する例を示します。

```
switch# configure terminal
switch(config)# monitor session 2
```

完全に新しいセッションを処理するために、削除したいセッション番号またはすべての SPAN セッションを削除することができます。

SPAN セッションを削除する手順は、次のとおりです。

コマンド	目的
switch(config)# **no monitor session** {**all** | *session-number*}	指定された SPAN セッションまたはすべてのセッションの設定を削除します。

宛先ポートの設定

SPAN 宛先ポートは、スイッチ上の物理ポートにのみ設定できます。イーサネット宛先ポートとファイバ チャネル宛先ポートでは、設定にわずかな違いがあります(次のトピックを参照)。

イーサネット宛先ポートの設定

イーサネット インターフェイスを SPAN 宛先ポートとして設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface ethernet** *slot/port*	スロット値およびポート値による選択で指定されたイーサネット インターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport monitor**	インターフェイスをモニタ モードに設定します。ポートが SPAN 宛先として設定されている場合、プライオリティ フロー制御はディセーブルです。
ステップ 4	switch(config-if)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	switch(config)# **monitor session** *session-number*	モニタ コンフィギュレーション モードを開始します。
ステップ 6	switch(config-monitor)# **destination interface ethernet** *slot/port*	イーサネット宛先ポートを設定します。

次に、イーサネット SPAN 宛先ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 2
switch(config-monitor)# destination interface ethernet 1/3
```

ファイバ チャネル宛先ポートの設定

ファイバ チャネル ポートを SPAN 宛先ポートとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface fc** *slot/port*	スロット値およびポート値による選択で指定されたファイバ チャネル インターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport mode SD**	インターフェイスを SPAN 宛先（SD）モードに設定します。
ステップ 4	switch(config-if)# **switchport speed 1000**	インターフェイス速度を 1000 に設定します。自動速度オプションは使用できません。
ステップ 5	switch(config-if)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	switch(config)# **monitor session** *session-number*	モニタ コンフィギュレーション モードを開始します。
ステップ 7	switch(config-monitor)# **destination interface fc** *slot/port*	ファイバ チャネル宛先ポートを設定します。

次に、イーサネット SPAN 宛先ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# interface fc 2/4
switch(config-if)# switchport mode SD
switch(config-if)# switchport speed 1000
switch(config-if)# exit
switch(config)# monitor session 2
switch(config-monitor)# destination interface fc 2/4
```

送信元ポートの設定

SPAN セッションに送信元ポートを設定できます。送信元ポートは、イーサネット、ファイバ チャネル、または仮想ファイバ チャネルのポートに設定できます。

SPAN セッションに送信元ポートを設定する手順は、次のとおりです。

コマンド	目的
switch(config-monitor)# **source interface** *type slot/port* [**rx** | **tx** | **both**]	送信元およびパケットをコピーするトラフィック方向を設定します。イーサネット、ファイバ チャネル、または仮想ファイバ チャネルのポート範囲を入力できます。コピーするトラフィック方向を、入力（rx）、出力（tx）、または両方向（both）として指定できます。デフォルトは both です。

次に、イーサネット SPAN 送信元ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface ethernet 1/16
```

次に、ファイバ チャネル SPAN 送信元ポートを設定する例を示します。

```
...
switch(config-monitor)# source interface fc 2/1
```

次に、仮想ファイバ チャネル SPAN 送信元ポートを設定する例を示します。

```
...
switch(config-monitor)# source interface vfc 129
```

送信元ポート チャネル、VLAN、または VSAN の設定

SPAN セッションに送信元チャネルを設定できます。これらのポートは、ポート チャネル、SAN ポート チャネル、VLAN、および VSAN に設定できます。モニタリング方向は入力のみで、グループ内のすべての物理ポートに適用されます。

SPAN セッションに送信元チャネルを設定する手順は、次のとおりです。

コマンド	目的
switch(config-monitor)# **source** {**interface** {**port-channel** | **san-port-channel**} *channel-number* **rx** | **vlan** *vlan-range* | **vsan** *vsan-range* }	ポート チャネル、SAN ポート チャネル、VLAN、または VSAN 送信元を設定します。モニタリング方向は入力のみで、グループ内のすべての物理ポートに適用されます。VLAN または VSAN 送信元の場合、監視方向は暗黙的です。

次に、ポート チャネル SPAN 送信元を設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface port-channel 1 rx
```

次に、SAN ポート チャネル SPAN 送信元を設定する例を示します。

```
...
switch(config-monitor)# source interface san-port-channel 3 rx
```

次に、VLAN SPAN 送信元を設定する例を示します。

```
...
switch(config-monitor)# source vlan 1
```

次に、VSAN SPAN 送信元を設定する例を示します。

```
...
switch(config-monitor)# source vsan 1
```

SPAN セッションの説明の設定

参照を容易にするために SPAN セッションの説明的な名前を提供する手順は、次のとおりです。

コマンド	目的
switch(config-monitor)# **description** *description*	SPAN セッションに説明的な名前を適用します。

次に、SPAN セッションの説明を設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# description monitoring ports fc2/2-fc2/4
```

SPAN セッションの一時停止またはアクティベーション

デフォルトでは、セション ステートは shut のままになります。パケットを送信元から宛先にコピーするセッションを開始する手順は、次のとおりです。

コマンド	目的
switch(config)# **no monitor session** {**all** | *session-number*} **shut**	指定された SPAN セッションまたはすべてのセッションを開始します。

次に、SPAN セッションを一時停止する例を示します。

```
...
switch(config)# monitor session 3 shut
```

SPAN セッションを一時停止する手順は、次のとおりです。

コマンド	目的
switch(config)# **monitor session** {**all** | *session-number*} **shut**	指定された SPAN セッションまたはすべてのセッションを一時停止します。

（注） Cisco Nexus 5000 シリーズ スイッチは、2 つのアクティブな SPAN セッションをサポートしています。2 つを超える SPAN セッションを設定すると、最初の 2 つのセッションがアクティブになります。起動中にアクティブなセッションの順序が逆になり、最後の 2 つのセッションがアクティブになります。たとえば、セッション 1 ～ 10 を設定して、1 と 2 がアクティブな場合、リブート後はセッション 9 と 10 がアクティブになります。確定した動作を可能にするには、**monitor session** *session-number* **shut** コマンドを使用して、セッション 3 ～ 10 を明示的に一時停止します。

SPAN 情報の表示

SPAN 情報を表示する手順は、次のとおりです。

コマンド	目的
switch# **show monitor** [**session** {**all** | *session-number* | **range** *session-range*} [**brief**]]	SPAN 設定を表示します。

次に、SPAN セッションの情報を表示する例を示します。

```
switch# show monitor
SESSION  STATE        REASON                    DESCRIPTION
-------  -----------  ----------------------    --------------------------------
2        up           The session is up
3        down         Session suspended
4        down         No hardware resource
```

次に、SPAN セッションの詳細を表示する例を示します。

```
switch# show monitor session 2
   session 2
---------------
type              : local
state             : up
source intf       :
    rx            : fc3/1
    tx            : fc3/1
    both          : fc3/1
source VLANs      :
    rx            :
source VSANs      :
    rx            : 1
destination ports : Eth3/1
```

CHAPTER 50

トラブルシューティング

この章では、Cisco Nexus 5000 シリーズ シリーズスイッチの問題を解決するための基本的なトラブルシューティングについて説明します。この章は、次の項で構成されています。

- 忘失パスワードの回復（50-1 ページ）
- Ethanalyzer の使用（50-3 ページ）
- ファイバ チャネルのトラブルシューティング（50-5 ページ）
- show tech-support コマンド（50-8 ページ）
- デフォルト設定（50-16 ページ）

忘失パスワードの回復

ここでは、スイッチのコンソール ポートを使用して、失われたネットワーク管理者パスワードを回復する方法について説明します。

次のどちらかの方法で、ネットワーク管理者パスワードを回復できます。

- network admin 権限を持つユーザ名で CLI から回復する
- スイッチの電源を再投入する

この項では、次のトピックについて取り上げます。

- network admin 権限での CLI の使用（50-1 ページ）
- スイッチの電源の再投入（50-2 ページ）

network admin 権限での CLI の使用

network-admin 特権を持つユーザ名でスイッチに、すでにログインしている、またはログイン可能である場合の手順は、次のとおりです。

ステップ 1 ユーザ名に network admin 権限があるかどうかを確認します。

```
switch# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
```

```
user:dbgusr
        this user account has no expiry date
        roles:network-admin network-operator
```

ステップ 2　ユーザ名に network admin 権限がある場合は、新しいネットワーク管理者パスワードを割り当てます。

```
switch# configure terminal
switch(config)# username admin password <new password>
switch(config)# exit
switch#
```

ステップ 3　設定を保存します。

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

スイッチの電源の再投入

network-admin 特権を持つスイッチ上でセッションを開始できない場合は、スイッチの電源を再投入してネットワーク管理者パスワードを回復する必要があります。

注意　この手順を実行すると、スイッチ上のすべてのトラフィックが中断されます。

（注）　管理者パスワードは、Telnet または SSH セッションからは回復できません。ローカル コンソール接続を使用できる必要があります。

スイッチの電源を再投入して、ネットワーク管理者パスワードを回復する手順は、次のとおりです。

ステップ 1　スーパーバイザ モジュールのコンソール ポートにターミナル セッションを確立します。

ステップ 2　スイッチの電源を再投入します。

ステップ 3　スイッチで Cisco NX-OS ソフトウェアのブート シーケンスが開始されたときに、コンソール ポート セッションから **Ctrl-B** キー シーケンスを押して、ブート プロンプト モードを開始します。

```
Ctrl+B
switch(boot)#
```

ステップ 4　ネットワーク管理者パスワードを再設定します。

```
switch(boot)# configure terminal
switch(boot-config)# admin-password <new password>
switch(boot-config)# exit
switch(boot)#
```

ステップ 5　bootflash: の内容を表示して、Cisco NX-OS ソフトウェア イメージ ファイルを見つけます。

```
switch(boot)# dir bootflash:
```

ステップ 6　Cisco NX-OS システム ソフトウェア イメージをロードします。

次の例では、システム イメージ ファイル名は nx-os.bin です。

```
switch(boot) # load bootflash:nx-os.bin
```

ステップ 7　新しい管理者パスワードを使用してスイッチにログインします。

```
switch login: admin
Password: <new password>
```

ステップ 8　SNMP パスワードとしても使用できるようにするために、新しいパスワードを再設定します。

```
switch# configure terminal
switch(config)# username admin password <new password>
switch(config)# exit
switch#
```

ステップ 9　設定を保存します。

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

Ethanalyzer の使用

Ethanalyzer は、Wireshark（旧称 Ethereal）オープン ソース コードに基づく Cisco NX-OS プロトコル アナライザ ツールです。Ethanalyzer は、パケットのキャプチャとデコードを行うための Wireshark のコマンドライン バージョンです。Ethanalyzer を使用してネットワークをトラブルシューティングし、コントロール プレーン トラフィックを分析できます。

Ethanalyzer を設定するには、次のコマンドを使用します。

コマンド	目的
ethanalyzer local interface *interface*	スーパーバイザで送信または受信されたパケットをキャプチャし、詳細なプロトコル情報を表示します。 次のコマンドでは、インターフェイスは inbound-hi（インバウンド高優先度インターフェイス）、inbound-low（インバウンド低優先度インターフェイス）、または mgmt（管理インターフェイス）のいずれかになります。
ethanalyzer local interface *interface* **brief**	スーパバイザで送信または受信されたパケットをキャプチャし、プロトコル情報の概要を表示します。
ethanalyzer local interface *interface* **limit-captured-frames**	キャプチャするフレーム数を制限します。
ethanalyzer local interface *interface* **limit-frame-size**	キャプチャするフレームの長さを制限します。
ethanalyzer local interface *interface* **capture-filter**	キャプチャするパケットのタイプをフィルタリングします。
ethanalyzer local interface *interface* **display-filter**	表示するキャプチャ済みパケットのタイプをフィルタリングします。
ethanalyzer local interface *interface* **write**	キャプチャしたデータをファイルに保存します。
ethanalyzer local read *file*	キャプチャされたデータ ファイルを開いて分析します。

Ethanalyzer は、Cisco NX-OS がハードウェアで転送するデータ トラフィックはキャプチャしません。

Ethanalyzer は、tcpdump と同じキャプチャ フィルタ構文を使用します。詳細については、次の URL を参照してください。

http://www.tcpdump.org/tcpdump_man.html

表示フィルタの構文については、次の URL を参照してください。

http://wiki.wireshark.org/DisplayFilters

次の例では、キャプチャされたデータ（4 パケットに限定された）を管理インターフェイス上に表示します。

```
switch# ethanalyzer local interface mgmt brief limit-captured-frames 4
Capturing on eth0
2005-01-25 07:18:08.997132 10.193.24.42 -> 10.200.0.103 TELNET Telnet Data ...
2005-01-25 07:18:09.166266 10.200.0.103 -> 10.193.24.42 TCP 1235 > telnet [ACK] Seq=0
Ack=19 Win=64129 Len=0
2005-01-25 7:18:09.166830 10.193.24.42 -> 10.200.0.103 TELNET Telnet Data ...
2005-01-25 07:18:09.376250 10.200.0.103 -> 10.193.24.42 TCP 1235 > telnet [ACK] Seq=0
Ack=99 Win=64049 Len=0
4 packets captured
```

次の例では、1 つの HSRP パケットについてキャプチャしたデータの詳細を表示します。

```
switch(config)# ethanalyzer local interface mgmt capture-filter "tcp port 23"
limit-captured-frames 1

Capturing on eth0
Frame 1 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Jan 25, 2005 08:49:49.250719000
    [Time delta from previous captured frame: 1106642989.250719000 seconds]
    [Time delta from previous displayed frame: 1106642989.250719000 seconds]
    [Time since reference or first frame: 1106642989.250719000 seconds]
    Frame Number: 1
    Frame Length: 60 bytes
    Capture Length: 60 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:tcp]
Ethernet II, Src: 00:1a:a2:d2:d7:00 (00:1a:a2:d2:d7:00), Dst: 00:0d:ec:6d:81:00
(00:0d:ec:6d:81:00)
    Destination: 00:0d:ec:6d:81:00 (00:0d:ec:6d:81:00)
        Address: 00:0d:ec:6d:81:00 (00:0d:ec:6d:81:00)
        .......0 ................= IG bit: Individual address (unicast)
        ......0.................= LG bit: Globally unique address (factory default)
    Source: 00:1a:a2:d2:d7:00 (00:1a:a2:d2:d7:00)
        Address: 00:1a:a2:d2:d7:00 (00:1a:a2:d2:d7:00)
        .......0 ................= IG bit: Individual address (unicast)
        ......0.................= LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
    Trailer: 000000000000
Internet Protocol, Src: 10.200.0.103 (10.200.0.103), Dst: 10.193.24.42 (10.193.24.42)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00..= Differentiated Services Codepoint: Default (0x00)
        ......0.= ECN-Capable Transport (ECT): 0
        .......0 = ECN-CE: 0
    Total Length: 40
    Identification: 0xa651 (42577)
    Flags: 0x04 (Don't Fragment)
        0...= Reserved bit: Not set
        .1..= Don't fragment: Set
        ..0.= More fragments: Not set
```

```
    Fragment offset: 0
    Time to live: 127
    Protocol: TCP (0x06)
    Header checksum: 0x2765 [correct]
        [Good: True]
        [Bad : False]
    Source: 10.200.0.103 (10.200.0.103)
    Destination: 10.193.24.42 (10.193.24.42)
Transmission Control Protocol, Src Port: 1288 (1288), Dst Port: telnet (23), Seq: 0, Ack:
0, Len: 0
    Source port: 1288 (1288)
    Destination port: telnet (23)
    Sequence number: 0    (relative sequence number)
    Acknowledgement number: 0    (relative ack number)
    Header length: 20 bytes
    Flags: 0x10 (ACK)
        0.......= Congestion Window Reduced (CWR): Not set
        .0......= ECN-Echo: Not set
        ..0.....= Urgent: Not set
        ...1 ....= Acknowledgment: Set
        ....0...= Push: Not set
        .....0..= Reset: Not set
        ......0.= Syn: Not set
        .......0 = Fin: Not set
    Window size: 64334
    Checksum: 0x934f [correct]
        [Good Checksum: True]
        [Bad Checksum: False]

1 packets captured
```

Wireshark の詳細については、http://www.wireshark.org/docs/ を参照してください。

ファイバ チャネルのトラブルシューティング

ここでは、ファイバ チャネルの問題を解決するためのトラブルシューティングについて説明します。この項では、次のトピックについて取り上げます。

- fctrace（50-5 ページ）
- fcping（50-6 ページ）

fctrace

fctrace 機能は、次の機能を提供します。

- データ トラフィックが経由したルートを追跡します。
- スイッチ間（ホップ単位）の遅延を計算します。

fctrace を実行するには、宛先の FC ID、N ポートの WWN、またはデバイス エイリアスを指定します。

トレース フレームは、通常、ファブリックの遠いエッジに到達するまでネットワークにルーティングされます。フレームは、ファブリックのエッジ（指定したポート WWN または FC ID のエンド ノードに接続された F ポート）に到達すると、発信側にループバックされます（送信元 ID と宛先 ID が入れ替わります）。

宛先に到達できない場合には、パス検出が開始され、障害ポイントまでのパスがトラッキングされます。

（注）　fctrace 機能を実行できるのは、TE ポートだけです。宛先へのパス上に TE ポートだけが存在していることを確認してください。パス上に E ポートが存在すると、fctrace フレームは、そのスイッチによってドロップされます。また、発信側で fctrace がタイムアウトになり、パス検出は開始されません。

fctrace 処理を実行する手順は、次のとおりです。

コマンド	目的

`switch# fctrace fcid 0xd70000 vsan 1`
`Route present for :  0xd70000`
`20:00:00:0b:46:00:02:82(0xfffcd5)`
`Timestamp Invalid.`
`20:00:00:05:30:00:18:db(0xfffcd7)`
`Timestamp Invalid.`
`20:00:00:05:30:00:18:db(0xfffcd7)`
	宛先 N ポートの指定された FC ID に対して、fctrace を実行します。

`switch# fctrace pwwn 21:00:00:e0:8b:06:d9:1d vsan 1 timeout 5`
`Route present for : 21:00:00:e0:8b:06:d9:1d`
`20:00:00:0b:46:00:02:82(0xfffcd5)`
`Timestamp Invalid.`
`20:00:00:05:30:00:18:db(0xfffcd7)`
`Timestamp Invalid.`
`20:00:00:05:30:00:18:db(0xfffcd7)`
	宛先 N ポートの pWWN を使用して、fctrace を実行します。
	デフォルトで、タイムアウトまでの待機期間は 5 秒です。有効範囲は 1 ～ 10 秒です。

`switch# fctrace device-alias disk1 v 1`
`Route present for : 22:00:00:0c:50:02:ce:f8`
`20:00:00:05:30:00:31:1e(0xfffca9)`
	宛先 N ポートのデバイス エイリアスを使用して、fctrace を実行します。

fcping

fcping 機能はエンドツーエンド接続をチェックして、ノードの到達可能性を確認します。fcping 機能を実行するには、FC ID、宛先ポート WWN、またはデバイス エイリアス情報を指定します。

fcping 処理を実行する手順は、次のとおりです。

	コマンド	目的

ステップ 1	`switch# fcping fcid 0xd70000 vsan 1`
	`28 bytes from  0xd70000  time = 730 usec`
	`28 bytes from  0xd70000  time = 165 usec`
	`28 bytes from  0xd70000  time = 262 usec`
	`28 bytes from  0xd70000  time = 219 usec`
	`28 bytes from  0xd70000  time = 228 usec`
	
	`5 frames sent, 5 frames received, 0 timeouts`
	`Round-trip min/avg/max = 165/270/730 usec`
		宛先の指定された pWWN または FC ID に対して、fcping を実行します。デフォルトでは、5 フレームが送信されます。

コマンド	目的
switch# **fcping fcid 0xd70000 vsan 1 count 10** 28 bytes from 0xd70000 time = 730 usec 28 bytes from 0xd70000 time = 165 usec 28 bytes from 0xd70000 time = 262 usec 28 bytes from 0xd70000 time = 219 usec 28 bytes from 0xd70000 time = 228 usec 28 bytes from 0xd70000 time = 230 usec 28 bytes from 0xd70000 time = 230 usec 28 bytes from 0xd70000 time = 225 usec 28 bytes from 0xd70000 time = 229 usec 28 bytes from 0xd70000 time = 183 usec 10 frames sent, 10 frames received, 0 timeouts Round-trip min/avg/max = 165/270/730 usec	count オプションを使用して、送信するフレーム数を設定します。指定できる範囲は 0 ～ 2147483647 です。値 0 を指定すると、コマンドによって無制限にフレームが送信されます。
switch# **fcping fcid 0xd500b4 vsan 1 timeout 10** 28 bytes from 0xd500b4 time = 1345 usec ... 5 frames sent, 5 frames received, 0 timeouts Round-trip min/avg/max = 340/581/1345 usec	タイムアウト値を設定します。デフォルトの待機時間は 5 秒です。有効範囲は 1 ～ 10 秒です。
switch# **fcping device-alias disk1 vsan 1** 28 bytes from 22:00:00:0c:50:02:ce:f8 time = 1883 usec 28 bytes from 22:00:00:0c:50:02:ce:f8 time = 493 usec 28 bytes from 22:00:00:0c:50:02:ce:f8 time = 277 usec 28 bytes from 22:00:00:0c:50:02:ce:f8 time = 391 usec 28 bytes from 22:00:00:0c:50:02:ce:f8 time = 319 usec 5 frames sent, 5 frames received, 0 timeouts Round-trip min/avg/max = 277/672/1883 usec	宛先の指定されたデバイス エイリアスに対して、fcping を実行します。
ステップ 2 switch# **fcping fcid 0x010203 vsan 1** No response from the N port. switch# **fcping pwwn 21:00:00:20:37:6f:db:dd vsan 1** 28 bytes from 21:00:00:20:37:6f:db:dd time = 1454 usec ... 5 frames sent, 5 frames received, 0 timeouts Round-trip min/avg/max = 364/784/1454 usec	N ポートがアクティブの場合でも、"No response from the N port" メッセージを返します。これは、N ポートでリソースが不足しているために起こります。 数秒後に、もう一度コマンドを実行してください。

スイッチ接続の確認

宛先スイッチとの接続を確認できます。

（注） この手順で使用される FC ID 変数はドメイン コントローラ アドレスです。ドメイン ID の複製ではありません。

宛先スイッチとの接続を確認する手順は、次のとおりです。

	コマンド	目的

ステップ 1	`switch# show fcdomain domain-list vsan 200`
	`Number of domains: 7`
	`Domain ID  WWN`
	`---------  ----------`
	`  0x01(1)  20:c8:00:05:30:00:59:df [Principal]`
	`  0x02(2)  20:c8:00:0b:5f:d5:9f:c1`
	`0x6f(111)  20:c8:00:05:30:00:60:df`
	`0xda(218)  20:c8:00:05:30:00:87:9f [Local]`
	`  0x06(6)  20:c8:00:0b:46:79:f2:41`
	`  0x04(4)  20:c8:00:05:30:00:86:5f`
	`0x6a(106)  20:c8:00:05:30:00:f8:e3`
		宛先スイッチのドメイン ID を表示します。
		ドメイン コントローラ アドレスを取得するには、ドメイン ID に FFFC を連結します。たとえば、ドメイン ID が 0xda（218）の場合、連結された ID は 0xfffcda になります。

ステップ 2	`switch# fcping fcid 0xFFFCDA vsan 200`
	`28 bytes from 0xFFFCDA time = 298 usec`
	`28 bytes from 0xFFFCDA time = 260 usec`
	`28 bytes from 0xFFFCDA time = 298 usec`
	`28 bytes from 0xFFFCDA time = 294 usec`
	`28 bytes from 0xFFFCDA time = 292 usec`
	
	`5 frames sent, 5 frames received, 0 timeouts`
	`Round-trip min/avg/max = 260/288/298 usec`
		エンドツーエンド接続をチェックして、宛先スイッチの到達可能性を確認します。

show tech-support コマンド

show tech-support コマンドは、使用中のスイッチに関する大量の情報を収集してトラブルシューティングを行う場合に便利です。シスコのテクニカル サポート担当者に問題を報告する場合に、このコマンドの出力を提出してください。

show tech-support コマンドを使用すると、複数の **show** コマンドの出力が一度に表示されます。このコマンド出力は、使用している設定によって異なります。問題を報告する際にスイッチに関する一般情報を表示するには、EXEC モードで **show tech-support** コマンドを使用します。

コマンドごとに詳細情報を表示することもできます。特定のインターフェイス、モジュール、または仮想 SAN（VSAN）の出力を指定できます。各コマンド出力は行で区切られ、出力の前にコマンドが表示されます。

（注） 自動スクロールをディセーブルにして、手動スクロールをイネーブルにするには、明示的に **terminal length** コマンドを 0（ゼロ）に設定します。設定された端末サイズを表示するには、**show terminal** コマンドを使用します。このコマンドの出力が表示されたら、必要に応じてターミナル長をリセットしてください。

ヒント **show tech-support** コマンドに **>**（左向き矢印）とファイル名を付加することにより、このコマンドの出力をファイルに保存できます。このファイルを保存する場合は、十分な容量があることを確認してください。これらのファイルのサイズは、それぞれ 1.8 MB 程度になることがあります。ただし、**gzip** *filename* コマンドを使用して、このファイルを zip に圧縮できます。圧縮されたファイルを目的の場所にコピーするには **copy** コマンドを、ファイルを解凍するには **gunzip** コマンドを使用します。

show tech-support コマンドのデフォルト出力には、次のコマンドの出力が含まれます。

- **show switchname**
- **show system uptime**
- **show interface mgmt0**
- **show interface mgmt1**
- **show system resources**
- **show version**
- **dir bootflash:**
- **show inventory**
- **show diagnostic result all**
- **show logging log**
- **show module**
- **show environment**
- **show sprom backplane**
- **show clock**
- **show callhome**
- **show cfs application**
- **show cfs lock**
- **show snmp**
- **show interface brief**
- **show interface**
- **show running-config**
- **show startup-config**
- **show ip route**
- **show arp**
- **show monitor session all**
- **show accounting log**
- **show process**
- **show process cpu**
- **show process log**
- **show process memory**
- **show processes log details**
- **show logging log**
- **show license host-id**
- **show license**
- **show license usage**
- **show system reset-reason**
- **show logging nvram**

- **show install all status**
- **show install all failure-reason**
- **show system internal log install**
- **show system internal log install details**
- **show cores**
- **show topology**
- **show kernel internal aipc**
- **show tech-support acl**
- **show vlan**
- **show vlan access-map**
- **show mac-address-table**
- **show spanning-tree summary**
- **show spanning-tree active**
- **show interface trunk**
- **show aclmgr status**
- **show aclmgr internal dictionaries**
- **show aclmgr internal log**
- **show aclmgr internal ppf**
- **show aclmgr internal state-cache**
- **show access-lists**
- **show platform software ethpm internal info all**
- **show object-group**
- **show logging onboard obfl-logs**

show tech-support brief コマンド

スイッチの設定の概要を素早く確認するには、**show tech-support brief** コマンドを使用します。このコマンドを使用すると、スイッチの現在の実行状態のサマリーが表示されます（次の例を参照）。

show tech-support brief コマンドは、使用中のスイッチに関する情報を収集してトラブルシューティングを行う場合に便利です。シスコのテクニカル サポート担当者に問題を報告する場合に、このコマンドの出力を提出してください。

ヒント　**show tech-support brief** コマンドに **>**（左向き矢印）とファイル名を付加することにより、このコマンドの出力をファイルに保存できます。

次に、スイッチ設定の概要を表示する例を示します。

```
switch# show tech-support brief
Switch Name           : switch
Switch Type            :
Kickstart Image       : 4.0(0) bootflash:///nuova-or-kickstart-nsg.4.0.0.001.bin
System Image         : 4.0(0) bootflash:/nuova-or-system-nsg.4.0.0.001.binnms-or-47
IP Address/Mask     : 172.16.24.47/24
```

```
Switch WWN           : 20:00:00:0d:ec:6b:cd:c0
No of VSANs           : 1
Configured VSANs   : 1

VSAN    1:    name:VSAN0001, state:active, interop mode:default
              domain id:0xa6(166), WWN:20:01:00:0d:ec:6b:cd:c1 [Principal]
              active-zone:<NONE>, default-zone:deny


--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                          Mode  Speed  Channel
                         Mode                                (Gbps)
--------------------------------------------------------------------------------
fc3/1      1      auto   on      down             swl    --           --
fc3/2      1      auto   on      sfpAbsent        --     --           --
fc3/3      1      auto   on      down             swl    --           --
fc3/4      1      auto   on      sfpAbsent        --     --           --
fc3/5      1      auto   on      down             swl    --           --
fc3/6      1      auto   on      sfpAbsent        --     --           --
fc3/7      1      auto   on      down             swl    --           --
fc3/8      1      auto   on      down             swl    --           --

--------------------------------------------------------------------------------
Interface                Status     IP Address        Speed    MTU   Port
                                                                     Channel
--------------------------------------------------------------------------------
Ethernet1/1              sfpIsAbsen --                --       1500  --
Ethernet1/2              sfpIsAbsen --                --       1500  --
Ethernet1/3              up         --                10000    1500  --
Ethernet1/4              sfpIsAbsen --                --       1500  --
Ethernet1/5              sfpIsAbsen --                --       1500  --
Ethernet1/6              sfpIsAbsen --                --       1500  --
Ethernet1/7              sfpIsAbsen --                --       1500  --
Ethernet1/8              sfpIsAbsen --                --       1500  --
Ethernet1/9              sfpIsAbsen --                --       1500  --
Ethernet1/10             sfpIsAbsen --                --       1500  --
Ethernet1/11             sfpIsAbsen --                --       1500  --
Ethernet1/12             sfpIsAbsen --                --       1500  --
Ethernet1/13             sfpIsAbsen --                --       1500  --
Ethernet1/14             sfpIsAbsen --                --       1500  --
Ethernet1/15             notConnect --                --       1500  --
Ethernet1/16             sfpIsAbsen --                --       1500  --
Ethernet1/17             sfpIsAbsen --                --       1500  --
Ethernet1/18             sfpIsAbsen --                --       1500  --
Ethernet1/19             notConnect --                --       1500  --
Ethernet1/20             sfpIsAbsen --                --       1500  --
Ethernet1/21             sfpIsAbsen --                --       1500  --
Ethernet1/22             sfpIsAbsen --                --       1500  --
Ethernet1/23             sfpIsAbsen --                --       1500  --
Ethernet1/24             sfpIsAbsen --                --       1500  --
Ethernet1/25             sfpIsAbsen --                --       1500  --
Ethernet1/26             sfpIsAbsen --                --       1500  --
Ethernet1/27             sfpIsAbsen --                --       1500  --
Ethernet1/28             sfpIsAbsen --                --       1500  --
Ethernet1/29             sfpIsAbsen --                --       1500  --
Ethernet1/30             sfpIsAbsen --                --       1500  --
Ethernet1/31             sfpIsAbsen --                --       1500  --
Ethernet1/32             sfpIsAbsen --                --       1500  --
Ethernet1/33             sfpIsAbsen --                --       1500  --
Ethernet1/34             sfpIsAbsen --                --       1500  --
Ethernet1/35             up         --                10000    1500  --
Ethernet1/36             sfpIsAbsen --                --       1500  --
Ethernet1/37             sfpIsAbsen --                --       1500  --
```

```
Ethernet1/38            sfpIsAbsen --                --       1500  --
Ethernet1/39            sfpIsAbsen --                --       1500  --
Ethernet1/40            sfpIsAbsen --                --       1500  --

--------------------------------------------------------------------------------
Interface                Status     IP Address        Speed    MTU
--------------------------------------------------------------------------------
mgmt0                    up         172.16.24.47      100      1500
```

show tech-support fc コマンド

スイッチの FC 設定に関する情報を取得するには、**show tech-support fc** コマンドを使用します。**show tech-support fc** コマンドの出力には、次のコマンドの出力が含まれます。

- **show interface brief**
- **show interface**
- **show port internal info all**
- **show port internal event-history lock**
- **show port internal event-history msgs**
- **show port internal event-history errors**
- **show port internal mem-stats detail**
- **show san-port-channel internal event-history all**
- **show san-port-channel internal event-history errors**
- **show san-port-channel internal event-history msgs**
- **show san-port-channel internal event-history lock**
- **show san-port-channel internal mem-stats detail**
- **show san-port-channel usage**
- **show san-port-channel summary**
- **show san-port-channel consistency detail**
- **show tech-support device-alias**
- **show fcdomain domain-list**
- **show tech-support fcns**
- **show fcns database vsan 1-4093**
- **show fcns database detail vsan 1-4093**
- **show fcns database local vsan 1-4093**
- **show fcns database local detail vsan 1-4093**
- **show fcns statistics vsan 1-4093**
- **show fcns statistics detail vsan 1-4093**
- **show fcns internal info vsan 1-4093**
- **show fcns internal event-history**
- **show fcns internal event-log**
- **show fcroute unicast**

- **show fcs database**
- **show fcs ie**
- **show fctimer**
- **show flogi database**
- **show flogi internal info**
- **show fspf**
- **show fspf database**
- **show tech-support rscn**
- **show rscn internal vsan 1-4093**
- **show rscn internal event-history**
- **show rscn internal mem-stats detail**
- **show rscn internal session-history vsan 1-4093**
- **show rscn internal merge-history vsan 1-4093**
- **show rscn statistics vsan 1-4093**
- **show rscn scr-table vsan 1-4093**
- **show rscn session status vsan 1-4093**
- **show vsan**
- **show vsan membership**
- **show tech-support zone**
- **show zone status vsan 1-4093**
- **show zoneset active vsan 1-4093**
- **show zoneset vsan 1-4093**
- **show zone vsan 1-4093**
- **show fcalias vsan 1-4093**
- **show zone-attribute-group vsan 1-4093**
- **show zone policy vsan 1-4093**
- **show zoneset pending active vsan 1-4093**
- **show zoneset pending vsan 1-4093**
- **show zone pending vsan 1-4093**
- **show zone pending active vsan 1-4093**
- **show fcalias pending vsan 1-4093**
- **show zone policy pending vsan 1-4093**
- **show zone pending-diff vsan 1-4093**
- **show zone analysis active vsan 1-4093**
- **show zone analysis vsan 1-4093**
- **show zone ess vsan 1-4093**
- **show zone internal vsan 1-4093**
- **show zone internal change event-history vsan 1-4093**

- **show zone internal ifindex-table vsan 1-4093**
- **show zone internal merge event-history vsan 1-4093**
- **show zone internal event-history**
- **show zone internal event-history errors**
- **show zone internal tcam event-history vsan 1-4093**
- **show zone statistics vsan 1-4093**
- **show system default zone**
- **show zone internal ddas-table**
- **show zone internal sdv-table vsan 1-4093**
- **show zone internal mem-stats**
- **show zone internal mem-stats detail**
- **show zone internal transit-table received vsan 1-4093**
- **show zone internal transit-table forwarded vsan 1-4093**
- **show zone internal transit-table rejected vsan 1-4093**

ヒント　**show tech-support zone** コマンドに **>**(左向き矢印)とファイル名を付加することにより、このコマンドの出力をファイルに保存できます。

show tech-support platform コマンド

スイッチのプラットフォーム設定情報を取得するには、**show tech-support platform** コマンドを使用します。

show tech-support platform コマンドの出力には、次のコマンドの出力が含まれます。

- **show platform fwm mem-stats detail**
- **show platform fwm info global**
- **show platform fwm info pif all verbose**
- **show platform fwm info lif all verbose**
- **show platform fwm info vlan all verbose**
- **show platform fwm info error stats**
- **show platform fwm info error history**
- **show platform fwm info stm-stats**
- **show platform fwm info pc all verbose**
- **show platform fwm info ppf**
- **show platform fwm info pss all**
- **show platform hardware fwm info vlan all**
- **show platform hardware fwm info pif all**
- **show platform hardware fwm info lif all**
- **show platform hardware fwm info global**

- **show platform software zschk internal info**
- **show platform software zschk internal msgs**
- **show platform software statsclient msgs**
- **show hardware internal gatos detail**
- **show hardware internal gatos all-ports detail**
- **show hardware internal altos detail**
- **show hardware internal altos event-history errors**
- **show hardware internal altos event-history messages**
- **show platform fcfib fcflow**
- **show platform fcfib event-history all**
- **show platform fcfib unicasts**
- **show platform fcfib unicasts forwarding-configuration**
- **show platform fcfib vsan**
- **show platform fcfib san-port-channel**
- **show platform software fcfib devices**
- **show platform software fcfib multipath**
- **show platform software fcfib vsanidxtable**
- **show platform software fcfib domainidxtable**
- **show platform hardware fcfib pathselecttable**
- **show platform hardware fcfib pathselecttable all**
- **show platform software fcfib fctable-check**
- **show fc2 internal event-history errors**
- **show system internal liod liod_db**
- **show system internal liod queues**
- **show system internal liod state**
- **show system internal liod time_db**
- **show system internal rib domain**
- **show system internal rib system-attributes**
- **show system internal rib unicast**
- **show system internal rib vsan-attributes**
- **show system internal fcfwd fwidxmap if_index**
- **show system internal fcfwd idxmap interface-to-port**
- **show system internal fcfwd pcmap**
- **show platform afm info global**
- **show platform afm info attachment brief**
- **show platform afm info group-cfg all**
- **show platform afm info lop all**
- **show platform software altos detail**

- **show platform software altos event-history errors**
- **show platform software altos event-history msgs**
- **show platform software altos ports all**
- **show platform hardware altos counters all**
- **show platform hardware altos counters interrupts all**
- **show platform hardware altos interrupts all detail**

デフォルト設定

表 50-1 に、この章で説明した機能のデフォルト設定値を示します。

表 50-1　　トラブルシューティング機能のデフォルト設定値

パラメータ	デフォルト
fctrace を呼び出すタイムアウト時間	5 秒
fcping 機能によって送信されるフレーム数	5 フレーム
リモート キャプチャ接続プロトコル	TCP
リモート キャプチャ接続モード	Passive
ローカル キャプチャ フレーム制限	10 フレーム
FC ID の割り当てモード	auto モード

CHAPTER 51

設定の制限値

Cisco Nexus 5000 シリーズ スイッチがサポートする機能には、設定の最大制限値があります。一部の機能については、最大値に達していない制限値をサポートする設定を検証しました。表 51-1 に、Cisco NX-OS Release 4.0が稼働するスイッチで、シスコが確認した制限値および最大制限値を示します。

表 51-1　設定の制限値

機能	確認された制限値	最大制限
スイッチあたりの VLAN[1]	250	1024 から設定済み VSAN（仮想 SAN）の数を引いた値
イーサネット MTU	9,216 バイト	9,216 バイト（ASIC 制限値）
PVRST+	250 PVRST+ インスタンス、 4,000 STP インターフェイス ステート	53,248 STP インターフェイス ステート[2]
スイッチあたりの MST インスタンス（すべてのインスタンスが RSTP 対応）	64	64（IEEE 標準）
ステーション テーブル[3]	16,000 エントリ	32,000 エントリ
IP マルチキャスト アドレス（IGMP スヌーピング）	1,000 個のアドレス	1,000 個のアドレス
スイッチあたりの VSAN[4]	32	256
ファブリックあたりのデバイス エイリアス	8,000	8,000
イベント トラップ:E メール経由で転送	4 つの宛先	50 個の宛先
単一の物理ファブリックまたは VSAN 内のスイッチ	50	239
VSAN あたりのドメイン	40	239
スイッチあたりのネイティブ FC リンク	8	8
N Port Virtualization（NPV）ポート グループあたりのファブリック ログイン（FLOGI）または FDISC の数	62	100
仮想または物理 F ポートあたりのゾーン（すべての VSAN を含む）	32	ASIC あたり 2,048[5]
スイッチあたりのゾーン セット（すべての VSAN を含む）	500	1,000

表 51-1　設定の制限値（続き）

機能	確認された制限値	最大制限
物理ファブリックあたりのゾーン メンバ（すべての VSAN を含む）	8,000	20,000
スイッチあたりのゾーン（すべての VSAN を含む）	8,000	8,000
SAN ファブリックの最大直径	3 ホップ	12 ホップ
スイッチあたりの FSPF インターフェイス インスタンス	256	4,096[6]
スイッチあたりの ISL インスタンス	256	256（最大 8 つのファイバ チャネル インターフェイス、それぞれに最大 32 の VSAN インスタンス）
仮想インターフェイス	52 個の仮想ファイバ チャネル インターフェイス	52 個の仮想ファイバ チャネル インターフェイス
Quality of Service（QoS）システム クラス	ユーザ設定可能な 4 つのクラス	ユーザ設定可能な 4 つのクラス
スイッチ全体の VLAN ACL（VACL）エントリ	1,024	ASIC の制限[7]
物理イーサネット インターフェイスあたりのポート ACL（PACL）エントリ	128	ASIC の制限[7]
ACL アカウンティング	32	ASIC ごとに 256 カウンタ[8]
ファイバ チャネル フロー	32	ASIC ごとに 256 カウンタ[8]
ポート チャネル	4 個の SAN ポート チャネルと 12 個のイーサネット ポート チャネル	16 個のポート チャネル（SAN およびイーサネット ポート チャネルの任意の組み合わせ）
SPAN セッション	2 つのアクティブ セッション	設定済みの 18 個のセッション（2 つはアクティブ）
出力 SPAN 送信元	2	2

1. 4094 Virtual LAN（VLAN）ID スペース全体がサポートされます。
2. 1024 STP インスタンス回数 52 10-ギガビット イーサネット ポート。
3. ステーション テーブルには、すべてのユニキャスト イーサネット MAC アドレスおよびイーサネット マルチキャスト アドレスが含まれます。
4. 4094 VSAN ID スペース全体がサポートされます。
5. この ASIC 制限が重要になるのは、将来のソフトウェアリリースのみです（イーサネット インターフェイスごとに複数の仮想インターフェイスを設定できる場合）。
6. これは、拡張 ISL（スイッチ間リンク）の数（16）と VSAN の数（256）を掛け合せた数です。
7. 各 ASIC は、複数のセクションに分割された 2,000 エントリの TCAM をサポートします。各セクションには最低 64 エントリが含まれている必要があり、64 エントリ単位でのみ拡張することができます。このソフトウェアでは次のエントリが予約済みです：スーパバイザ エンジンへのパケット リダイレクションに 128 エントリ、2 つの SPAN セッションに 64 エントリ、VACL に 1024 エントリ、PACL に 576 エントリ、QoS に 64 エントリ。
8. 各 ASIC がサポートする 256 カウンタは、ポリサー（ACL アカウンティング、ファイバ チャネル フローなど）の間で共有されます。バイトまたはパケットのいずれかをカウントするように各カウンタを設定できます。VACL または PACL には、システム全体で 32 アカウンティング エントリという制限が適用されます。