BladeSymphony 10Gb DCB スイッチ

Network OS 管理者ガイド

３．０．０対応

HITACHI

■対象製品

このマニュアルは BladeSymphony 10Gb DCB スイッチモジュールを対象に記載しています。また、DCB スイッチモジュールのソフトウェア Network Operating System 3.0 の機能について記載しています。
なお、本マニュアル記載以外の機能については、サポート対象外となります。

■注意・警告など

次に示す表記と説明がこのマニュアルで使用されています。これらは記載順に重要度が高くなります。

NOTE

ヒント、ガイド、アドバイス、重要情報、関連情報などを示しています。

ATTENTION

ハードウェアやデータに悪影響がある可能性を示しています。

CAUTION

ハードウェア、ファームウェア、ソフトウェア、データの破損・破壊に至る状況があることを示しています。

■輸出時の注意

本製品を輸出される場合には，外国ため替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上，必要な手続きをお取りください。
なお，ご不明な場合は，弊社担当営業にお問い合わせください。

■商標一覧

Brocade, B-wing シンボルは、Brocade Communications Systems, Inc.の米国および他の国々における登録商標です。

Cisco は，米国 Cisco Systems, Inc. の米国および他の国々における登録商標です。

Ethernet は，米国 Xerox Corp. の商品名称です。

Microsoft は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。

UNIX は，X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。

Windows は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。

イーサネットは，富士ゼロックス（株）の商品名称です。

そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■ご注意

このマニュアルの内容については，改良のため，予告なく変更する場合があります。

■発行

２０１３年　１０月　(第３版)

■著作権

目　次

図一覧

表一覧

1 Network OS と Brocade VCS ファブリック テクノロジ イントロダクション

1.1 Network OS イントロダクション

Brocade Network OS (NOS) は、ミッションクリティカル、次世代データセンタを対象として設計されており、次の機能をサポートします。

- 簡単化されたネットワーク管理

  Brocade VCS ファブリックは、自己形成、自己修復機能を持ち、非常に大規模で動的なクラウドでのデプロイメントに必要なスケーラブルな運用基盤を提供します。マルチノードのファブリックは、単一の論理要素として管理することができ、ファブリックが配備されて、特定のワークロードのニーズに最適化されたさまざまな構成に簡単に再配備することができます。
  概要については 24 ページの『1.2 Brocade VCS』を参照下さい。Brocade VCS ファブリック テクノロジの詳細は、90 ページの『9 ファブリック管理』を参照下さい。
- 高い回復力

  Brocade VCS ファブリックはハードウェアベースの ISL トランキングを使用し、トラフィックが中断することなく、自動リンクフェイルオーバーを提供します。
- ネットワーク利用率の改善

  Transparent Interconnection of Lots of Links (TRILL)に基づくレイヤ２ルーティングサービスは、ネットワークに等価コストマルチパスを提供し、その結果、ネットワークの利用率を改善します。Brocade VCS ファブリック テクノロジは、レイヤ 2 ドメインの成長に対する制約を取り除き、トロンボーンネットワークを排除し、ファブリック内での VLAN 間ルーティングを有効にする、複数のアクティブな、完全にロードバランスされたレイヤ 3 ゲートウェイを提供します。

  Virtual Router Redundancy Protocol (VRRP)は、参加しているホストへの仮想 IP ルーターを動的に割り当てることによって、静的なデフォルトルート環境での単一障害点を排除します。仮想ルーター内のすべてのルーターのインタフェースは、同じ IP サブネットに属している必要があります。異なる LAN 上の別のアドレス･マッピングを使用して仮想ルーターID（VRID）を再利用することに対する制限はありません。

  TRILL に関する追加情報は、90 ページの『9.1 TRILL』を参照下さい。

  VRRP/VRRP-E の概要については、90 ページの『9 ファブリック管理』参照下さい。
- サーバ仮想化

  Automatic Migration of Port Profile (AMPP)機能は、イーサネットポリシーに基づくファブリック全体のコンフィグレーションを提供し、ポート毎のプロファイルの転送を行い、仮想マシン(VM)の可搬性を支援するためのネットワークレベルの機能を有効にします。

  AMPP に関する更に詳細な情報は、153 ページの『14 AMPP の設定』を参照下さい。

Network OS では、単一の業界標準のコマンドラインインタフェース(CLI)で全ての機能を設定できます。Network OS の全コマンドをアルファベット順にリストされ詳細を説明している『Network OS Command Reference』を参照下さい。

1.1.1 Brocade VCS ファブリック用語

このドキュメントでは次の言葉が使われます。

エッジポート	イーサネットファブリック内でエンドステーションやスイッチやルーターを含む末端装置に接続される全てのスイッチポート
イーサネットファブリック	分散インテリジェンスを実現するため情報を交換するイーサネットスイッチが結合されたグループ
ファブリックポート	イーサネットファブリック内のインタースイッチリンク(ISL)の両端のポート
インタースイッチリンク(ISL)	VCS ファブリック内のスイッチ間を接続するインタフェース。イーサネットファブリック内のスイッチ間の接続インタフェースの両端のポートは、ISL ポートかファブリックポートと呼ばれます。ISL は、単一リンクもしくは Brocade トランクで構成する複数リンクとなる。このトランクには、Brocade 独自のトランク、または標準の IEEE 802.3ad ベースのリンクアグリゲーションとして作成することができます。
RBridge	VCS ファブリック内の物理スイッチ
RBridge ID	RBridge のユニークな識別子。コマンドでは、VCS ファブリック内の全てのインタフェースを参照する際に RBridge ID が使われる。RBridge ID の設定に関する詳細は、94 ページの『9.3 Brocade VCS ファブリックの構成管理』を参照下さい。
VCS ID	VCS ファブリックのユニークな識別子。デフォルトの VCS ID は 1 です。VCS ファブリック内の全てのスイッチは、同じ VCS ID が必要です。
WWN	工場でスイッチに設定されるグローバルにユニークな識別子。

1.2 Brocade VCS ファブリック テクノロジ イントロダクション

Brocade VCS ファブリック テクノロジは、フラットで仮想化されたコンバージドデータセンタネットワークの構築を可能とするレイヤ２イーサネットテクノロジです。Brocade VCS ファブリック テクノロジは、スケーラブルに思いのままにネットワークを拡張することができます。

Brocade VCS ファブリック テクノロジは 3 つのコアな設計に基づいています。

- 自動化
- 弾力性
- 進化的デザイン

２つ以上の Brocade VCS ファブリックスイッチが接続されると、それらはイーサネットファブリックを形成し、分散インテリジェンスを実現するため、相互に情報を交換します。外部のネットワークに対して、イーサネットファブリックは一つのロジカルシャーシとして見えます。

図 1-1 に、従来の階層的イーサネットアーキテクチャを使ったデータセンタと VCS アーキテクチャを使った同じデータセンタの例を示します。Brocade VCS ファブリック アーキテクチャはアクセス及び

アグリゲーションレイヤを結合し、サーバラックを追加するといった拡張性があります。

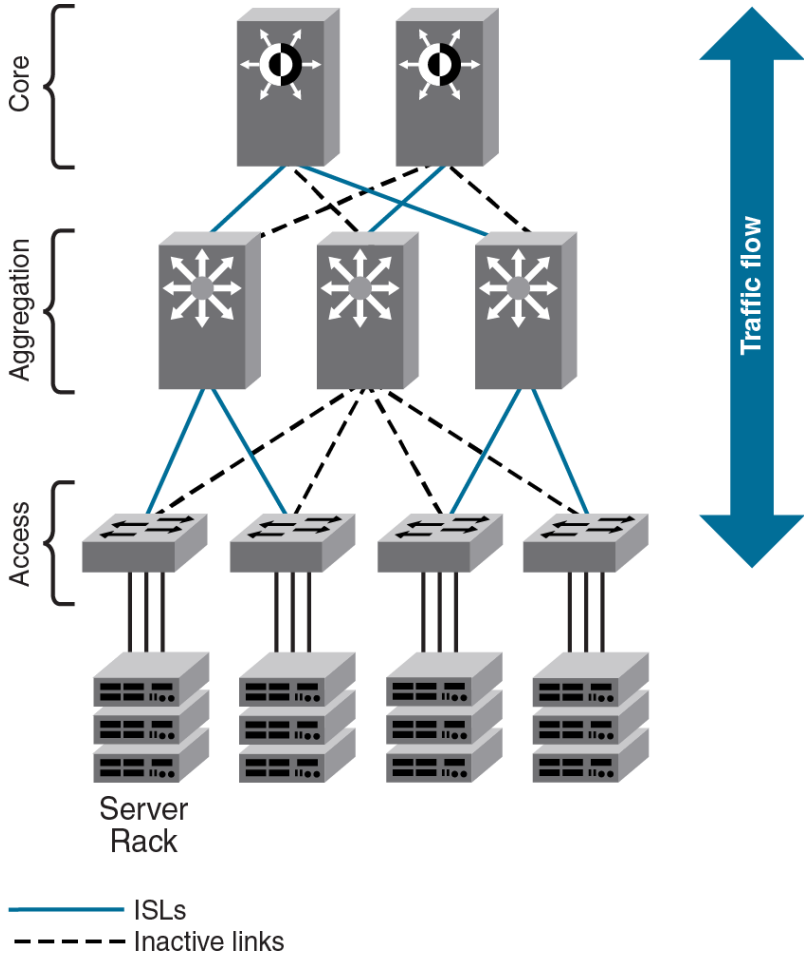

図 1-1 従来のイーサネットと VCS アーキテクチャの比較

1.2.1 自動化

弾力性は、ファイバーチャネルストレージネットワークの基礎的な属性であり、また、クラスタ化されたアプリケーションや厳しいコンピューティングサービスレベルアグリーメント（SLAs）が要求される現代のデータセンタの要件でもあります。VCS ファブリックテクノロジを開発する上で、このコア特性は、イーサネットファブリックデザインに引き継がれています。

STP を使用している従来のイーサネットネットワークでは、リンクの 50%だけがアクティブになります。図 1-2 の点線で示すように、残りはプライマリ接続が失敗した場合にバックアップとして機能します。

２つ以上の VCS モードのスイッチが接続されると、図 1-2 に示すようなイーサネットファブリックを形成します。

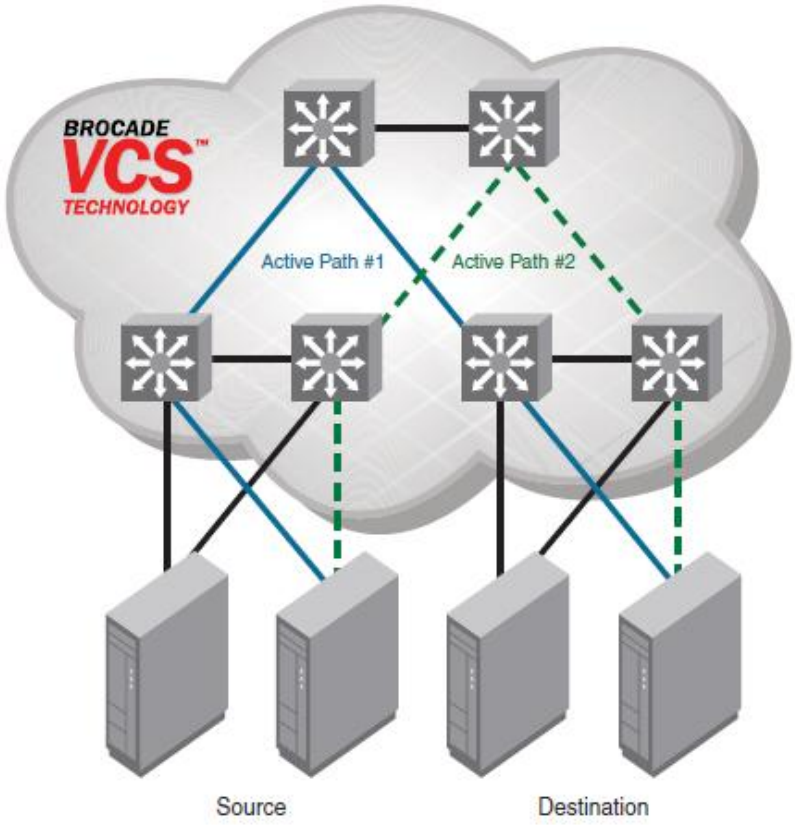

図 1-2 マルチパスを持ったイーサネットファブリック

イーサネットファブリックは次の特徴を持ちます。

- スイッチングに基づくネットワークです。イーサネットファブリックは、基本となるテクノロジとして Transparent Interconnection of Lots of Links (TRILL)と呼ばれる新しい規格を使用します。
- すべてのスイッチは、自動的に互いに接続されているすべての物理的および論理的なデバイスを認識しています。
- ファブリック内のすべてのパスが使用可能です。トラフィックは、常に等価コストパスに分散されます。図 1-2 に示すように、ソースからデスティネーションまでのトラフィックは２つのパスを通ります。
- トラフィックは最短のパスを通ります。
- 単一のリンク障害が発生すると、トラフィックは自動的に別の利用可能なパスを経由します。図 1-2 では、Active Path #1 の一つのリンクがダウンした場合、トラフィックは Active Path #2 を通って途切れることなく経由します。
- イーサネットファブリックが接続しているサーバやデバイスや外部のネットワークに単一の論理スイッチに見えるため、ファブリック内にスパニングツリープロトコル(STP)は必要ありません。
- トラフィックはあるイーサネットファブリックから別のイーサネットファブリックに切り替えることができます。

1.2.2 分散インテリジェンス

VCS ファブリックテクノロジでは、すべての関連情報は、図 1-3 に示すように、結合されたファブリ

ック機能を提供するために、スイッチの各メンバに自動的に配布されます。ブロケードの VCS ファブリックは、それぞれの新しいスイッチがファブリックの設定を継承し、新しいポートがすぐに利用できるように、一つの "論理的なシャーシ"として管理できるように設計されています。ファブリックは、一つのスイッチとしてもとのネットワークに戻ります。これは、大いに信頼性を向上させ、トラブル低減し、管理レイヤの複雑さを軽減します。

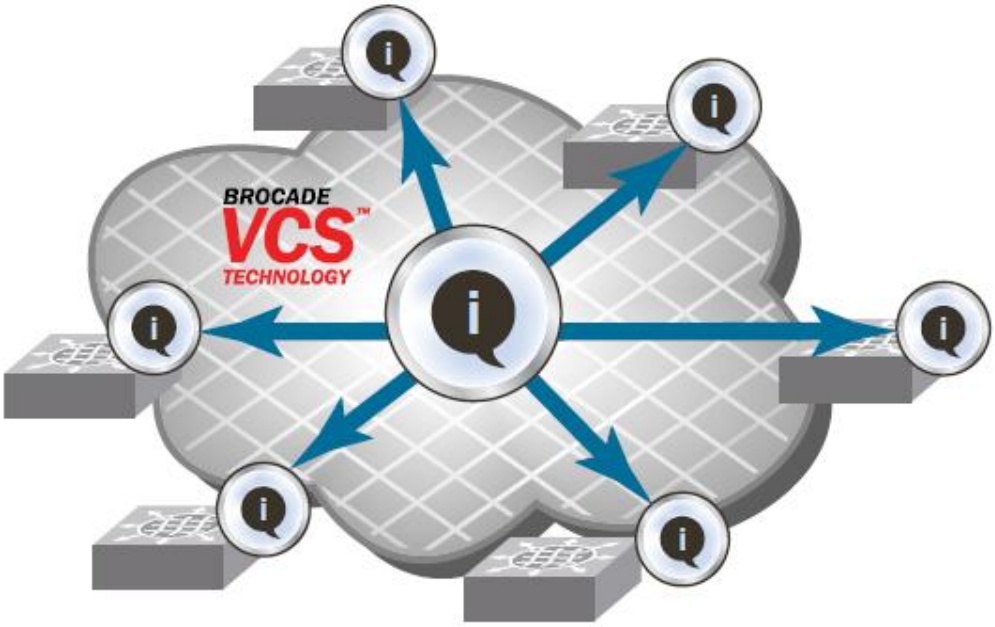

図 1-3 イーサファブリック内の分散インテリジェンス

分散インテリジェンスは次の特徴を持ちます。

- ファブリックは自己形成します。２つの VCS モードのスイッチが接続されると、ファブリックは自動的に生成され、スイッチは共通のファブリック構成を検出します。
- ファブリックはマスタレスです。一つのスイッチが構成情報を格納するわけでもファブリックを制御するわけでもありません。どのスイッチが故障しても取り除かれても、継続できないようなファブリックのダウンタイムやトラフィック遅延を起こしません。
- ファブリックは全てのメンバ、デバイス、仮想マシン(VMs)を認識します。もし、VM がファブリック内のある VCS ポートから別の VCS ポートに移動する場合、ポートプロファイルが自動的に新しいポートに移動します。

1.2.3 ロジカルシャーシ

イーサネットファブリックの全てのスイッチは、それらが一つのロジカルシャーシであるかの様に管理されます。外部のネットワークにとって、ファブリックは他のレイヤ２スイッチと違いがありません。図 1-4 イーサファブリック内のロジカルシャーシは、２つのスイッチを備えたイーサネットファブリックを示しています。外部ネットワークは、ファブリック内のエッジポートだけを認識して、ファブリック内の接続は認識しません。

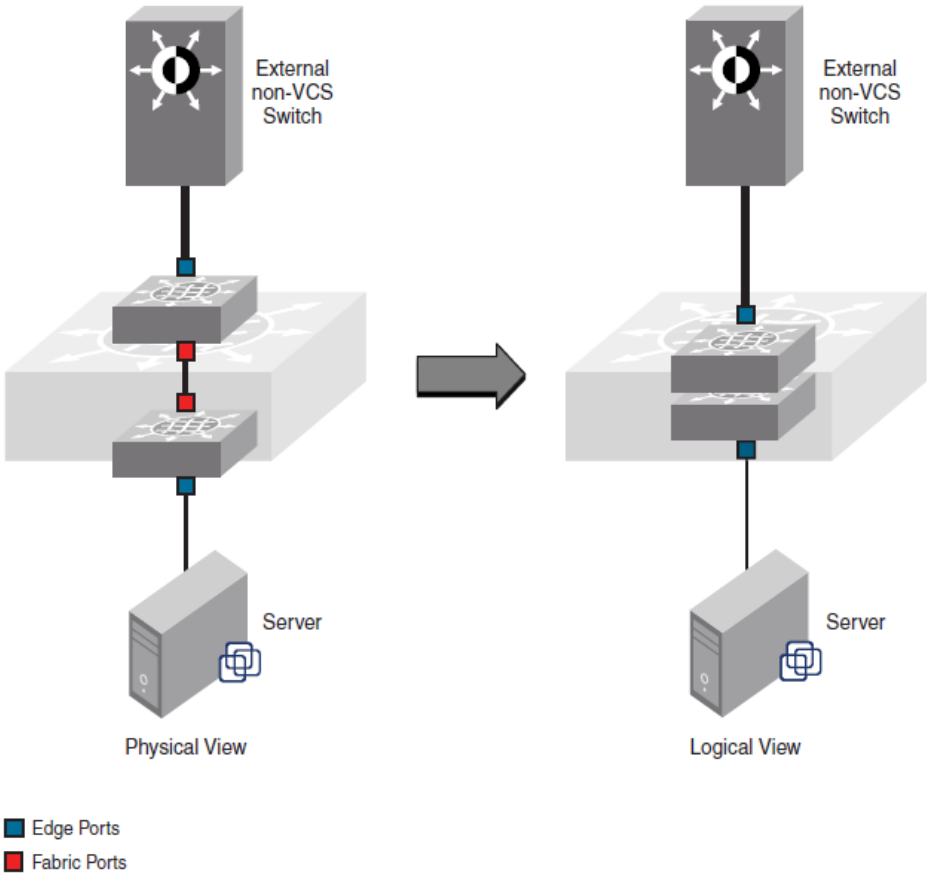

図 1-4 イーサファブリック内のロジカルシャーシ

ファブリック内の各物理スイッチは、シャーシ型スイッチのモジュールであるかのように管理されます。VCS モードのスイッチがファブリックに接続されると、そのスイッチはファブリックの設定を引き継いで、即座に新しいポートが有効になります。

1.2.4 イーサネットファブリックの形成

VCS ファブリックプロトコルは、最小のユーザー設定でイーサネットファブリックの形成を支援するように設計されています。イーサネットファブリックの形成手順に関する詳細な情報は、90 ページの『9.2 Brocade VCS ファブリックの形成』を参照下さい。VCS モードを有効・無効にする方法に関する情報は、94 ページの『9.3 Brocade VCS ファブリックの構成管理』を参照下さい。

内蔵 DCB スイッチは、Brocade VCS ファブリックモードを無効にした状態で出荷されています。Brocade vcs ファブリックモードを有効にする方法については、94 ページの 『9.3.1 VCS ファブリック設定作業』を参照してください。

1.2.5 自動的隣接検出

VCS モードのスイッチにスイッチを接続すると、VCS モードのスイッチは、隣接スイッチが VCS モードであるかどうかを決定します。もし、スイッチが VCS モードで VCS ID が同じであれば、スイッチはイーサネットファブリックに加わります。

VCS ID を変更する方法は、94 ページの『9.3 Brocade VCS ファブリックの構成管理』参照下さい。

1.2.6　自動 ISL 形成とハードウェアベーストランキング

スイッチがイーサネットファブリックに参加すると、ファブリック内の直接接続されたスイッチ間は自動的に ISL が形成されます。

２つのスイッチ間に２本以上の ISL があるなら、Brocade ISL トランクが自動的に形成されます。同一の隣接した Brocade スイッチと接続した全ての ISL は、トランクを形成しようとします。これらのトランクを形成するために、ユーザーは介入する必要はありません。

ISL とトランクの有効・無効に関する情報は、95 ページの『9.4 ファブリックインタフェースの構成管理』を参照下さい。

1.2.7　Principal RBridge の選択

イーサネットファブリック内で最も小さい WWN を持つ RBridge は Principal RBridge に選ばれます。

Principal RBridge の役割は、ファブリックに新たに参加した RBridge がファブリック内に既に存在する RBridge ID と競合しているかどうかを判断することです。もし競合していると、Principal RBridge は参加した RBridge を分離したままにします。

RBridge ID の設定に関する情報は、94 ページの『9.3 Brocade VCS ファブリックの構成管理』を参照下さい。

1.3　Brocade VCS ファブリック テクノロジ の使用例

この節では、Brocade VCS ファブリック テクノロジのための以下の使用例を示します。

- 従来のイーサネット
- 大規模なサーバ仮想化

1.3.1　従来のイーサネットアクセスとアグリゲーションの使用例

VCS は、図 1-5 に示すように、既存のトップオブラックスイッチと同じように展開することができます。右端の 2 つのサーバラックでは、2 つのスイッチのイーサネットファブリックは、各ラックのイーサネットスイッチを置き換えます。

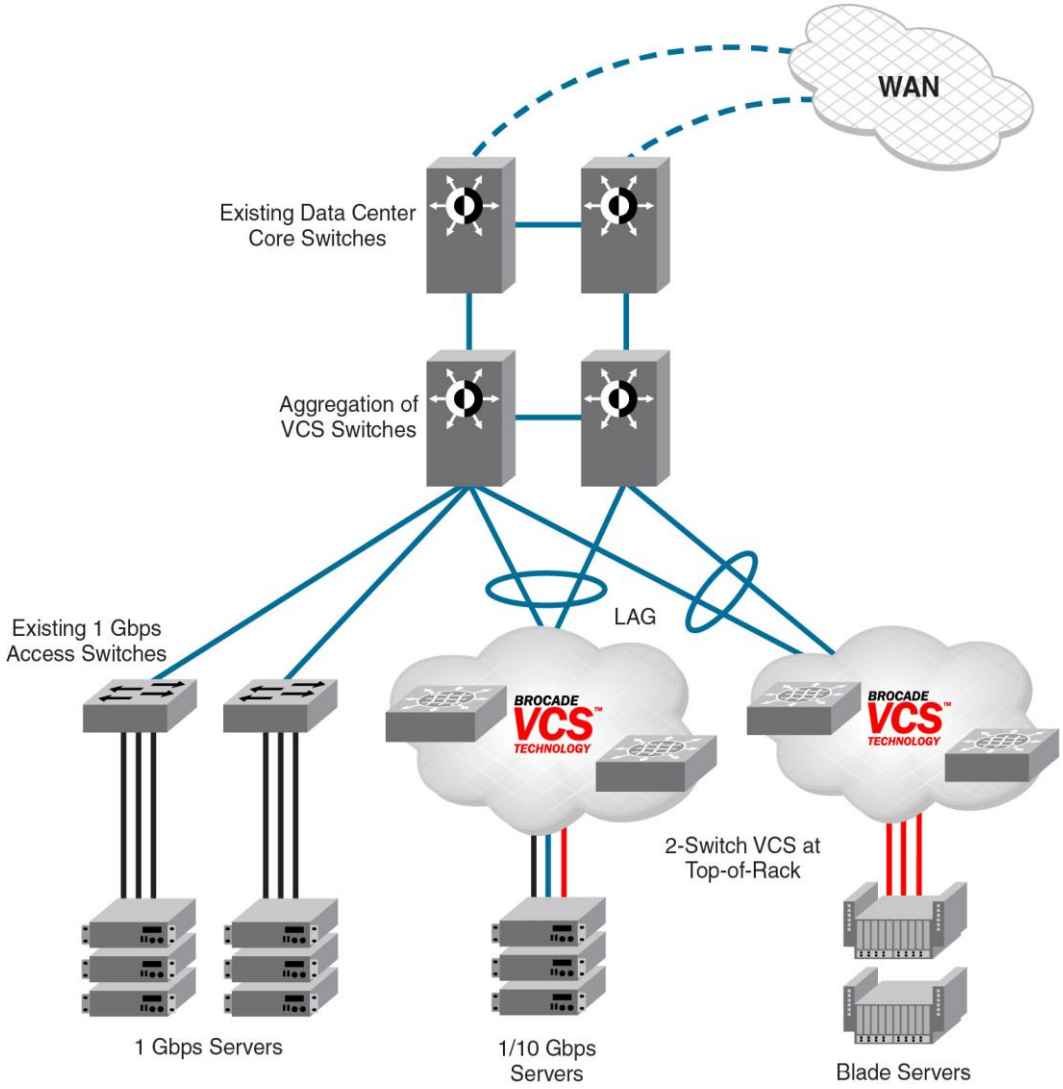

図 1-5 サーバラック上部の Brocade VDX スイッチのペア

サーバは、アクティブ／アクティブな接続、エンドツーエンドを可能にする、単一の top-of-rack(ToR) スイッチと見えます。この使用例での VCS ファブリック テクノロジは次のような利点を提供します。

- 増加する効果的帯域をもった複数のアクティブ - アクティブ接続
- 既存のアーキテクチャの維持
- 既存のコアおよびアグリゲーションネットワーク製品と連携して動作
- 既存のアクセススイッチとの共存
- 1Gbps と 10Gbps のサーバ接続性をサポート
- サーバラックやブレードサーバと共に動作

1.3.2 大規模サーバ仮想化の使用例

図 1-6 は、エッジでの Brocade VCS ファブリックを使用した論理的な 2 層アーキテクチャを示しています。各々の Brocade VCS ファブリックはファブリックの外のスイッチへの一つの仮想スイッチとなります。その結果、ネットワークを平坦化します。

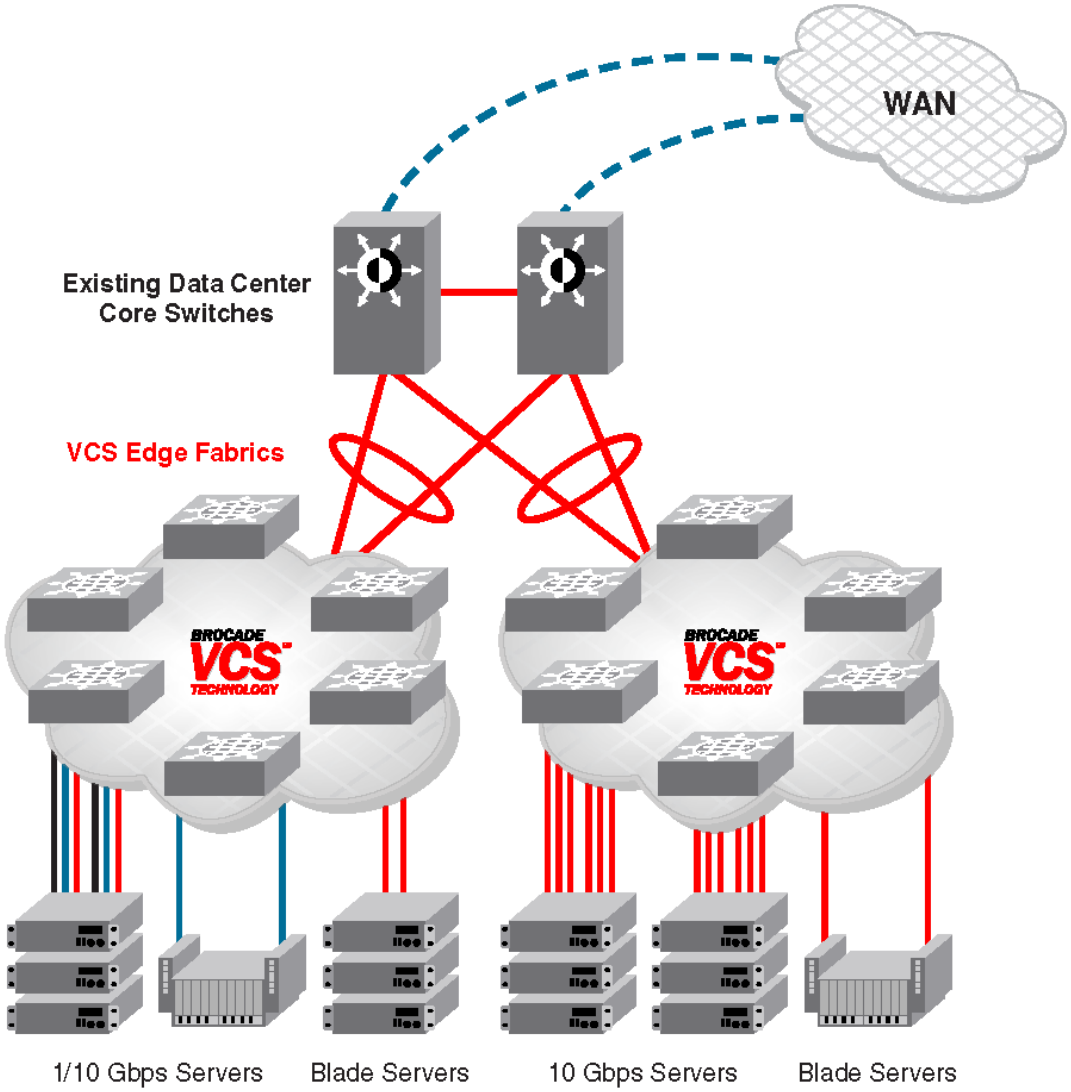

図 1-6 仮想マシンの移動を可能にしたフラットなレイヤ 3 ネットワーク

この使用例での VCS ファブリック テクノロジは次のような利点を提供します。

- マルチパスネットワークを最適化（すべてのパスおよびレイヤ 3 ゲートウェイがアクティブで、単一障害箇所がなく、STP を必要としません。）
- 仮想マシン(VM)の可搬性の範囲の拡大

1.4 トポロジとスケーリング

Brocade VCS ファブリックに最大 24 のスイッチが存在することができます。Brocade VCS ファブリックを構築するために任意のネットワークトポロジを使用することができますが、次のトピックは拡張性、性能、データセンタで見られるトポロジの一般的な可用性に関する考慮事項について述べています。

- コア・エッジトポロジ
- リングトポロジ

- フルメッシュトポロジ

1.4.1　コア・エッジトポロジ

コア・エッジトポロジでは、デバイスは、コアスイッチを介して相互に接続されているエッジスイッチに接続します。図 1-7 に示す例では、3 つのコアスイッチを使用しています。高い可用性と優れたスループット、または、より効率的にリンクとポートを使用する必要があるか応じて、コア内により多くまたは、より少ないスイッチを使用することができます。

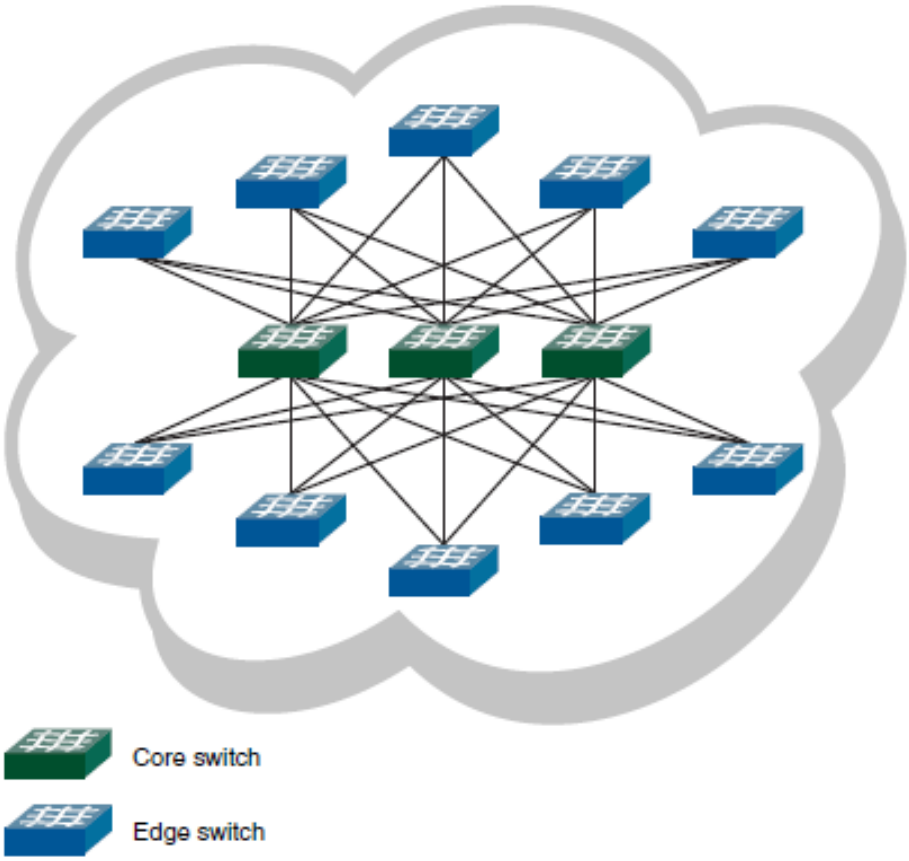

図 1-7 コア・エッジトポロジ

このトポロジは、信頼性が高く高速で拡張性に優れています。複数のコアスイッチを持っているので信頼性が高くなります。もし、コアスイッチまたはコアスイッチへのリンクに障害が発生した場合、代替パスが利用可能です。このため、コアスイッチ数を増やすことでクラスタが許容できるリンクやコアスイッチの障害数も増えます。
また、複数のコアスイッチが負荷を共有しているため、スループットが高く、ホップカウントが低いため、高いパフォーマンスと低遅延が保証されます。
トポロジの拡大には、さらなるコアスイッチやリンクの追加を必要とします。しかし、一般的には、例えば完全なメッシュトポロジーほどは必要ありません。

1.4.2　リングトポロジ

リングトポロジでは、単一の連続した経路を形成し、正確に 2 つの他のノードに各ノードを接続します。各ノードがすべてのパケットを扱って経路に沿ってノードからノードへ伝わります。図 1-8 にリングトポロジを示します。

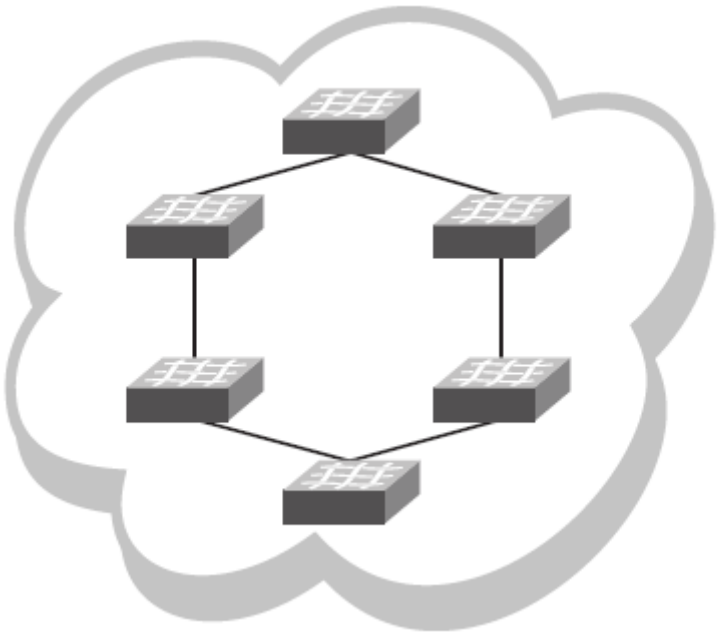

図 1-8 リングトポロジ

このトポロジは、非常にスケーラブルですが、障害やトラフィックの影響を受けやすいです。スイッチ間リンクおよびポートの効率的利用において高度にスケーラブルであり、ノード追加は、2 つのポートだけをリングに接続すればよいです。この 2 つのノード間では 1 本の経路だけを提供するので、障害に影響されやすくなります。ファブリックのスループットは最も遅いリンクまたはノードによって制限されます。そのために二つのスイッチ間で通信を行うのにかかるレイテンシが高くなる可能性があります。このトポロジはポートの使用効率が重要だが、可用性とスループットがそれほど重要ではない場合に有用です。

1.4.3　フルメッシュトポロジ

フルメッシュトポロジでは、他のすべてのクラスタノードに各ノードを接続します。図 1-9 に、フルメッシュトポロジを示します

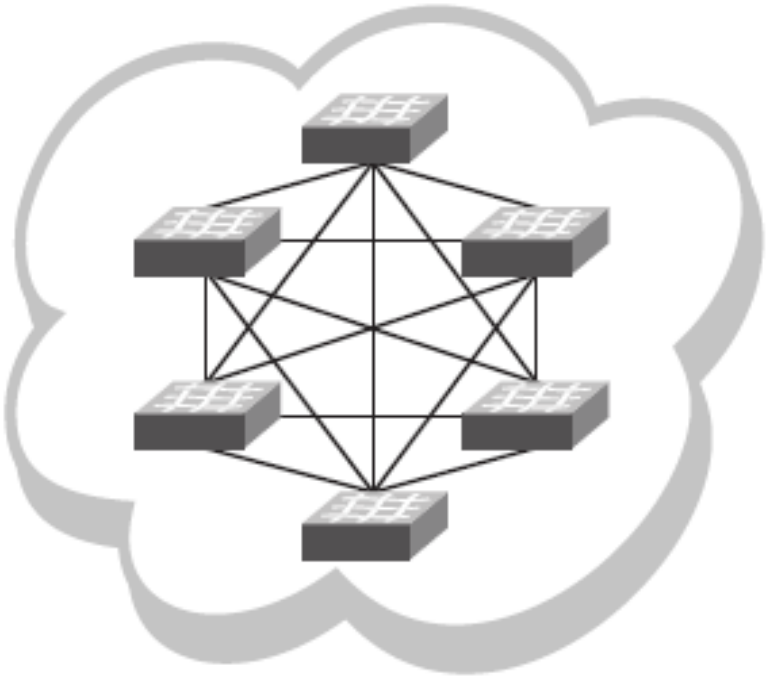

図 1-9　フルメッシュトポロジ

このトポロジは、ファブリックを通して多くの経路を提供しますので、ケーブルまたはノードに障害が発生した場合に、信頼性が高く、ファブリック内のどのノードにでも 1 ホップで着くことができるので、低レイテンシで高速です。しかし、各ノード追加は指数関数的にファブリックリンクとスイッチポートの数を増加させるので、スケーラビリティはよくありません。
このトポロジは小規模なファブリックにのみ適しています。

1.5 レイヤ２イーサネットの概要

内蔵 DCB スイッチは、古典的なレイヤ 2 イーサネットネットワークもサポートします。（図 1-10 を参照）レイヤ 2 イーサネットの動作では、コンバージドネットワークアダプタ（CNA）を持つホストは、DCB スイッチの DCB ポートに直接接続することができます。また、古典的な 10 ギガビットイーサネットネットワークインターフェースカード（NIC）を使用している別のホストは、DCB ポートに直接接続するか、または古典的なレイヤ 2 イーサネットネットワークを介して接続することができます。

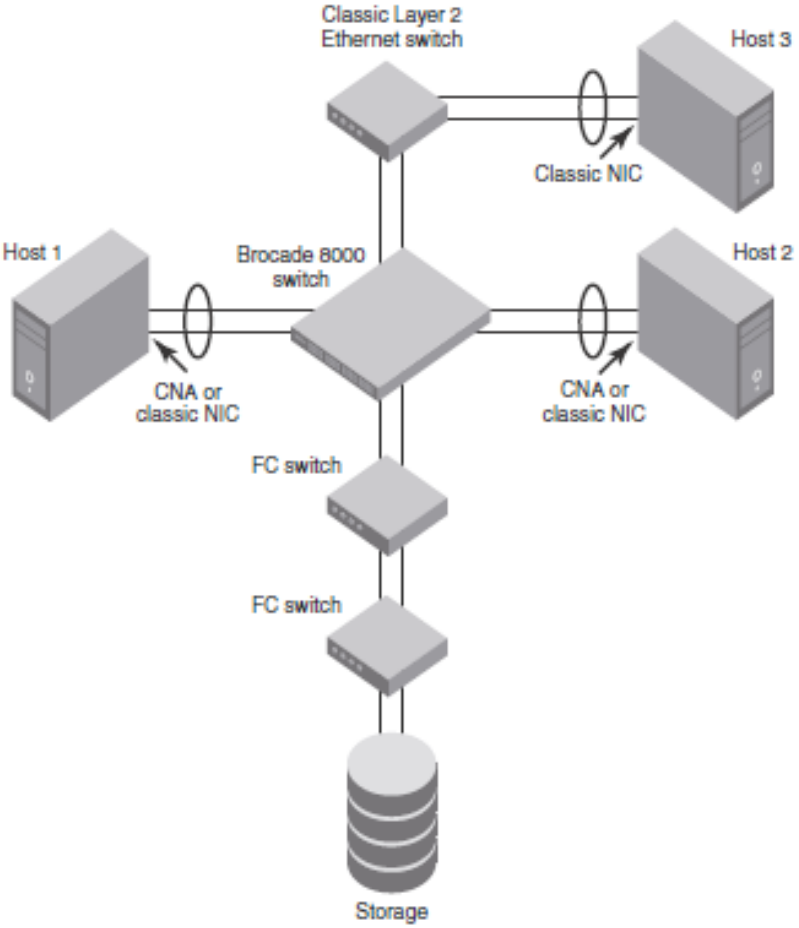

図 1-10 複数のスイッチファブリック構成

1.5.1 レイヤ 2 転送

レイヤ 2 イーサネットフレームは、DCB ポートに転送されます。802.1Q VLAN のサポートは、特定の VLAN に着信フレームをタグ付けするために使用され、802.3ac VLAN タギングのサポートは、外部デバイスからの VLAN タグ付きフレームを受け入れるために使用されます。

Network OS v3.0.0 は、レイヤ 2 スイッチの間に次の 802.1D ブリッジングプロトコルを使用してループフリーネットワーク環境を維持します。

- スパニングツリープロトコル（STP）
- ラピッドスパニングツリープロトコル（RSTP）
- マルチプルスパニングツリープロトコル（MSTP）
- パーVLAN スパニングツリープロトコル（PVST+）
- ラピッドパーVLAN スパニングツリープロトコル（RPVST+）

これらのプロトコルの設定の詳細については、178 ページの『16 スパニングツリーの設定』を参照してください。

内蔵 DCB スイッチは、次のようにイーサネットフレームを処理します。

- 宛先 MAC アドレスがルックアップテーブルに登録されていない場合、フレームは入力ポートを除いて、同じ VLAN 内のすべてのポートにフラッディングされます。
- 宛先 MAC アドレスがルックアップテーブル内に存在する場合、フレームが唯一の正しい出力ポートに切り替えられます。
- 宛先 MAC アドレスがルックアップテーブルに存在しており、出力ポートが入力ポートと同じである場合、フレームは廃棄されます。
- イーサネットフレームチェックシーケンス（FCS）が誤っているならば、スイッチがカットスルーモードに入っているので、正しくフォーマットされたイーサネットフレームは誤った FCS で送出されます。
- イーサネットフレームが短すぎる場合、フレームは廃棄され、エラーカウンタがインクリメントされます。
- イーサネットフレームが長すぎる場合、フレームは切り捨てられ、エラーカウンタがインクリメントされます。切り捨てられたフレームは誤った FCS で送出されます。
- ブロードキャスト宛先 MAC アドレスに送信されたフレームは、入力ポートを除いて、同じ VLAN 内のすべてのポートにフラッディングされます。
- ルックアップテーブルの MAC アドレスエントリがタイムアウトするとき、それらは削除されます。このイベントでは、フレームフォワディングがユニキャストからフラッディングに変わります。
- デバイスが新しい場所に移動したときにルックアップテーブル内の既存の MAC アドレスエントリが破棄されます。デバイスを移動する場合、新しいポートからの入力フレームは、古いルックアップテーブルエントリは破棄され、新しいエントリがルックアップテーブルに挿入されます。新しいポートへのフレーム転送は、ユニキャストのままです。
- ルックアップテーブが一杯の時、最も古い MAC アドレスがある時間が経過しタイムアウトに達したあと、新しいエントリは最も古い MAC アドレスに代わります。まだトラフィックの実行を持っている MAC アドレスは、タイムアウトされません。

NOTE
ルックアップテーブルは、その 32K 容量の 90%に達すると、新しいエントリは、古いエントリの置き換えを開始します。

1.5.2 VLAN タグ付け

レイヤ 2 スイッチは、常に着信フレームに VLAN ID を付け加えます。着信フレームがタグなしの場合は、そのタグはポート設定に基づいて追加されます。ポートは、単一の VLAN または複数の VLAN にタグなしトラフィックを分類できます。着信フレームが既にタグ付けされている場合、ポートは転送またはポート構成で許可される VLAN のルールに従ってフレームを破棄します。
以下に、VLAN タグ付けの 3 つの例を示す。

- DCB ポートが着信フレームに単一の VLAN ID をタグ付けするように構成されている場合、タグが付いていない着信フレームは、VLAN ID でタグ付けされます。
- DCB ポートが着信フレームに複数の VLAN ID をタグ付けするように構成されている場合、タグ

が付いていない着信フレームは、ポートの設定に基づいて、適切な VLAN ID でタグ付けされます。
- DCB ポートが外部からタグ付きフレームを受け入れるように構成されている場合は、VLAN ID でタグ付けされている着信フレームは、変更されずに渡されます。

VLAN の設定の詳細については、167 ページの『15 VLAN の設定』を参照してください。

1.5.3 フレーム分類（着信）

内蔵 DCB スイッチは、以下の基準に基づいて着信イーサネットフレームを分類することができます。

- ポート番号
- プロトコル
- MAC アドレス

分類されたフレームは、VLAN ID または、802.1p イーサネットプライオリティーを付け加えることができます。802.1p のイーサネットプライオリティタギングは、レイヤ 2 サービスの分類（CoS）を使用して行われます。802.1p のイーサネットプライオリティーは、VLAN 内のトラフィックに優先度を設定するレイヤ 2 CoS を使用して、VLAN のフレームをタグ付けするために使用されます。内蔵 DCB スイッチでは、外部デバイスによってタグ付けされたフレームを受け入れます。
フレーム分類のオプションは次のとおりです。

- 物理ポート番号による VLAN ID とレイヤ 2 CoS
  このオプションを使用すると、内蔵 DCB スイッチの物理ポート上に予め設定された VLAN ID およびレイヤ 2 CoS に着信フレームを分類するためにポートを設定します。
- LAG の仮想ポート番号による VLAN ID とレイヤ 2 CoS
  このオプションを使用すると、リンクアグリゲーショングループ（LAG）仮想ポートのプリセット VLAN ID およびレイヤ 2 CoS に着信フレームを分類するためにポートを設定します。
- レイヤ 2 CoS 変換
  このオプションを使用すると、QoS 変換機能を有効にすることにより、Layer 2 CoS セッティングを変更するようポートを設定します。
- レイヤ 2 CoS トラスト
  このオプションを使用すると、QoS トラスト機能を有効にすることで、着信フレームのレイヤ 2 CoS を受け入れるようポートを設定されます。

QoS を設定する詳細については、240 ページの『21 QoS の設定』を参照してください。

1.5.4 輻輳制御とキューイング

内蔵 DCB スイッチは、いくつかの輻輳制御とキューイング機能をサポートしています。出力キューが輻輳状態に近づくと、ランダム早期検出（RED）を選択的に使用され、最大リンク利用率を維持するために積極的にフレームをドロップします。着信フレームは、着信フレームのレイヤ 2 CoS が設定に基づいて、プライオリティキューに分類されるか、レイヤ 2 CoS フィールドが DCB ポートまたは VLAN

のセッティングに基づいた書き換えによって分類されます。
内蔵 DCB スイッチは、出力ポートにキューのフレームに 2 つのスケジューリング機能（厳密な優先順位キューイング、不足加重ラウンドロビン（DWRR）キューイング）の組み合わせをサポートしています。
802.1Qaz Enhanced Transmission Selection（ETS）で指定されるようにスケジューリングアルゴリズムは、8 つのトラフィッククラスに取り組んでいます。
キューイング機能を、次に説明します。

- RED－RED は、リンクの使用率が増加します。複数の着信 TCP トラフィックストリームが同じアウトバウンドポートに切り替えられる場合、他のトラフィックストリームが大きなフレームを送信しながら、いくつかのトラフィックストリームが小さなフレームを送信していると、リンク使用率が 100%に達することができません。RED が有効になっている場合は、リンクの使用率が 100 パーセントに近づきます。
- 分類－ユーザー優先度を設定する。
    - インバウンドフレームは、受信ポートに設定されたユーザー優先度でタグ付けされます。アウトバウンドポートでフレームを検査するときにタグが付加されます。デフォルトでは、すべてのフレームは、優先順位をゼロにタグ付けされています。
    - 外部タグ付けされたレイヤ 2 フレームは、ポートが外部からのタグ付きレイヤ 2 フレームを受け入れるように設定されているときは、ユーザー優先度は着信フレームのレイヤ 2 CoS に設定されています。
- キューイング
    - 入力キューイング ― 入力キューイング次の方法でトラフィックフローを最適化します。DCB ポートはいくつかのプライオリティの値がタグ付けされている着信トラフィックがあり、異なるプライオリティの設定からのトラフィックが、別のアウトバウンドポートに切り替えられます。他が混雑していないけれども、いくつかのアウトバウンドポートがすでにバックグラウンドトラフィックで混雑しています。入力キューイングでは、混雑していないポートへの切り替えられるトラフィックストリームのトラフィックレートは高いままです。
    - 出力キューイング ― 出力キューイングは、次の方法でトラフィックフローを最適化します。いくかのポートは、異なる優先度設定でインバウンドトラフィックを伝送します。すべてのポートからのトラフィックは、同じアウトバウンドポートに切り替えられます。インバウンドのポートが、異なるトラフィックレートを持っている場合、いくつかのアウトバウンド優先度グループを、その他を混雑していないままにして、混雑させます。出力キューイングでは、混雑していないトラフィックストリームのトラフィックレートは高いままです。
    - マルチキャストレート制限 ― マルチキャストレート制限の限定的な例は、典型的なマルチキャストレートは、いくつかのプライオリティ値のタグが付いているマルチキャストインバウンドトラフィックを、いくつかのポートが運んでいるときです。異なる優先順位の設定を使用もったトラフィックが異なるアウトバウンドポートに切り替えられます。マルチキャストレート制限は、出力ポート上の総マルチキャストトラフィックレートが指定された一連のレート制限未満になるように設定されています。
    - マルチキャスト入力キューイング ― 典型的なマルチキャスト入力キューイングの例は、いくつ

かのポートが複数のプライオリティ値のタグが付いているマルチキャストのインバウンドトラフィックを運んでいるときです。異なる優先順位の設定をもったラフィックが異なるアウトバウンドポートに切り替えられます。他が混雑していないが、いくつかのアウトバウンドポートがすでにバックグラウンドトラフィックが混雑しています。混雑していないポートへの切り替えは、トラフィックストリームのトラフィックレートは高いままとなります。すべてのアウトバウンドポートは、すべての着信ポートからのいくつかのマルチキャストフレームを運ぶ必要があります。これは、設定された閾値に対する相対的な値でマルチキャストトラフィックの配信を可能にします。

- マルチキャスト出力キューイング ― 典型的なマルチキャスト出力キューイングの例は、複数のポートがマルチキャストインバウンドトラフィックを運んでいるときです。各ポートは、異なる優先順位が設定されています。すべてのポートからのトラフィックは、同じアウトバウンドポートに切り替えられます。インバウンドポートはトラフィックレートを変化させた場合、他が混雑していないまま、一部の送信優先度グループは混雑します。混雑していないトラフィックストリームのトラフィックレートは高いままです。アウトバウンドポートは、すべての着信ポートからのいくつかのマルチキャストフレームを運ぶ必要があります。

- スケジューリング ― スケジューリングポリシー（ストリクトプライオリティ 0 およびストリクトプライオリティ 1 のモードを使用）の典型的な例は、ポート 0-7 は、インバウンドトラフィックを運び、ポート 0 は優先順位 0 を持つ、ポート 1 は優先順位 1 を持つなど、各ポートはユニークなプライオリティレベルを持ちます。すべてのトラフィックは、同じアウトバウンドポートに切り替えられます。ストリクトプライオリティ 0 モードでは、すべてのポートが DWRR スケジューリングを持っているため、すべてのポートの 1 秒あたりのフレーム（FPS）は、DWRR の設定に対応しています。ストリクトプライオリティ 1 モードでは、優先順位 7 のトラフィックがストリクトプライオリティを使用するため、優先度 7 は、より高い FPS を達成することができます。同じ優先度をもった入力ポートからのフレームは、出力ポートにラウンドロビン方式でスケジューリングされます。
  スケジューリングポリシーを設定する場合、DWRR スケジューリングを使用している各優先グループは、PG_Percentage パラメータを設定することにより、総帯域幅の割合を使用するように設定できます。

QoS を設定する詳細については、240 ページの『21 QoS の設定』を参照してください。

1.5.5 アクセス制御

アクセスコントロールリスト（ACL）は、レイヤ 2 スイッチング、セキュリティのために使用されます。標準 ACL は、着信ポートの送信元アドレスを検査します。拡張 ACL では、送信元アドレスと宛先アドレスとプロトコルによってフィルタリングできます。ACL は、DCB ポートまたは VLAN に適用することができます。

ACL は、次のように機能します。

- 物理ポート上で設定された標準イーサネット ACL は、送信元 MAC アドレスに基づいてフレームを許可または拒否するために使用されます。デフォルトでは、すべてのフレームの受け入れを許可することになっています。

- 物理ポート上で設定された拡張イーサネット ACL は、送信元 MAC アドレス、宛先 MAC アドレス、および EtherType に基づいてフレームを許可または拒否するために使用されます。デフォルトでは、すべてのフレームの受け入れを許可します。
- LAG の仮想ポートに設定された標準イーサネット ACL は、送信元 MAC アドレスに基づいてフレームを許可または拒否するために使用されます。デフォルトでは、すべてのフレームの受け入れを許可します。 LAG ACL は、LAG 内のすべてのポートに適用されます。
- LAG の仮想ポートで設定された拡張イーサネット ACL は、送信元 MAC アドレス、宛先 MAC アドレス、および EtherType に基づいてフレームを許可または拒否するために使用されます。デフォルトでは、すべてのフレームの受け入れを許可します。LAG ACL は、LAG 内のすべてのポートに適用されます。
- VLAN に設定された標準イーサネット ACL は、送信元 MAC アドレスに基づいてフレームを許可または拒否するために使用されます。デフォルトでは、すべてのフレームの受け入れを許可します。VLAN ACL は、VLAN のための Switch Vertical Interface（SVI）に適用されます。
- VLAN 上で設定された拡張イーサネット ACL は、送信元 MAC アドレス、宛先 MAC アドレス、および EtherType に基づいてフレームを許可または拒否するために使用されます。デフォルトでは、すべてのフレームの受け入れを許可します。VLAN ACL は、VLAN のための Switch Vertical Interface（SVI）に適用されます。

ACL の設定の詳細については、231 ページの『20 アクセスコントロールリスト(ACL)の設定』を参照してください。

1.5.6 トランキング

NOTE
イーサネットネットワークの用語の"トランキング"は、任意の一つのリンクまたはポートの限界を超えてリンク速度を高め、高可用性のための冗長性を高めるために並列に複数のネットワークリンク（ポート）を使用することを指します。

802.1ab Link Layer Discovery Protocol（LLDP）は、接続されたスイッチまたはホストへのリンクを検出するために使用されます。トランクは、隣接するスイッチまたはホストおよび内蔵 DCB スイッチの間で設定することができます。
Data Center Bridging Capability Exchange Protocol（DCBX）は、隣接するスイッチ、またはホスト上の DCB 対応ポートを識別するために使用されています。LLDP および DCBX の設定の詳細については、216 ページの『18 NIC 冗長(track)の設定』を参照してください。
802.3ad Link Aggregation Control Protocol（LACP）は、すべての個々のリンクの組み合わせた帯域幅を持つトランクを作成するために複数のリンクを結合するために使用されます。LACP の設定の詳細については、205 ページの『17 リンクアグリゲーションの設定』を参照してください。

NOTE
Brocade ソフトウェアは、最大 24 の LAG インタフェースをサポートしています。

1.5.7　フロー制御

802.3x イーサネットポーズとイーサネットの Priority-based Flow Control (PFC)は、リンクの送信元側でトラフィックを遅くすることにより、フレーム破棄を防ぐために使用されます。多くは輻輳などが原因で、スイッチまたはホスト上のポートが送信元から多くのトラフィックを受信する準備ができていない場合、送信元へポーズフレームを送信し、トラフィックフローを一時停止します。輻輳が解消された時、送信元へトラフィックフローを一時停止する要求を止め、任意のフレームを落とすことなく、トラフィックを再開します。

イーサネットポーズが有効になっている場合、ポーズフレームは、トラフィックの送信元に送信されます。同様に、PFC が有効になっている場合、ポーズフレームが送信元スイッチに送信され、フレームのドロップはありません。

イーサネットポーズと PFC の設定の詳細については、240 ページの『21 QoS の設定』を参照してください。

2 Network OS CLI の使い方

2.1 コマンドラインインタフェース(CLI)

Network OS CLI は、イーサネット/IP ネットワーク管理でよく知られた業界標準の階層化コマンドラインインタフェースとなっています。
システムは、Network OS のデフォルトコンフィグレーションとスタートアップコンフィグレーションを使って立ち上がります。ログイン後は、Network OS シェルモードとなります。Network OS シェルモードでの CLI コマンドの使用方法は、43 ページの『2.1.5 Network OS CLI コマンドモード』を参照下さい。

2.1.1 コンフィグレーションの変更の格納

スイッチに対するあらゆるコンフィグレーションの変更は、running-config ファイルに反映されます。変更を恒久的に反映するためには、下記に示すように copy コマンドを使って、running-config を startup-config に適用します。
特権実行モードでの running-config ファイルの適用例

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

2.1.2 Network OS CLI インタフェースの RBAC 権限

ロールベースアクセス制御(RBAC)は、アカウントに割当られているロール(役割)に基づいて、ユーザーアカウントの権限を定義するものです。ロールは、スイッチのユーザーアカウントのアクセス権限が定義されたものです。ユーザーは、何れか一つのロールに関連付けられます。RBAC に関する詳細は、111 ページの『11.2 ロールベースアクセス制御』を参照下さい。

2.1.3 デフォルトロール

デフォルトのロール属性は、変更することが出来ません。しかし、デフォルトでのロールは非デフォルトのユーザーアカウントに割り当てることが出来ます。次に示すロールがデフォルトのロールです。

- 管理者のロールは最も高い特権レベルを持っています。管理者ロールに関連付けられたユーザーは、全てのコマンド(CLI)を使用することが出来ます。デフォルトでは、管理者のロールはリード/ライト権限を持っています。
- ユーザーのロールは、特権実行モードにおいて show コマンドにほぼ限定されている制限された権限となります。ユーザーアカウントは、グローバルコンフィグレーションモードに於いてコンフィグレーションコマンドを使うことが出来ないユーザロールに関連付けられています。デフォルトでは、ユーザロールはリード権限のみです。

2.1.4　telnet を使った Network OS CLI へのアクセス方法

NOTE

この例では、スイッチにログインするために管理者ロールを使っていますが、何れの権限でも使うことが出来ます。

Network OS CLI へアクセスするための手順は、コンソールインタフェースでも telnet セッションでも同じで、ログインプロンプトが表示されます。

```
switch login: admin
Password:**********
switch#
```

NOTE

複数のユーザーは telnet セッションで、特権実行モードを使って操作することは可能です。

Network OS V3.0.0 は 32 セッションまでサポートしています。

2.1.5　Network OS CLI コマンドモード

表 2-1 に Network CLI コマンドモードとアクセス方法をリストしています。

NOTE

現在の作業ディレクトリを表示するために'pwd'コマンドを使います。このコマンドはグローバルコンフィグレーション(global configuration)モードとグローバルコンフィグレーションモードからアクセス可能なモードで使用できます。

表 2-1　Network OS CLI コマンドモード

コマンドモード	プロンプト	コマンドモードへの移行方法	説　明
Privileged EXEC	switch#	スイッチのデフォルトモード	システムパラメータの表示変更を行います。これは、管理者モードで基本的な構成コマンドを含んでいます。
Global configuration	switch(config)#	特権実行モードから'configure terminal'コマンドを実行	スイッチ全体に影響する機能を構成します。

表 2-1　Network OS CLI コマンドモード（続き）

コマンドモード	プロンプト	コマンドモードへの移行方法	説　明
Interface configuration	Port-channel: switch(config-Port-channel-63)# 10-Gigabit Ethernet (DCB port): switch(conf-if-te-0/1)# VLAN: switch(conf-Vlan-1)#	特権実行モードから次のいずれかのコマンドを入力してインタフェースを指定します。 • interface port-channel • interface tengigabitethernet • interface vlan	インタフェース個別の表示設定を行います。
Protocol configuration	LLDP: switch(conf-lldp)# Spanning-tree: switch(conf-mstp)# switch(conf-rstp)# switch(conf-stp)# switch(conf-pvst)# switch(conf-rpvst)#	特権実行モードから次のいずれかのコマンドを入力してプロトコルを指定します。 • protocol lldp • protocol spanning-tree mstp • protocol spanning-tree rstp • protocol spanning-tree stp • protocol spanning-tree pvst • protocol spanning-tree rapid-pvst	各プロトコルの表示設定
AMPP port-profile mode	AMPP port-profile: switch(config-port-profile-name)# VLAN-profile sub-mode: switch(config-vlan-profile)# QoS-profile sub-mode: switch(config-qos-profile)# Security-profile sub-mode: switch(config-security-profile)#	特権実行モードからポートプロファイルコンフィギュレーションモード port-profile コマンドを入力して port-profile コンフィギュレーションモードを開始します。 port-profile コンフィギュレーションモードから、次のいずれかのコマンドを入力することにより、AMPP サブモードを指定します。 • vlan-profile • qos-profile • security-profile	AMPP 機能のアクセスおよび設定をします。
Feature configuration	CEE map: switch(config-cee-map-default)# Standard ACL: switch(conf-macl-std)# Extended ACL: switch(conf-macl-ext)#	特権実行モードから次のいずれかのコマンドを入力してDCB機能を指定します。 • cee-map default • mac access-list standard • mac access-list extended	CEE マップ機能のアクセスおよび設定をします。
DSCP mutation mapping	DSCP Mutation Map: switch(dscp-mutation-mapname)#	特権実行モードから次のコマンドを使用して着信した DSCP 値を再配置します。 qos map dscp-mutation *mapname*	
DSCP to CoS priority mapping	DSCP to CoS Map: switch(dscp-cos-mapname)#	特権実行モードから次のコマンドを使用して CoS プライオリティマップにDSCPを作成します。 qos map dscp-cos *mapname*	
DSCP to traffic class mapping	DSCP to Traffic Class Map: switch(dscp-traffic-class-mapname)#	特権実行モードから次のコマンドを使用して DSCP にトラフィッククラスマップを作成します。 qos map dscp-traffic-class *mapname*	

表 2-1　Network OS CLI コマンドモード（続き）

コマンドモード	プロンプト	コマンドモードへの移行方法	説　明
QoS Policer configuration	Police Priority Map switch(config-policemap)# Class Map: switch(config-classmap)# Policy Map: switch(config-policymap)# Policy-class-map submode switch(config-policymap-class)# Policy-class-map-policer attributes submode switch(config-policymap-class-police)#	特権実行モードから次のいずれかのコマンドを入力して Policer コンフィグレーションモードを指定します。 • police-priority-map *mapname* • class-map *mapname* • policy-map *mapname* policy-map モードから pollicy-class-map サブモードを開始するには、class *classmap name* を入力します。 policy-map-class サブモードから policy-class-map-policer 属性サブモードを開始するには、ポリシング属性に続きポリシーを入力します。	

NOTE

いずれのモードでも'Ctrl+Z'を押下するか'end'コマンドを入力すると、特権実行モードに移行します。'exit'コマンドを入力すると、直前のモードに移行します。

2.1.6　Network OS CLI キーボードショートカット

表 2-2 に Network OS CLI のキーボードショートカットを示します。

表 2-2　Network OS CLI キーボードショートカット

キーボードショートカット	解説
Ctrl+B または左矢印キー	一文字戻る
Ctrl+F または右矢印キー	一文字進む
Ctrl+A	コマンドラインの先頭に移動する
Ctrl+E	コマンドラインの末尾に移動する
Esc B	一単語戻る
Esc F	一単語進む
Ctrl+Z	特権実行モードに戻る
Ctrl+P または上矢印キー	最近使用したコマンドを先頭にコマンド履歴を表示する
Ctrl+N または下矢印キー	最近使用したコマンドを最後にコマンド履歴を表示する

NOTE

特権実行モードでは、'show history'コマンドで最近入力したコマンドリストが表示されます。内蔵 DCB スイッチでは、全てのターミナルから入力された直前の 1000 コマンドを記憶しています。

2.1.7　ショートカットとしての’do’コマンド使用方法

いずれかのコマンドモードで操作中に、特権実行モードのコマンドを実行したい場合、'do'コマンドが使えます。

例えば、もし LLDP の設定中に、'dir'コマンドのように特権実行モードのコマンドを実行したい場合、まず LLDP コンフィグレーションモードを抜けなければなりません。'dir'コマンドとともに do'コマンドを使用すると、コンフィグレーションモードを変更する必要がありません。以下に例を示します。

```
switch(conf-lldp)#do dir
Contents of flash://
   -rw-r-----            1276   Wed Feb  4 07:08:49 2009    startup_rmon_config
   -rw-r-----            1276   Wed Feb  4 07:10:30 2009    rmon_config
   -rw-r-----            1276   Wed Feb  4 07:12:33 2009    rmon_configuration
   -rw-r-----            1276   Wed Feb  4 10:48:59 2009    starup-config
```

2.1.8　Network OS CLI コマンド表示とコマンドシンタックス

クエスチョンマーク('?')をタイプすると、現在のコマンドモードで利用可能なコマンドをリストします。

```
switch(conf-lldp)# ?
Possible completions:
  advertise            The Advertise TLV configuration.
  description          The User description
  disable              Disable LLDP
  do                   Run an operational-mode command
  exit                 Exit from current mode
  hello                The Hello Transmit interval.
  help                 Provide help information
  iscsi-priority       Configure the Ethernet priority to advertise for iSCSI
  mode                 The LLDP mode.
  multiplier           The Timeout Multiplier
  no                   Negate a command or set its defaults
  profile              The LLDP Profile table.
  pwd                  Display current mode path
  system-description   The System Description.
  system-name          The System Name
  top                  Exit to top level and optionally run command
```

同じ文字で始まるコマンドを表示するには、入力した文字に続いてクエスチョンマーク('?')をタイプしてください。

```
switch#e?
Possible completions:
  exit   Exit the management session
```

コマンドに関連するキーワードや引数を表示するには、キーワードに続いてクエスチョンマーク('?')を入力してください。

```
switch#terminal ?
Possible completions:
  length     Sets Terminal Length for this session
  monitor    Enables terminal monitoring for this session
  no         Sets Terminal Length for this session to default :24.
  timeout    Sets the interval that the EXEC command interpreter wait for user
             input.
```

不完全なキーワードとクエスチョンマーク('?')をタイプされ、キーワードが入力文字で始まるキーワードの場合は、CLI はそのキーワードのヘルプを表示します。

```
switch#show d?
Possible completions:
  debug    Debug
  diag     Show diag related information
  dot1x    Show dot1x
  dpod     Provides License Information on Pod in fabric
```

不完全なキーワードとクエスチョンマーク('?')をタイプされ、キーワードが幾つかのキーワードにマッチする場合は、マッチした全てのキーワードのヘルプを表示します。

```
switch#show i?
  interface  Interface status and configuration
  ip         Internet Protocol (IP)
```

Network OS CLI はコマンドの省略形が使用できます。この例では、'show qos interface all'コマンドの省略形を示しています。

```
switch#sh q i a
```

装置がコマンドを認識できない場合は、エラーメッセージを表示します。

```
switch#hookup
        ^
syntax error: unknown argument.
```

不完全なコマンドが入力された場合は、エラーメッセージを表示します。

```
switch#show
           ^
syntax error: unknown argument.
```

2.1.9　Network OS CLI コマンド補完機能

コマンドやキーワードを自動的に補完するために、コマンドやキーワードを入力して Tab キーを押します。例えば、CLI コマンドプロンプトで、'te'と入力し Tab キーを押します。

```
switch#te
```

CLI は次のコマンドを表示します。

```
switch#terminal
```

もし、タイプされた文字に関連する一つ以上のコマンドやキーワードがあれば、Network OS CLI は全ての選択肢を表示します。例えば、CLI コマンドプロンプトで、'show l'と入力し Tab キーを押します：

```
switch#show l
```

CLI は次のコマンドを表示します。

```
switch#show l
Possible completions:
  lacp
  license    Display license keys installed on the switch.
  lldp       Link Layer Discovery Protocol(LLDP).
  logging    Show logging
```

2.1.10 Network OS CLI コマンド出力修飾子

Network OS CLI は表 2-3 に示すコマンド出力修飾子を使用して CEE CLI の show コマンド出力をフィルタすることができます。

表 2-3　CEE CLI コマンド出力修飾子

出力フィルタ	説　明
Append	指定されたファイルに出力を追加します。
Redirect	指定されたコマンド出力をファイルにリダイレクトします。
Include	指定された表現を含むコマンド出力を表示します。
Exclude	指定された表現を含まないコマンド出力を表示します。
Begin	指定された表現で始まるコマンド出力を表示します。
Last	コマンド出力の最後の数行を表示します。
Tee	指定されたファイルにコマンド出力をリダイレクトします。この修飾子は、コマンド出力が表示されないことに注意してください。
until string	出力テキストが文字列に一致したときに出力を終了します。
Count	コマンド出力の行数を表示します。
Linnum	コマンド出力で表示される行に番号を付加します。
More	１画面ごとにコマンド出力を一時停止します。
Nomore	一時停止することなく、全てのコマンド出力を表示します。
FLASH	フラッシュメモリに出力をリダイレクトします。

3 スイッチ管理の基本

3.1 スイッチに接続する

内蔵 DCB スイッチに接続するには、シリアルポートを使ったコンソールセッションか、管理ポートへの telnet/SSH により接続することが出来ます。ログインするためには、装置内にローカルに定義されているアカウントか、認証サーバによる認証システムを構築されている場合は、認証サーバに定義されたアカウントをご使用いただけます。初期設定のためには、装置のデフォルト構成定義である事前定義の管理者アカウントご使ください。

- シリアルポートもしくは管理ポート経由での接続方法については、『BladeSymphony ユーザーズガイド』の『10Gb DCB スイッチモジュールの設定』をご参照下さい。
- また、ネットワーク経由の接続については、53 ページの『3.5 イーサネット管理インタフェースの構成』も参照下さい。

3.1.1 telnet または SSH による接続

1. マネージメントモジュールでスイッチベイの IP アドレス設定を行い、イーサネットケーブルをマネジメントモジュールの RJ-45 ポートに接続します。(詳細は、『BladeSymphony ユーザーズガイド』を参照下さい。)
2. 管理端末から、スイッチの管理用 IP アドレスを使って telnet もしくは SSH セッションをオープンします。(更に詳細な管理 IP アドレス設定については、53 ページの『3.5 イーサネット管理インタフェースの構成』を参照下さい。)
3. ログインプロンプトに対して、ユーザーアカウントを入力します。
4. パスワードを入力します。
5. 正常にログインできたか確認します。(ホスト名称に続いてシャープ('#')のプロンプトが表示されます。)

```
login as: admin
admin@10.20.49.112's password:******
-----------------------------------------------------
WARNING: The default password of 'admin' and 'user' accounts have not been
changed.
Welcome to the Brocade Network Operating System Software
admin connected from 10.110.100.92 using ssh on VDX6720-24
```

3.2 スイッチの情報設定

スイッチは、IP アドレス、ワールドワイドネーム（WWN)、スイッチ ID、RBridge ID、ホスト名やシャーシ名で識別されます。'switch-attributes'コマンドでホスト名やシャーシ名をカスタマイズできます。

- ホスト名は３０文字までで、英文字で始まり、英文字、英数字、アンダースコアが使用できます。デフォルトのホスト名称は"sw0"です。ホスト名は、プロンプトに表示されます。
- 各プラットフォームに対してシャーシ名称をカスタマイズすることをお奨めします。もし、意味のあるシャーシ名を割り当てるなら、システムログはシャーシ名でスイッチを識別できます。シャーシ名は３０文字までで、英文字で始まり、英文字、英数字、アンダースコアが使用できます。

3.2.1　ホスト名の設定と表示

1. グローバルコンフィグレーションモードに入るため、'configure terminal'コマンドを実行します。
2. ローカル RBridge ID を決定するため、'switch-attributes'コマンドに続けてクエスチョンマーク('?')を入力します。
3. 'switch-attributes'コマンドに続いて RBridge ID を入力します。
4. 'host-name'オペランドに続き、ホスト名を入力します。
5. 'copy running-config file startup-config'コマンドを使って、変更を格納します。
6. 'do show running-config switch-attributes'コマンドに続けて rbridge-id を入力して設定を確認します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# switch-attributes ?
Possible completions:
  <NUMBER:1-239> Specify the rbridge-id 1
switch(config)# switch-attributes 1
switch(config-switch-attributes-1)# host-name lab1_vdx0023
switch(config-switch-attributes-1)# exit
switch(config)# do copy running-config startup-config
switch(config)# do show running-config switch-attributes 1
switch-attributes 1
  chassis-name VDX6720-24
  host-name lab1_vdx0023
```

3.2.2 シャーシ名の設定と表示

1. グローバルコンフィグレーションモードに入るため、'configure terminal'コマンドを実行します。
2. ローカル RBridge ID を決定するため、'switch-attributes'コマンドに続けてクエスチョンマーク('?')を入力します。
3. 'switch-attributes'コマンドに続いて RBridge ID を入力します。
4. 'chassis-name'オペランドに続いて、シャーシ名を入力します。
5. 'copy running-config file startup-config'コマンドを使って、変更を格納します。
6. 'do show running-config startup-config'コマンドに続けて rbridge-id を入力して構成の変更内容を確認します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# switch-attributes ?
Possible completions:
  <NUMBER:1-239> Specify the rbridge-id 1
switch(config)# switch-attributes 1
switch(config-switch-attributes-1# chassis-name lab1_vdx0023
switch(config)# do copy running-config startup-config
switch(config)# do show running-config switch-attributes 1
switch-attributes 1
 chassis-name lab1_vdx0023
 host-name lab1_vdx0023
```

3.2.3 スイッチタイプ

スイッチタイプ属性は、'show chassis'コマンドで表示される一意のデバイスモデル識別子です。下記に出力例を示します。

```
switch# show chassis
Chassis Family: VDX87xx
Chassis Backplane Revision: 1
switchType: 1000
Use table to convert this parameter
(output truncated)
```

3.3 装置の有効化・無効化

デフォルトでは、装置の電源投入、診断、初期化が完了すると、装置は有効化されています。全てのインタフェースはオンラインです。必要に応じて、無効化した後、再度有効化する必要があります。

- 'chassis disable'コマンドは、全てのインタフェースをオフラインにする場合に使います。全てのインタフェースは、オフラインになります。
- 'chassis enable'コマンドは、インタフェースをオンラインに戻すために使用します。POST をパスし

た全てのインタフェースが有効化され、オンラインに戻ります。

NOTE
装置を無効化するとスイッチの動作は中断されます。一部のインタフェースだけを有効・無効にしたい場合は、'shutdown'コマンドを使用してください。このコマンドの詳細は、『Network OS Command Reference』を参照下さい。

3.4 装置のリブート

Network OS はシステムをリブートするために、'reload'と'fastboot'の２つの手段を提供します。

NOTE
リブート動作は両方とも現状状態を初期化し、実行前に確認のためのプロンプトを表示します。ネットワークに接続しているスイッチをリブートすると、スイッチを通過する全ての通信は停止します。スイッチの全てのポートは、スイッチがオンラインになるまでインアクティブ状態となります。

3.4.1 リブート

- 'reload'コマンドは、CPU の”cold reboot”(電源オフとリスタート)と起動時に POST(Power-on self-test)を実行します。
- 'fastboot'コマンドは、起動時の POST を省略し、CPU の"cold reboot"を実行します。POST を省略することでブート時間を短縮することができます。もし、POST が前もって無効化していた場合は、'fastboot'と'reload'は同じ動作となります。

3.4.2 動作モード

Network OS は、スタンドアロンモードおよび Brocade VCS ファブリックモードの 2 つの動作モードをサポートしています。スイッチが起動した時、これらのモードのいずれかになります。デフォルトでは、スタンドアロンモードで起動します。

(1) VCS モード

装置の VCS 設定を表示するには、'show vcs' コマンドを発行します。以下のコマンド出力は、1 の VCS ID と 1 の RBridge ID を持つ単一ノードの VCS を示しています。デフォルト値を変更するには、VCS コマンドを使用します。

```
switch# show vcs
Config Mode    : Local-Only
VCS ID         : 1
Total Number of Nodes          : 2
```

```
Rbridge-Id    WWN                 Management IP    Status         HostName
------------------------------------------------------------------------------
1        10:00:00:05:33:15:DE:CC  10.24.82.120     Online         dutA1-sw0
                                  fd00:60:69bc:64:205:33ff:fe15:decc
```

(2) スタンドアロンモード

デフォルトは、スタンドアロンモードで起動します。この制限されたモードでは、スイッチは、IP スタティック・ルートと In-band 管理を除いて Network OS V2.0.0 で利用できたレガシー機能だけをサポートします。他のすべてのレイヤ 3 機能、または Network OS v3.0.0 で導入された他の機能は、スタンドアロン･モードでは使用できません。

デフォルトモードで VCS 設定を表示すると VCS モードが無効になっていることを示しています。VCS モードを有効にするには'vcs enable'コマンドを使用します。スイッチが再起動され、VCS モードで起動します。

```
switch# show vcs
Config Mode    : Local-Only
```

NOTE

Network OS v3.0.0 を実行しているすべてのスイッチのコンフィギュレーションモードは、スイッチがスタンドアロンモードであるか、または VCS モードであるかどうかにかかわらず、常に "ローカルのみ"になります。show vcs 出力のコンフィギュレーションモードのパラメータは、スイッチに行った設定はローカルであり、自動的にファブリックの他のスイッチに配信されていないことを示しています。

例外については、74 ページの『5.7.2　設定パラメータの自動配布』を参照下さい。

3.5 イーサネット管理インタフェースの構成

イーサネットネットワークインタフェースは、Network OS の CLI への直接アクセスを含む管理用アクセスを可能とします。他の管理用インタフェースでシステムを管理する前に、シリアル接続を使って、少なくとも一つの IP アドレスを設定します。また、静的 IP アドレス設定や自動的に IP アドレスをクライアントに割り当てる DHCP クライアント機能を使うことができます。また、IPv6 アドレスに対しては、スタティック IPv6 をサポートしています。

静的 IP アドレスの設定と DHCP の利用は排他的です。もし、DHCP が有効なら、静的 IP アドレス設定する前に、DHCP クライアント機能を外します。DHCP を無効化するために'no ip address dhcp'コマンドを使います。

NOTE

もしネットワークインタフェースがまだ設定されていない場合、IP アドレスを設定するためにシリアルポートを経由して接続する必要があります。シリアルポートで接続するためには、ユーザーズガイ

ドを参照してください。

3.5.1　静的 IPv4 イーサネットアドレスの構成

DHCP サービスが利用できない環境では、静的イーサネットインタフェースアドレスを使います。静的 IPv4 アドレスまたは IPv6 アドレスを構成するために、まず DHCP を無効化しなければなりません。詳細は、55 ページの『3.5.3 DHCP を使った IP アドレスの設定』を参照下さい。

1．シリアルポート経由でスイッチに接続します。
2. グローバルコンフィグレーションモードに入るため、'configure terminal'コマンドを実行します。
3．管理ポートを定義するために、' interface Management <rbridge-id>/<管理ポート番号>’コマンドを入力します。
   このコマンドを使用すると、IPv4 アドレスと IPv6 アドレスの構成パラメータを選択することができる管理インターフェースコンフィギュレーションモードに入ります。
   ・スイッチは、一つの管理ポートを持っており、管理ポート番号は常に 0 です。
4．DHCP 機能を無効化するために、'no ip address dhcp'コマンドを実行します。
5．’ip address <IPv4>/<prefix_lenght>'コマンドを実行します。
6．’do show running-config interface Management’コマンドで設定を確認します。
7．IPv4 フォーマットのゲートウェイアドレスを設定するため、'ip route 0.0.0.0/0 <IP_address>' コマンドを実行します。
8．’do show running-config ip route’コマンドで設定を確認します。

NOTE

IPv4 アドレス指定のサブネットマスクの指定はサポートしていません。代替として、プレフィックス番号を指定します。ネットワークマスクのプレフィックス番号を入力するために、IP アドレスの直後に、'/'スラッシュとマスクを示すビットを入力します。例えば、24 ビットのネットワークマスクをもつ IP アドレスは、“209.157.22.99/24”を入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# interface Management 1/0
switch(config-Management-1/0)# no ip address dhcp
switch(config-Management-1/0)# ip address 10.24.85.81/20
switch(config-Management-1/0)# do show running-config interface Management
interface Management 1/0
no ip address dhcp
ip address 10.24.85.81/20
ip gateway-address 10.24.80.1
no ipv6 address autoconfig
!
```

```
switch(config-Management-1/0)# exit
switch (config)# ip route 0.0.0.0/0 10.24.80.1
switch (config)# do show running-config ip route
ip route 0.0.0.0/0 10.24.80.1
```

3.5.2 静的 IPv6 イーサネットアドレスの構成

1. グローバルコンフィグレーションモードに入るため、'configure terminal'コマンドを実行します。
2. ' interface Management <rbridge-id>/<管理ポート番号>'コマンドを入力します。
   このコマンドを使用すると、IPv4 アドレスと IPv6 アドレスの構成パラメータを選択することができる管理インターフェースコンフィギュレーションモードに入ります。
   ・スイッチは、一つの管理ポートを持っており、管理ポート番号は常に 0 です。
3. ' ip address <IPv4>/<prefix_lenght>'コマンドを実行します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# interface Management 1/0
switch(config-Management-1/0)# ipv6 address
fd00:60:69bc:832:e61f:13ff:fe67:4b94/64
```

3.5.3 DHCP を使った IP アドレスの設定

NOTE
DHCP は IPv6 アドレスをサポートしません。

デフォルトでは、DHCP は無効になっています。サービスを明示的に有効にする必要があります。IPv4 アドレスの DHCP を有効にするには、'ip address dhcp'コマンドを使用して、IPv6 アドレスの DHCP を有効にするには、'ipv6 address dhcp'コマンドを使用します。Network OS の DHCP クライアントは、次のパラメータをサポートしています。

- 外部のイーサネットポートの IP アドレスとプレフィックス
- デフォルトゲートウェイ IP アドレス

DHCP が有効なスイッチをネットワークに接続し電源を入れた場合、スイッチは自動的にイーサネット IP アドレス、プレフィックス長、デフォルトゲートウェイを DHCP サーバから取得します。DHCP クライアントは同一サブネットにある DHCP サーバにのみ接続可能です。もし、DHCP サーバが同一サブネットにない場合、DHCP は有効化しないで下さい。

次の例では、IPv4 アドレスの DHCP を有効にします。

```
switch(config)# interface Management 1/1
switch(config-Management-1/1)# ip address dhcp
```

'show running-config interface Management'コマンドは、DHCP が有効になっているかどうかを示しま

す。次の例では、IPv4 アドレスの DHCP を有効にしてスイッチを示しています。

```
switch# show running-config interface Management
interface Management 2/0
ip address dhcp
ip address 10.24.73.170/20
ip gateway-address 10.24.64.1
no ipv6 address autoconfig
!
```

NOTE
DHCP が有効になると、静的な IP アドレス設定は削除されます。

3.5.4　ネットワークインタフェースの表示

もし、IP アドレスがネットワークインタフェースに割り当てられてない場合は、シリアルポートのコンソールセッションを使って、Network OS の CLI に接続します。そうでない場合は、telnet か SSH によりスイッチに接続します。'show interface management'コマンドを使って、ネットワークインタフェースを表示します。以下に、例を示します。

```
switch# show interface Management
interface Management 9/0
 ip address 10.24.81.65/20
 ip gateway-address 10.24.80.1
 ipv6 ipv6-address [ ]
 ipv6 ipv6-gateways [ fe80::21b:edff:fe0f:bc00 fe80::21b:edff:fe0c:c200 ]
 line-speed actual "1000baseT, Duplex: Full"
 line-speed configured Auto
```

3.5.5　管理インタフェースの速度の設定

管理インタフェースは、100Mbps/全二重設定されています。本設定のまま変更しないで下さい。

3.6　アウトバンドの telnet／SSH 接続

Secure Shell（SSH）および telnet は、リモートネットワーキングデバイスの管理機能への安全なアクセスを可能にするためのメカニズムです。SSH は telnet と同様の機能を提供しますが、セキュリティを提供しない telnet 接続とは異なり、SSH は、デバイスへの安全な暗号化された接続を提供します。

SSH および telnet のサポートは、特権実行モードで有効であり、IPv4 アドレスと IPv6 アドレスをサポートしています。

3.6.1　telnet 接続の確立

telnet セッションを確立するには、デフォルトの設定を使用できます。

```
switch# telnet 10.17.37.157
Trying 10.17.37.157...
Connected to 10.17.37.157.
Escape character is '^]'.

Network OS (sw0)
sw0 login:
```

telnet はポート 23 で接続されます。'telnet' <ip_address>コマンドのオプショナルポートオペランド（0-65535）を使用して、デフォルトのポートを上書きすることができます。デバイスは、接続が成功すると、そのポートでリッスンする必要があります。

以下の例では、デフォルトポートを上書きします。

```
switch# telnet 10.17.37.157 87
Trying 10.17.37.157...
Connected to 10.17.37.157.
Escape character is '^]'.

Network OS (sw0)
sw0 login:
```

次の機能は、telnet ではサポートしていません。

- telnet セッションの表示
- ハング telnet セッションの終了

3.6.2　SSH サポート機能

SSH は SSHv2 をサポートしています。しかし全て機能ではなく以下機能をサポートしています。

次の暗号アルゴリズムをサポートしています。

- **3des** Triple-DES（デフォルト)
- **aes256-cbc**：256 ビットキーによる CBC モードの AES
- **aes192-cbc**：192 ビットキーによる CBC モードの AES
- **aes128-cbc**：128 ビットキーによる CBC モードの AES

次の HMAC（Hash-based Message Authentication Code）メッセージ認証アルゴリズムをサポートしています。

- **hmac-md5**：128 ビットキーによる MD5 暗号化アルゴリズム（デフォルト）

- **hmac-md5-96**：96 ビットキーによる MD5 暗号化アルゴリズム
- **hmac-sha1**：160 ビットキーによる SHA1 暗号アルゴリズム
- **hmac-sha1-96**：96 ビットキーによる SHA1 暗号アルゴリズム

SSH ユーザー認証は、外部認証、認可、および Accounting(AAA)サーバの装置に保存されたパスワードで行います。
以下の機能は、SSH ではサポートしていません。
- SSH セッション表示
- 古い SSH キーの削除

3.6.3 SSH 接続の確立

特権実行モードでデフォルトのパラメータを使用して SSH 接続を確立するためには、'ssh -l '<username> <ip_address>コマンドを入力します。デフォルトの暗号化およびハッシュアルゴリズムを上書きするには、-m および-c オプションを使用します。
以下の例では、デフォルトの設定を上書きします。

```
switch# ssh -l admin -m hmac-md5 -c aes128-cbc 10.20.51.68
The authenticity of host '10.20.51.68 (10.20.51.68)' can't be established.
RSA key fingerprint is ea:32:38:f7:76:b7:7d:23:dd:a7:25:99:e7:50:87:d0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.20.51.68' (RSA) to the list of known hosts.
admin@10.20.51.68's password:********

WARNING: The default password of 'admin' and 'user' accounts have not been
changed.

Welcome to the Brocade Network Operating System Software
admin connected from 10.20.51.66 using ssh on C60_68F
```

3.7 スイッチバナーの設定

バナーは、スイッチのコンソールに表示されるテキストメッセージです。このメッセージに、スイッチにアクセスする際にユーザーが必要となる情報やスイッチに関する情報を含めることができます。このバナーは、最大 2048 文字まで指定できます。マルチラインバナーを作成するには、'banner login' コマンドに続き、Esc+m のキーを入力します。入力を終了するには、Ctrl+D を入力します。

3.7.1 バナーの設定と表示

1．'configure terminal'を使って、グローバルコンフィグレーションモードに入ります。
2．'banner login'コマンドおよび二重引用符で囲まれた（" "）テキストメッセージを入力します。
3．設定されたバナーを表示するため、'do show running-config banner'コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# banner login “Please do not disturb the setup on this switch”
switch(config)# do show running-config banner
banner login “Please do not disturb the setup on this switch”
```

バナーを削除するには、no banner login コマンドを使用します。

3.8 サポートデータの採取

もし障害が発生した場合は、解析用にデータを採取して、保守員に送付する必要があります。'copy support'コマンドは、重要なシステムデータを採取し外部ホストに転送することが出来ます。

3.8.1 外部ホストへの supportsave データのアップロード

supportsave データをインタラクティブにアップロードするために、'copy support-interactive'コマンドを使用し、必要な情報を入力します。外部ホストの IP アドレスに IPv6 アドレスを指定する場合、Network OS の v3.0.0 以降が必要です。インタラクティブではない方法でアップロードする方法は、『Network OS Command Reference』を参照してください。

```
switch# copy support-interactive
Server Name or IP Address: 10.38.33.131
Protocol (ftp, scp): ftp
User: admin
Password: ********
Directory:/home/admin/support
VCS support [y/n]? (y): n
Module timeout multiplier[Range:1 to 5.Default:1]:
copy support start
Saving support information for chassis:sw0, module:RAS...
(output truncated)
```

3.8.2 supportsave 操作のステータス表示

'show copy-support status'コマンドを入力します。

```
switch# show copy-support status
```

```
Slot Name       SS type        Completion Percentage
#######################################################
M1             NORMAL         [100%]
L1/0           NORMAL         [100%]
L1/1           NORMAL         [100%]
L2/0           NORMAL         [100%]
L2/1           NORMAL         [100%]
L4/0           NORMAL         [100%]
L4/1           NORMAL         [100%]
```

3.8.3 supportsave データの自動アップロード設定

supportSave 情報を収集するために faist-fault data capture(FFDC)とトレースデータファイルを自動的にリモートサーバにアップロードするようにスイッチを設定することができます。
この機能を有効にするには、専用サーバを構成する必要があります。この機能を有効にするには、以下の例に示す'autoupload enable'コマンドを使用します。

```
switch# autoupload enable host 10.31.2.27 user supportadmin directory
/users/support/ffdc_autoupload password *******
Support auto file transfer enabled.
```

3.8.4 自動アップロード設定の表示

'show autoupload'コマンドを使用してスイッチの自動アップロード設定を表示します。

```
switch# show autoupload
Host IP Addr: 10.38.33.131
User name:admin
Remote Dir: /home/admin/support
Auto Upload protocol:   ftp
Auto-FTP:     On
```

3.8.5 追加の supportsave 設定コマンド

追加の supportsave データを設定するために次のコマンドを使用します。

- faist-fault data capture(FFDC)の無効化/有効化をするために'support'コマンドを使用します。FFDC はデフォルトで有効です。FFDC を設定する前に、'rbridge-ID <rbridge-id>'コマンドで RBridge ID サブコンフィギュレーションモードに入ります。
- 'show support'コマンドで、core ファイルのリストを表示します。
- 'clear support'コマンドで、サポートデータを消去します。

これらのコマンドの更に詳細な情報は、『Network OS Command Reference』を参照下さい。

3.9 メッセージロギング

使用可能なメッセージ･ロギングの種類およびセットアップ手順は、『Network OS Message Reference』の″Introduction to Brocade Error Message Logging″に記載されています。

NOTE

監査ログ(auditlog)に表示されるユーザーID が、'admin'と表示される場合があります。

4 ネットワークタイムプロトコル

4.1 日付と時刻の設定

スイッチは、リアルタイムクロック（RTC）を持っており、現在の日付と時刻を維持します。スイッチの動作は日付と時間に依存していませんが、ロギング、エラー検出、およびトラブルシューティングのイベントをログに記録する時に使用されているので、正しく設定する必要があります。

‘clock set’コマンドは、ローカルクロックの日付と時刻を設定します。日付と時刻の有効な値の範囲は、1970 年 1 月 1 日～2038 年 1 月 19 日の間になります。タイムゾーンが設定されていない場合、デフォルトはグリニッジ標準時（GMT）となります。アクティブな NTP サーバがスイッチに設定されている場合は、ローカル時刻の設定を上書きします。

'clock set YYYY-MM-DDTHH:MM:SS'コマンドを実行します。

- YYYY は、年を指定します。年の値の範囲は 1970～2038 です。
- MM は、月を指定します。月の値の範囲は 01～12 です。
- DD は、日を指定します。日の値の範囲は 01～31 です。
- T は固定で‘T’を入力します。
- HH は、時を指定します。時の値の範囲は 00～23 です。
- MM は、分を指定します。分の値の範囲は 00～59 です。
- SS は、秒を指定します。秒の値の範囲は 00～59 です。

以下に日付と時刻の設定および表示の例を示します。

```
switch# clock set 2011-09-17T12:15:00
switch# show clock
rbridge-id 1: 2012-05-04 16:01:51 Etc/GMT+0
```

4.2 タイムゾーンの設定

名前で地域や都市を指定することにより、タイムゾーンを設定することができます。タイムゾーンは、Africa, America, Pacific, Europe, Antarctica, Arctic, Asia, Australia, Atlantic, Indian, また US 州や longitudinal city のリージョンを指定できます。
タイムゾーンの設定は次の特徴があります。

- 自動的に夏時間に補正できます。
- スイッチでタイムゾーンを変更するとローカルタイムゾーン設定の更新と、ローカルタイムへの計算が行われます。
- デフォルトでは、グリニッジ標準時(GMT)のタイムゾーン(0,0)となっています。ファブリック内のすべてのスイッチが一つのタイムゾーンである場合は、デフォルトの設定でタイムゾーンの設定を

保持することが可能です。

- 既に実行中のシステムサービスは、次のリブートまでタイムゾーンの変更は適用されません。
- タイムゾーンの設定は、高可用機能を利用時フェイルオーバーしても引き継がれます。
- タイムゾーン設定は、NTP サーバとの同期には影響を受けません。

4.2.1 タイムゾーン設定

スイッチのタイムゾーンを設定するには、'clock timezone'コマンドを使用します。このコマンドを使用して、タイムゾーンを設定する必要のあるすべてのスイッチを設定する必要があります。タイムゾーンの設定は、不揮発メモリに格納されますので、各スイッチで一度、設定する必要があります。
設定可能な地域や都市の完全なリストについては、360 ページの『32 サポートされているタイムゾーンと地域』を参照してください。

'clock timezone region [/country|/state/] city'コマンドを入力します。

```
switch# clock timezone Asia/Tokyo
```

NOTE

スイッチのファームウェアをアップグレードした後、タイムゾーン情報を再設定する必要がある場合があります。

4.2.2 現在の時刻とタイムゾーンの表示

'show clock'コマンドを使用してローカル日付、時刻およびタイムゾーンを表示します。

NOTE

このコマンドはローカルスイッチ上の現在をサポートします。

'show clock'コマンドを入力します。

```
switch# show clock
rbridge-id 1: 2012-05-04 16:01:51 Asia/Tokyo
```

4.2.3 タイムゾーン設定の削除

'no clock timezone'コマンドを使用してローカルクロックのタイムゾーン設定を削除します。この操作は、ローカルタイムゾーンをデフォルト値（GMT）に戻します。

'no timezone'コマンドを入力します。

```
switch# no clock timezone
```

4.3 Network Time Protocol

Network Time Protocol (NTP)は、ネットワーク内のすべてのスイッチで同一な時間を維持します。NTP コマンドは、ネットワーク内のすべてのローカルクロック間の時刻同期を維持するために、外部のタ

イムサーバの設定をサポートします。
ネットワーク内の時間を最新の状態に維持するため、各スイッチは、少なくともーつの外部 NTP サーバと時刻同期することをお勧めします。外部 NTP サーバはファブリック全体の時刻同期を維持するために、互いに同期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は、不揮発性メモリに現在のクロックサーバの値を維持します。デフォルトでは、この値は、スイッチのローカルクロックサーバになります。

NOTE
Network Time Protocol (NTP) コマンドは、個々のスイッチに設定されている必要があります。ネットワークの時刻同期は、すべてのスイッチで共通の外部タイムサーバを使用されている時にのみ保証されます。

'ntp server'コマンドは、IPv4 または IPv6 形式の 5 つのサーバーアドレスを登録することができます。複数の NTP サーバのアドレスを登録した場合は、リストの最初のサーバをアクティブな NTP サーバとして使用します。もし、到達可能な NTP サーバがない場合は、新しいアクティブな NTP サーバが登録されるまで、ローカルスイッチ時刻をデフォルト時刻として使用します。

4.3.1 外部ソースへのローカル時間の同期

'ntp server'コマンドを使用して、NTP サーバとローカルスイッチの時刻を同期します。
'ntp server'コマンドは 5 つの IP アドレスを登録できます。リスト内の少なくとも 1 つの IP アドレスが到達可能な NTP サーバを設定しなければなりません。
'ntp server <*ip_address*>'コマンドを入力します。

```
switch(config)# ntp server 192.168.10.1
```

4.3.2 アクティブな NTP サーバの表示

'show ntp status'コマンドを使って、現在のアクティブな NTP サーバの IP アドレス、もしくは、LOCL を表示します。LOCL は、NTP サーバが登録されていなかったり、利用可能な NTP サーバが無い場合に、スイッチのローカルタイムが使われることを示しています。

NOTE
引数に'all'を指定すると、ローカルな情報のみを表示します。

'show ntp status'コマンドを入力します。

```
switch# show ntp status
active ntp server is 192.168.10.1
```

4.3.3 NTP サーバ IP アドレスの削除

'no ntp server'コマンドを使用して、サーバ IP アドレスのリストから NTP サーバの IP アドレスを削除します。残りのリスト内に少なくとも 1 つの IP アドレスが到達可能である必要があります。

‘no ntp server’コマンドを入力します。

```
switch(config)# no ntp server 192.168.10.1
switch# show ntp status
rbridge-id 1: active ntp server is LOCL
```

5 構成情報の管理

5.1 スイッチ構成情報の概要

同じファブリック内のスイッチ間で一貫性のある構成設定を維持し、ファブリックの中断を最小限に抑えることは、スイッチ管理で重要な部分です。標準的な構成情報の管理方法として、緊急時に参照できるように全ての重要なコンフィグレーションデータを外部のホストにスイッチごとにバックアップすることを推奨します。
典型的な構成情報の管理方法は下記のとおりです。

- running configuration を startup configuration ファイルへの格納(70 ページの『5.4 コンフィグレーションの変更の格納』参照)
- コンフィグレーションファイルのリモートホストへのアップロード(71 ページの『5.5 コンフィグレーションのバックアップ』参照)
- アーカイブからのコンフィグレーションファイルの回復(72 ページの『5.6 コンフィグレーションの回復』参照)
- すべてのスイッチのコンフィギュレーションファイルをリモートへのアーカイブ(73 ページの『5.7 VCS ファブリックモードでの構成情報管理』参照)
- リモートから複数のスイッチへのコンフィギュレーションファイルのダウンロード 73 ページの『5.7 VCS ファブリックモードでの構成情報管理』参照)

5.2 フラッシュメモリ上のファイル管理

Network OS はスイッチのフラッシュメモリ上に作成されたフィルを削除、名称変更、表示するツールを提供しています。構成情報を含む全てのファイルに'display'コマンドを使うことが出来ます。'rename'と'delete'コマンドは、フラッシュメモリ上に作成したコンフィグレーションファイルのコピーにのみに使えます。システムのコンフィグレーションファイルは、名称変更も削除も出来ません。

5.2.1 フラッシュメモリファイルの一覧表示

フラッシュメモリ上のファイルの一覧表示するために、特権実行モードで'dir'コマンドを使用します。

```
switch# dir
drwxr-xr-x   2 root     sys         4096 Feb 13 00:39 .
drwxr-xr-x   3 root     root        4096 Jan 1   1970 ..
-rwxr-xr-x   1 root     sys          417 Oct 12  2010 defaultconfig.novcs
-rwxr-xr-x   1 root     sys          697 Oct 12  2010 defaultconfig.vcs
-rw-r--r--   1 root     root        6800 Feb 13 00:37 startup-config
```

5.2.2 フラッシュメモリからファイルの削除

フラッシュメモリからファイルを削除するために、特権実行モードで'delete file'コマンドを使用します。

```
switch# delete myconfig
```

5.2.3 ファイル名の変更

フラッシュメモリ上のファイル名称を変更するために、特権実行モードで'rename <source_file> <destination file>'コマンドを使用します。

```
switch#rename myconfig myconfig_20101010
```

5.2.4 フラッシュメモリ上のファイルの内容表示

フラッシュメモリ上のファイルの内容を確認するために、特権実行モードで'show file <file>'コマンドを使用します。

```
switch# show file defaultconfig.novcs
!
no protocol spanning-tree
!
vlan dot1q tag native
!
   cee-map default
   remap fabric-priority priority 0
   remap lossless-priority priority 0
   priority-group-table 1 weight 40 pfc on
   priority-group-table 2 weight 60 pfc off
   priority-group-table 15.0 pfc off
   priority-table 2 2 2 1 2 2 2 15.0
!
interface Vlan 1
shutdown
!
port-profile default
vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
!
protocol lldp
!
end
```

!

NOTE
running configuration の内容を表示するには、'show running-config'コマンドを使用し、startup configuration の内容を表示するには、'show startup-config'コマンドを使用します。

5.3 コンフィグレーションファイルのタイプ

Network OS は、３つのタイプのコンフィグレーションをサポートしています。表 5-1 に標準のコンフィグレーションファイルのタイプと用途を示します。

表 5-1　標準のスイッチコンフィグレーションファイル

ファイルのタイプ	説　明
Default configuration ·defaultconfig.novcs ·defaultconfig.vcs	カスタマイズしたコンフィグレーションが利用できない場合は、デ default configuration が適用されます。 このコンフィグレーションはスタンドアロンと Brocade VCS ファブリックモードは、それぞれ別のコンフィギュレーションファイルになります。
Startup configuration ·startup-config	起動時及びリブート後に有効になるコンフィグです。
Running configuration ·running-config	スイッチで現在使用しているコンフィグです。コンフィグレーションを変更する際は、running configuration に書き込まれます。running configuration は、startup configuration にコピーしなければ、リブート後に引き継がれません。

スイッチを起動直後の running configuration は startup configuration と同じです。スイッチを設定することによって、変更がコンフィグレーション(running configuration)に書き込まれます。変更を格納するために、現在使われているコンフィグレーション(running configuration)を startup configuration に格納します。スイッチをリブートすると、コンフィグレーションの変更は有効になります。

5.3.1 default configuration

Network OS は、スタンドアロンおよび Brocade VCS ファブリックモードのスイッチのために 2 つの異なる default configuration ファイルを提供しています。スタンドアロンからの Brocade VCS ファブリックモードに変更すると、システムはモードに基づいて、適切な default configuration を選択します。default configuration ファイルは、Network OS のファームウェアパッケージの一部であり、自動的に以下の条件下で startup configuration に適用されます。

- Brocade VCS ファブリックモードを有効または無効にした場合、モードに適した default configuration がスイッチをリブート時に適用されます。
- default configuration をリストアするとき。

default configuration の変更、削除および名称の変更はできません。

(1) default configuration の表示

default configuration ファイルを表示するために、特権実行モードで'show file <file>'コマンドを使用します。

```
switch# show file defaultconfig.novcs
switch# show file defaultconfig.vcs
```

5.3.2 startup configuration

startup configuration は不揮発情報で、システムがリブートするときに適用されます。

- 『5.3.1 default configuration』記載の契機で、default configuration を startup configuration として使用します。
- startup configuration は、常に現在の Brocade VCS ファブリック･モードと一致しています。モードを変更するときに、バックアップ･コピーを作成しない限り、startup configuration の内容は削除されます。
- running configuration に対して設定変更を行い、'copy'コマンドを使用して startup configuration に変更を保存すると、running configuration が startup configuration になります。

(1) startup configuration の表示

startup configuration の内容を表示するには、特権実行モードで'show startup-config'コマンドを使用します。

```
switch# show startup-config
```

5.3.3 running configuration

running configuration は、現在スイッチで有効なコンフィグレーションです。スイッチを使用中に行った、あらゆるコンフィグレーションの変更は、running configuration に適用されます。

- running configuration は揮発情報です。
- コンフィグレーションの変更を格納するために、running configuration を startup configuration へ 'copy'コマンドで格納する必要があります。もし、変更が確定ではない場合は、一旦ファイルへコピーして、後に変更を適用してください。

(1) running configuration の表示

running configuration の内容を表示するには、特権実行モードで'show running-config'コマンドを使用してください。

```
switch# show running-config
```

5.4 コンフィグレーションの変更の格納

コンフィグレーションの変更は揮発情報ですので、もし格納してない場合はリブート後に消えてしまいます。変更を格納するには２つの方法があります。

- running configuration を startup configuration へ copy します。変更はリブート時に有効になります。
- running configuration を一般ファイルに copy して、後日そのファイルを startup configuration に適用します。

NOTE

ファームウェアの更新をする前に、running configuration をいつもバックアップコピーしてください。

NOTE

コンフィグレーションを変更した場合、startup configuration へ copy した後、製品運用に入る前に一旦 reload を実行してください。

なお、下記のいずれかの機能/設定を使われる場合は必ず reload を実行してください。

・アクセスコントロールリスト(ACL)

・エッジループ検出機能(ELD)

・リンクアグリゲーション

5.4.1 running configuration の格納

変更を加えたコンフィグレーションを格納するために、running configuration を startup configuration に copy します。次回のスイッチのリブートで、startup configuration が使われ、変更が有効となります。

特権実行モードで'copy running-config startup-config'コマンドを使用してください。

```
switch# copy running-config startup-config
copy running-config startup-config
This operation will modify your startup configuration. Do you want to continue?
[Y/N]: y
```

5.4.2 running configuration の一般ファイルへの格納

もし、コンフィグレーションの変更を格納したいが、スイッチのリブート時に適用したくない場合は、running configuration を一般ファイルへ格納します。後日、その変更を適用できることになります。

1．特権実行モードで'copy running-config <file>'コマンドを入力します。ファイル名は URL として指定します。

```
switch# copy running-config flash://myconfig
```

2．ディレクトリの内容を表示して、作業内容を確認します。

```
switch# dir
total 32
drwxr-xr-x    2 root    sys      4096 Feb 17 17:50 .
drwxr-xr-x    3 root    root     4096 Jan  1  1970 ..
-rwxr-xr-x    1 root    sys       417 Oct 12  2010 defaultconfig.novcs
-rwxr-xr-x    1 root    sys       697 Oct 12  2010 defaultconfig.vcs
-rw-r--r--    1 root    root     6777 Feb 17 17:50 myconfig
-rw-r--r--    1 root    root     6800 Feb 13 00:37 startup-config
```

5.4.3　以前に格納したコンフィグレーション変更の適用

以前にファイルに格納したコンフィグレーションの変更を適用したい場合、そのファイル(下記の例では'myconfig'となっている)を、startup configuration に copy します。スイッチのリブート後、変更が有効になります。

特権実行モードで'copy <file> startup-config'コマンドを入力します。ファイル名は URL として指定します。

```
switch# copy flash//:myconfig startup-config
This operation will modify your startup configuration. Do you want to continue?
[Y/N]: y
```

5.5 コンフィグレーションのバックアップ

コンフィグレーションを紛失したり、意図しない変更をした場合に回復できるよう、いつもコンフィグレーションファイルのバックアップコピーをとっておいてください。次の推奨手順を示します。

- ファブリック内のすべてのスイッチの startup configuration のバックアップコピーを採取する。
- 外部のホストにバックアップコピーをアップロードする。
- 一つのスイッチから別のコンフィギュレーションファイルをコピーすることは避けてください。代わりにバックアップコピーからスイッチのコンフィギュレーションファイルを復元します。

NOTE

コンフィグレーションファイルのサイズによっては、バックアップコピーまたは外部ホストへのアップロードに５分程度かかることがあります。

5.5.1　startup configuration の外部ホストへのアップロード

特権実行モードで'copy startup-config <destination_file>'コマンドを使用します。
次のサンプルでは、FTP を使ってリモートサーバのファイルに startup configuration をコピーしています。

```
switch# copy startup-config
ftp://admin:******@122.34.98.133/archive/startup-config_vdx24-08_20101010
```

5.6 コンフィグレーションの回復

コンフィグレーションの回復は、外部ホストからアーカイブされたバックアップコピーをダウンロードすることでスイッチ上のコンフィグレーションファイルを上書きすることで行います。典型的な方法として次の２つがあります。

- 72 ページ記載の『5.6.1 以前の startup configuration の回復』
- 73 ページ記載の『5.6.2 default configuration の回復』

NOTE

Network OS 2.x を使用して作成されたコンフィギュレーションファイルは、Network OS 3.x を実行しているシステムにロードしてはいけません。ACL（Access Control List）および VLAN コンフィギュレーション情報は、Brocade Network OS 3.x で変更されました。また、Brocade Network OS 2.x のコンフィギュレーションファイルをロードするときに、コンフィギュレーションの影響を受ける行はスキップされます。

5.6.1　以前の startup configuration の回復

スイッチを Brocade VCS ファブリックモードからスタンドアロンモードに戻してオリジナルのスタンドアロンの startup configuration を再適用する場合の方法です。

1．VCS ファブリックモードをディセーブルにしてスイッチを再起動します。
VCS ファブリックモードに関連付けられているスタートアップコンフィギュレーションは自動的に削除されます。スイッチスタンドアロンモードで起動すると、対応するデフォルトコンフィグレーションをロードします。
2．FTP サーバから以前アーカイブした startup configuration ファイルを running configuration にコピーします。
3．スイッチの running configuration を startup configuration にコピーします。

```
switch# no vcs enable

The switch automatically reboots at this point.

switch# copy ftp://admin:******@122.34.98.133//archive/¥
startup-config_vdx24-08_20101010 running-config
switch# copy running-config startup-config
```

ATTENTION
ダウンロードするコンフィグファイルが対象のスイッチのものかよく確認してください。スイッチ名と日付によってアーカイブファイルを区別する方法を推奨します。

5.6.2 default configuration の回復

この回復手順は、ファームウェアのデフォルト状態に回復する場合に使用します。VCS ファブリックおよびスタンドアロンモードの初期値を格納したファイルは、スイッチ上で常に存在していて、'copy' コマンドを使用して簡単に回復することが出来ます。
ファームウェアのデフォルト状態に回復するには、特権実行モードで以下の手順を実行します。

1．startup configuration を default configuration で上書きするため 'copy <source_file> <destination_file>'コマンドを使います。

```
switch# copy flash://default-config.novcs startup-config
This operation will modify your startup configuration. Do you want to
continue? [Y/N]: y
```

2．スイッチをリブートします。

```
switch# reload
```

スイッチがスタンドアロンモードまたは VCS ファブリックの一部であるかどうかに応じてコンフィグレーションの回復操作は異なります。
スタンドアロンモードでは、すべてのインタフェースがシャットダウンされます。スイッチが再起動後、回復したデフォルト設定が使用されます。次のパラメータは、このコマンドの影響を受けません。

- インタフェース管理 IP アドレス
- スイッチにインストールされているソフトウェア機能ライセンス

VCS ファブリックモードでは、すべてのインタフェースがオンラインのままです。次のパラメータは、このコマンドの影響を受けません。

- インタフェース管理 IP アドレス
- スイッチにインストールされているソフトウェア機能ライセンス
- 仮想 IP アドレス

5.7 VCS ファブリックモードでの構成情報管理

いくつかのパラメータを除いて、VCS ファブリック内の単一のスイッチに加えた設定変更は、自動的に配布されていません。複数のスイッチ上のイーサネットファブリックのパラメータとソフトウェア機能を設定するときは、個別に各スイッチを設定する必要があります。多数のスイッチ上のイーサネットパラメータとソフトウェア機能が設定されている場合、一つのスイッチから構成情報をアップロードし、ファブリック内のその他のスイッチにダウンロードすることができます。

NOTE
構成ファイルを共有できるスイッチは、同じモデル、同じバージョンのファームウェアでなければなりません。

5.7.1　多数のスイッチへの構成情報のダウンロード

1．一つのスイッチを設定します。
2．70 ページの『5.4.1 running configuration の格納』に記載されている通り、running configuration を startup configuration へコピーします。
3．コンフィグレーションを外部のホスト(72 ページの『5.5.1 startup configuration の外部ホストへのアップロード』)にアップロードします。
4．それぞれの対象スイッチに構成情報をダウンロードします。詳細な情報は、72 ページの『5.6 コンフィグレーションの回復』を参照下さい。

5.7.2　設定パラメータの自動配布

VCS ファブリックの一部である１つの RBridge において、以下のパラメータを設定した時に、それらが自動的に VCS ファブリック内のすべてのスイッチに配信されます。

- 仮想 IP アドレス

'show running configuration'コマンドでは、VCS ファブリック内のすべての RBridge で同じ設定に表示されます。多数の RBridge からコピー操作では、すべてのファブリック全体の構成パラメータが含まれています。

6 ファームウェアのインストールと管理

6.1 ファームウェアアップグレードの概要

ファームウェアのアップグレードは、.plist ファイルにリストされている複数のファームウェアパッケージから構成されます。.plist ファイルには、特定のファームウェア情報（タイムスタンプ、プラットフォームコード、バージョンなど）およびダウンロードされるファームウェアパッケージの名前が含まれています。これらのパッケージは、機能追加やファームウェアの不具合を是正するために定期的に利用できるようになります。
Network OS3.0.0 以降では、ファームウェアのアップグレードは段階的に行われます。'firmware download'コマンドは、現在のインストールやダウンロードしているパッケージと新しいファームウェアパッケージで新機能が含んでいるか、または変更されたかを比較します。
ファイル転送プロトコル（FTP）またはセキュアコピープロトコル（SCP）を使用して、リモートサーバからファームウェアをダウンロードすることができます。
Network OS は、スイッチにファームウェアをダウンロードするためのコマンドラインインターフェース（CLI）を提供します。ファームウェアのダウンロードプロセスが予期しない再起動によって中断された場合、Network OS が以前にインストールされたファームウェアを回復する試みを行います。別のファームウェアのダウンロードを開始する前に回復処理を完了するまで待つ必要があります。

ATTENTION
Network OS をインストールすると、サービスが中断され、保存されていない running configuration は、インストール中に失われます。

6.1.1 ファームウェアのアップグレード

スイッチは、2 つのファームウェアイメージを格納するために、不揮発性記憶領域の 2 つのパーティション（プライマリとセカンダリ）を維持します。以下にスイッチ上の'firmware download'コマンド（オプションなし）を入力した後、デフォルトの動作を説明します。

1．Network OS は、セカンダリパーティションにファームウェアをダウンロードします。
2．スイッチはパーティションを交換して、再起動を実行します。システムが立ち上がった後は、以前のセカンダリパーティションがプライマリパーティションになります。
3．システムは、プライマリからセカンダリパーティションにファームウェアをコピーして、新しいファームウェアをコミットします。

アップグレードプロセスは、ファームウェアを最初にダウンロードして、それからコミットします。
アップグレードの進行状況を監視するには、'show firmwaredownloadstatus'コマンドを使用します。

6.2 アップグレードの準備

ファームウェアのアップグレードの準備のために、この章に記載されている作業を実行してください。

失敗やタイムアウトのような好ましくない状況になった場合、ファームウェアアップグレードのトラブルシュートに必要な情報を保守員に連絡してください。

1．現在のファームウェアバージョンを確認します。76 ページの『6.2.1 スイッチのファームウェアバージョンを取得する』を参照下さい。
2．ファームウェアのアップグレードの前に、スイッチのコンフィグレーションをバックアップしてください。71 ページの『5.5 コンフィグレーションのバックアップ』を参照下さい。
3．補助的にシリアルコンソールを使用してください。シリアルコンソールはトラブル時のログなどを出力するなど保証されます。
4．アップグレードで発生した全ての core ファイルを採取するため'copy support'コマンドを実行してください。この情報は、障害発生時にファームウェアアップグレードプロセスのトラブルシュートに役立ちます。
5．補助的に、全ての既出のメッセージを消去するため'clear logging raslog’コマンドをご使用下さい。

ATTENTION

Network OS 3.0.0 リリースでは、'firmware download'コマンドは、ローカルスイッチでのみサポートされています。ファブリック内のすべてのスイッチをアップグレードするには、79 ページの『6.5 VCS ファブリックモードでのファームウェアアップグレード』を参照下さい。

6.2.1 スイッチのファームウェアバージョンを取得する

次の情報を得るために'show version'コマンドを使用します。

- Network Operating System Version - ファームウェアのバージョン番号
- Build Time - ファームウェアが作成された日付と時間
- Firmware name - ファームウェアイメージの名称
- Control Processor - スイッチ内プロセッサのモデルとメモリ

6.3 リモートサーバからのファームウェアのアップグレード

通常の環境では、デフォルトオプションで'firmware download'コマンドを使うことを推薦します。もし、アップグレードを適用する前に、アップグレードを評価する必要がない場合は、autocommit モードを無効化しないで下さい。autocommit モードの変更に関して詳細は、77 ページの『6.4 ファームウェアアップグレードの検証』を参照下さい。

CAUTION

アップグレード処理を中断しないで下さい。もし、問題が発生した場合は、'firmware download'コマンドを再度実行する前に、タイムアウト(ネットワークの問題の場合は 30 分)を待ってください。例えばスイッチの電源を落とすなどしてアップグレードを中断すると、スイッチが動作不能となり、保守員コールとなります。

複数のスイッチをアップグレードする時は、次のスイッチをアップグレードする前に各スイッチで次の手順を完了させてください。

1．FTP または SSH サーバがリモートサーバで動作しており、有効なユーザーID とパスワード情報を取得していることを確認してください。
2．FTP または SSH サーバへファームウェアパッケージを格納してください。
3．ファームウェアパッケージのアーカイブを解凍します。
4．現在のファームウェアバージョンを確認するため'show version'コマンドを使ってください。
5．ファームウェアを対話的にアップグレードするために'firmware download interactive'コマンドを使います。
6．"Do you want to continue (Y/N) [Y]:"プロンプトに対して"y"を入力します。
7．アップグレードプロセスの間、状況をモニタするため別の CLI セッションにて'show firmwaredownloadstatus'を使用します。
8．スイッチがリブートした後、アップグレードを確認するために’show version'コマンドを使用します。

```
switch# firmware download interactive
Server name or IP address: 10.31.2.25
File name: /users/home40/Builds/NOS_v3.0.0
Protocol (ftp, scp): ftp
User: admin
Password: **********
Do manual download [y/n]: n

System sanity check passed.

Do you want to continue? [y/n]:y
```

6.4 ファームウェアアップグレードの検証

片方のパーティションのみにファームウェアをダウンロードすることにより、新しい（または古い）バージョンをダウンロードして検証した後に以前のバージョンのファームウェアを復元することができます。以前のバージョンは、セカンダリパーティションに保存され、'firmware restore'コマンドで復元することができます。
ファームウェアの復元を有効にするには、nocommit オプションを使用して'firmware download'コマンドを実行します。このオプションは、'firmware download'コマンドが両方のパーティションへファームウェアをコピーすることを抑止します。

ATTENTION
ファームウェアのアップグレードを評価した場合、オリジナルバージョンに回復する前にアップグレードしたファームウェアによってのみサポートされている全ての機能が無効となっているかを確認し

てください。

6.4.1　単一パーティションへのファームウェアダウンロード

1．FTP または SSH サーバがリモートサーバで動作しており、有効なユーザーID があることを確認してください。
2．FTP または SSH サーバへファームウェアパッケージを格納してください。
3．ファームウェアパッケージのアーカイブを解凍します。
4．'show version'コマンドを使用して現在のファームウェアバージョンを確認します。
5．ファームウェアを対話的にアップグレードするために'firmware download interactive'コマンドを使います。
6．“Do Auto-Commit after Reboot [y/n]:”プロンプトに対して"n"を入力します。

```
switch# firmware download interactive
Server name or IP address: 10.31.2.25
File name: /users/home40/Builds/hydra_plat_dev01
Protocol (ftp, scp): ftp
User: admin
Password: **********
Do manual download [y/n]: y
Reboot system after download? [y/n]:y
Do Auto-Commit after Reboot? [y/n]:n

System sanity check passed.

You are running firmware download on dual MM system with 'manual' option. This
will upgrade the firmware only on the local MM.

This command will cause a cold/disruptive reboot and will require that
existing telnet, secure telnet or SSH sessions be restarted.

Do you want to continue? [y/n]:y
(output truncated)
```

スイッチがリブートして新しいファームウェアで立ち上がってきます。スイッチとのセッションは自動的に切れます。

7. スイッチのプライマリパーティションが新しいファームウェアとなっているかを確認するため、'show version all-partitions'コマンドを入力します。新しいバージョンのファームウェアを評価する準備が出来ています。

ATTENTION
もし、ファームウェアを回復したい場合、ここでバージョンアップ手順を中止し、79 ページの『6.4.3 以前のファームウェアバージョンへの回復』に進んでください。そうでなければ、アップグレードプロセスを完了させるため 79 ページの『6.4.2 ファームウェアアップグレードのコミット』に進んでください。

6.4.2 ファームウェアアップグレードのコミット

もし、ファームウェアのアップグレードを続けるならば、セカンダリパーティションを新しいファームウェアでアップデートするために、'firmware commit'コマンドを使用します。コミットが完了するまで数分かかります。

1．特権実行モードで'firmware commit'コマンドを入力します。

```
switch# firmware commit
Validating primary partition...
Doing firmwarecommit now.
Please wait ...
Replicating kernel image
.............
FirmwareCommit completes successfully.
```

2．'show version'コマンドを all-partitions オプション指定で実行します。スイッチ上の両パーティションが新しいファームウェアとなっています。

6.4.3 以前のファームウェアバージョンへの回復

ファームウェアアップグレードを中断して元に戻すために、'firmware restore'を使います。このオプションは、ファームウェアのアップグレードの間 autocommit モードが無効の場合に使用できます。

1．'firmware restore'コマンドを実行します。
ファームウェアのコミット操作は、セカンダリパーティションからプライマリパーティションへオリジナルのファームウェアをコピーすることから始まります。このプロセスが完了すると、両方のパーティションはオリジナルファームウェアになります。この操作が完了するまで数分かかります。

2．全てのプロセスが完了してスイッチが起動して操作可能になるまで待ちます。

3．'show version all partitions'コマンドを入力して、両方のパーティションがオリジナルのファームウェアであることを確認します。

6.5 VCS ファブリックモードでのファームウェアアップグレード

'firmware download'コマンドは、ローカルスイッチのアップグレードにのみサポートされています。VCS のファブリック内のすべてのスイッチをアップグレードするには、別途、各スイッチ上の'firmware download'を実行する必要があります。ファブリック内の各スイッチは、別のスイッチのファームウェ

アダウンロードを開始する前に、現在のスイッチのファームウェアダウンロードを完了します。このプロセスでは、トラフィックの混雑を最小限に抑えることができます。
'show firmwaredownloadstatus'コマンドを入力して、ダウンロード処理が完了したことを確認し、次のスイッチに移ります。

6.6 エラー処理

アップグレードされている間に'firmware download'コマンドが失敗した場合、プロセスが中止され、すべてのモジュールとパーティションは以前のファームウェアに修復されます。

7 ライセンスの管理

Brocade Network Operating System (Network OS)は、ライセンスキーにより有効化されるオプション機能とスタンドアロン及び VCS™をサポートしています。追加ライセンスを購入することで、それらの機能が使用できます。ライセンスは、スイッチソフトウェアに含まれていたり、個別に購入することができます。表 7-1 に各機能に必要なライセンスの一覧を示します。

表 7-1　Network OS のオプション機能のライセンス一覧

ライセンス	説明
VCS_FABRIC	• Brocade VCS ファブリックライセンスは、内蔵 DCB スイッチで２４ノードまでの VCS ファブリックを構成することが出来ます。ファブリック内に３ノード以上ある場合、各ノードに VCS ファブリックライセンスをインストールする必要があります。 • もし、VCS ファブリックが２ノード以内ならば、VCS ファブリックライセンスは必要ありません。 • Brocade VCS ファブリックライセンス持つスイッチがライセンス持っていないスイッチに接続することはできません。2 ノードの VCS では、両方のスイッチが VCS ライセンス持つ、あるいは両方のスイッチが VCS ライセンスを持っていない状態でなければなりません。
FCOE_BASE	• Fibre Channel over Ethernet 機能を有効にするために、Brocade FCoE ライセンスが必要です。単一のスイッチ上で、このライセンスを使用することができますが、FCoE 機能は、そのノードだけに制限されます。マルチホップ FCoE トラフィックをサポートするためには、VCS ファブリックモードを有効にして、各ノードで Brocade FCoE のライセンスをインストールする必要があります。また、2 ノードを超過する VCS ファブリックの場合、FCoE トラフィックがファブリック内のすべてのノードを横断できるように、FCoE のライセンスに加えて、VCS ファブリックライセンスが必要です。 • FCoE ライセンスがない時、FCoE のログインが許可されません。また、FCoE トラフィックも、スイッチを通過しません。FCoE のコマンドが実行された時は、"No FCoE license present"のエラーを表示します。

7.1 ライセンスの管理

管理タスクと関連するコマンドは、永続ライセンスと一時ライセンスの両方に適用されます。

NOTE

Network OS v3.0.0 のライセンス管理は、ローカル RBridge でサポートされています。ファブリック内のリモートノード上のライセンスを設定または表示することができません。

7.1.1 スイッチライセンスＩＤの表示

スイッチライセンスＩＤは、スイッチでどのライセンスが有効かを特定します。ライセンスキーを有効化する際、スイッチライセンスＩＤが必要です。

スイッチライセンスＩＤを表示するため、特権実行モードで'show license id'コマンドを入力します。

```
switch# show license id
Rbridge-Id            License ID
========================================
2             10:00:00:05:33:54:C6:3E
```

7.1.2 ライセンスキーの取得

ライセンスアップグレードオーダーは、トランザクションキーや Brocade software portal へのリンクを含んだメールにより提供されます。デバイスを指定したライセンスファイルは、software portal でスイッチライセンスＩＤと共にトランザクションキーを入力すると生成されます。スイッチライセンスＩＤを保持するために、'show license id'コマンドをご使用下さい。

ライセンスインストールガイドやメールに書かれた手順に従ってライセンスをインストールしてください。ライセンスキーは、大文字小文字を区別します。エラーを避けるために、ライセンスをインストールする場合は、トランザクションキーをコピー＆ペーストしてください。

インストール手順にそって XML ファイルに含まれたライセンスキーをメールで受け取ることが出来ます。

NOTE

将来参照する場合に備えて、ライセンスキーは安全な場所に保管下さい。'show license'コマンドはライセンスキーを表示しません。

7.1.3 ライセンスのインストール

ライセンスをインストールする際、機能によっては、スイッチのリブートが必要となります。

ライセンスをインストールするために、次手順を実行してください。

1．ライセンスキーを連絡しているメールを開いて、XML ファイルからライセンスキーを取り出してください。ライセンスキーは、<licKey>タグから</licKey>タグの間に記述されています。スペースや英数字以外の文字も含めて、文字列全体をコピーしてください。
2．'license add licstr'コマンドに続いて、ライセンスキーを入力します。もしライセンスキーがスペースを含んでいる場合、ダブルクォーテーション(")で囲んでください。
3．'show license'コマンドを入力して、追加したライセンスを確認してください。コマンドをスイッチにインストールされている全てのライセンスをリストします。何もリストされない場合は、'license add licstr'コマンドをもう一度入力してください。

ライセンスの種類によってスイッチをリロードするか、シャーシまたは特定のポートを無効にし、再度有効にするよう求められることがあります。表 7-2 にライセンスインストール後に機能を完全に機能させるための最小限の手順を示します。コマンド出力に沿って適切な作業を行ってください。

表 7-2　ライセンスのインストール後にアクティブにするための要件

ライセンス	説明
VCS_FABRIC	次のいずれかのアクションは、構成に応じて必要となる場合があります。 • ポートまたはシャーシを有効にする。 • ポートまたはシャーシを無効にしてから再有効化。

(1) Brocade VCS ファブリックライセンスの追加

次の例は、VCS ファブリックライセンスを追加して、結果を確認しています。ライセンスは、コマンドが実行された後直ちに有効になります。その他の作業は必要ありません。

```
switch# license add licstr "*B
r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANF
av5W:gWx3hH2:9RsMv3BHfeCRFM2gj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#"

Adding license [*B r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANF
av5W:gWx3hH2:9RsMv3BHfeCRFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#
]
switch# show license
Rbridge-Id: 2
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
   VCS Fabric license
   Feature name:VCS_FABRIC
```

7.1.4　ライセンスの表示

インストールされているライセンスを表示するために'show license'コマンドを使用します。

```
switch# show license
```

```
Rbridge-Id: 2
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
   VCS Fabric license
   Feature name:VCS_FABRIC
```

7.1.5 ライセンスの削除

ライセンスを削除する場合、ライセンスの種類に応じて、ライセンス依存の設定をクリアするか、スイッチをリロードするか、またはシャーシまたは特定のポートをディセーブルにして再度有効するよう求められることがあります。表 7-3 にライセンスの削除後に機能を完全にするための最小限の手順を示します。コマンド出力に沿って適切な作業を行ってください。

表 7-3　ライセンスの削除後に非アクティブにするための要件

ライセンス	説明
VCS_FABRIC	ライセンスを削除する前に、シャーシを無効にすることが必要です。

いくつかのライセンスが必要な機能は、その機能のライセンスを削除する前に、機能に関連するすべてのコンフィギュレーションをクリアする必要があります。いくつかの機能を使うには、スイッチを再起動するか、ポートまたはスイッチ全体を無効し、再度有効にすることが必要な場合があります。

ライセンスを削除するために、次の手順を実行してください。

1．有効なライセンスを表示するために、'show license'コマンドを入力します。
2．'license remove'コマンドに引き続いて、ライセンスキーと機能名称を入力します。ライセンスキーは、大文字小文字を区別します。表示されたとおり正確に入力してください。もし、ライセンスキーがスペースを含む場合は、ダブルクォーテーション(")で囲む必要があります。
3．コマンド表示に従って、適切な作業を行ってください。ライセンスタイプによっては、スイッチのリブートが促されます。
4．ライセンスが削除されたか確認するために、'show license'コマンドを入力してください。ライセンスキーが何も内場合、"No licenses"と表示されます。

NOTE

licenseString オペランドに指定して'license remove'コマンドを使用するために、オリジナルのライセンス文字列を覚えておく必要があります。'show license'コマンドでは、ライセンスキーは表示されません。

次の例では、VCS ライセンスの表示および削除を示しています。

```
switch# show license
Rbridge-Id: 2
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

```
   VCS Fabric license
   Feature name:VCS_FABRIC

switch# license remove " VCS_FABRIC "

License Removed [VCS_FABRIC]

For license to take effect, enable the switch and any disabled ports...
```

8 SNMP 管理

8.1 SNMP の概要

Simple Network Management Protocol (SNMP)は、ネットワークデバイスを監視および管理するための標準的な方法です。スイッチは、SNMP エージェントと管理情報ベース（MIB）を運びます。SNMP は、複雑なネットワークを管理するためのプロトコルのセットです。SNMP は、ネットワークのさまざまな部分にプロトコルデータユニット（PDU）と呼ばれるメッセージを送ります。SNMP 準拠のデバイスはエージェントと呼ばれ、エージェント自身に関するデータを管理情報ベース（MIB）に格納し、SNMP 要求に応えてこのデータを返します。
スイッチにパケットが到着すると、ACL、VLAN、または特定の IP アドレスを使用して SNMP のアクセス権を制限することにより、防御の第一レベルを構成します。次のレベルは、SNMP バージョン 1 および 2c にコミュニティを使用します。
Brocade MIB ファイルの命名規則、ロード命令、および Brocade SNMP エージェントを使用する方法についての詳細は、『Network OS Message Reference』を参照してください。
SNMPv3 のコマンドの詳細については、『Network OS Command Reference』を参照してください。
サポートトラップの詳細については、『Network OS MIB Reference』を参照してください。

8.2 SNMP コミュニティ設定

SNMP version 1 / 2c は SNMP アクセス制限のためにコミュニティを使います。デフォルトでは、ユーザー向けに３種の read-write コミュニティと３種の read-only コミュニティの、６つのコミュニティが設定されています。

NOTE
システムが立ち上がってきた時は、６つのデフォルトコミュニティの一つを指定することが出来ます。

次のコミュニティは、read-write 権限です。

- "Secret Code"
- "OrigEquipMfr"
- "private"

次のコミュニティは、read-only です。

- "public"
- "common"
- "ConvergedNetwork"

8.2.1　SNMP コミュニティの追加

'snmp-server community'コマンドは、コミュニティ文字列と、これらコミュニティの read-write または read-only アクセス権限を設定します。スイッチに SNMP エージェントの設定を行う場合は、このコマンドをご使用下さい。SNMPv1 と SNMPv2c 共通です。グローバルコンフィグレーションモードで、'SNMP server'コマンドを実行します。

1．'configure terminal'コマンドを実行します。

2．'snmp-server community string [ro|rw]'コマンドを実行します。下記は例です。

```
switch(config)# snmp-server community private rw
```

- string は、コミュニティ名を 2 から 16 文字で指定します。
- ro もしくは rw は、コミュニティが read-only (ro) か read-write (rw)かを示します。

上記の例では、read-write 属性を持ったコミュニティ"private"を追加します。

8.2.2　read-only コミュニティのアクセス権の変更

次の例は、コミュニティ"user123"の属性を、read-only から read-write へ変更します。

1．'configure terminal'コマンドを入力します。

2．'snmp-server community user123 rw'コマンドを入力します。

```
switch(config)# snmp-server community user123 rw
```

8.2.3　SNMP コミュニティの削除

次の例は、コミュニティ"public"を削除します。

1．'configure terminal'コマンドを入力します。

2．' no snmp-server community string [ro | rw]'を入力します。以下は例です。

```
switch(config)# no snmp-server community private
```

8.2.4　SNMP コミュニティの表示

設定されているコミュニティ名を表示するために、' show running-config snmp-server'コマンドを入力します。

```
switch# show running-config snmp-server
```

8.3　SNMP サーバ

'snmp-server host'コマンドは、SNMP version 1 / 2c の Trap の送信先 IP アドレス、SNMP バージョン、コミュニティと SNMP サーバのポートを設定します。

コミュニティに関連する SNMP トラップホストを設定するため、ホストを設定する前に、' snmp-server community'コマンドを使って、コミュニティを作成します。

エージェントは、６つのコミュニティとコミュニティに関連づけられた trap recipient と trap recipient の重要度をサポートしています。各コミュニティのトラップ受信のデフォルト値は 0.0.0.0 です。コミ

ュニティ名の長さは、2 から 16 文字です。各コミュニティデフォルト値は、以下の通りです。

- common—read-only
- public—read-only
- ConvergedNetwork—read-only
- OrigEquipMfr—read-write
- private—read-write
- Secret C0de—read-write

NOTE

read-only や read-write グループのひとつの SNMPv1 または SNPMv2c のコミュニティを新たに追加する場合は、上記にあげた６つのうち、いずれかを削除する必要があります。

8.3.1　SNMP サーバホストの設定

グローバルコンフィグレーションモードで、'SNMP server'コマンドを使います。

１．'configure terminal'コマンドを入力します。

２．' snmp-server host ipv4_host | ipv6_host | dns_host community-string [version{1|2c}] [udp-port port] [severity-level {none | debug | info | warning | error | critical}]'を入力します。

- ・ipv4_host | ipv6_host | dns_host は、ホストの IP アドレスを指定します。
- ・community-string は、コミュニティストリングを設定します。
- ・version オプションは、SNMPv1、または SNMPv2c の設定パラメータを選択します。このパラメータは、コミュニティストリングが含まれています。デフォルトの SNMP バージョンは 1 です。
- ・udp-port オプションは、SNMP トラップを受信する UDP ポートを指定します。デフォルトのポートは 162 で、ポートの許容範囲は、0 から 65535 までです。
- ・severity-level オプションは、host と v3host 両方のセキュリティレベルに基づいてトラップをフィルタリングする機能を提供します。RASlog(swEvent)トラップのみ、セキュリティレベルに基づいてフィルタリングすることができます。セキュリティレベルなしが指定されている場合は、すべてのトラップがフィルタリングされず、RASlog トラップが受信されません。クリティカルのセキュリティレベルが指定された場合、トラップはフィルタリングされず、ホストにすべてのトラップが受信されます。
- severity-level オプションは None、Debug、Info、Warning、Error、Critical を指定します。
  次の例は、read-only ユーザーとして、コミュニティ：commaccess を設定し、SNMP version 2c の trap recipient として 10.32.147.6 / ターゲットポート 162 を設定します。

```
switch(config)# snmp-server host 10.32.147.6 commaccess version 2c udp-port
162 severity warning
```

8.3.2　SNMP サーバホストの削除

'no snmp-server host host community-string string version 2c'コマンドは、バージョン 2c からバージョン 1 まで続けて使用でき、'no snmp-server host host community-string string'コマンドは完全にスイッチの設定から SNMP サーバホストを削除します。

8.3.3　SNMP サーバの連絡先の設定

SNMP サーバの連絡先情報を設定するには、'snmp-server contact'コマンドを使用します。デフォルトの連絡先は、 "Field Support"が設定されています。

1．'configure terminal'コマンドを入力します。

2．'snmp-server contact string'を入力します。

次の例は、デフォルトの連絡先を"Operator 12345"に設定します。テキストにスペースを含む場合は、ダブルクォーテーションで囲みます。

```
switch(config)# snmp-server contact "Operator 12345"
```

8.3.4　SNMP サーバの連絡先の削除

スイッチの設定から SNMP サーバの連絡先を削除するには、'no snmp-server contact string'コマンドを使用します。

8.3.5　SNMP サーバロケーションの設定

SNMP サーバのロケーション文字列を設定するには、'snmp-server location'コマンドを使用します。デフォルトの SNMP サーバのロケーション文字列は、 "End User Premise"です。

1．'configure terminal'コマンドを入力します。

2．'snmp-server location string'コマンドを入力します。次の例は、デフォルト値を "Building 3 Room 214"に変更するものです。テキストにスペースを含む場合は、ダブルクォーテーションで囲む必要があります。

```
switch(config)# snmp-server location "Building 3 Room 214"
```

8.3.6　SNMP 設定情報の表示

現在の SNMP ホスト情報、コミュニティ、連絡先、およびロケーションなどの SNMP 設定を表示するには、'show running-config snmp-server'コマンドを使用します。このコマンドには、デフォルト設定はありません。このコマンドは、特権実行モードでのみ実行できます。

'show running-config snmp-server'コマンドを入力します。

```
switch# show running-config snmp-server
```

9 ファブリック管理

9.1 TRILL

Brocade VCS イーサネットファブリックは、分散インテリジェンスを実現するために、お互いに情報を交換するスイッチのグループとして定義されます。Brocade イーサネットファブリックは、Transparent Interconnection of Lots of Links (TRILL)プロトコルを使います。TRILL は、互いに接続するために、ルーティングブリッジ(RBridges)と呼ばれるデバイスの集合を作ることにより、イーサネットを拡張するという目的のために設計されています。
動的なリンクステート型のルーティングプロトコルは、RBridge 間をどのように転送するかを決定します。Brocade VCS ファブリックベースの TRILL ネットワーク上のリンクステート型ルーティングは、Fabric Shortest Path First (FSPF)プロトコルを使って実行され、STP に比べて高速なコンバージェンスを可能とします。TRILL によりレイヤ２ネットワークがレイヤ３ ＩＰネットワークのような振る舞いをします。TRILL はまた、ユニキャストとマルチキャストの両トラフィックを転送する機能を定義しています。そして、単一のトランスポート層の上でこれらの用途の異なるクラスを統一してサポートできます。

9.2 Brocade VCS ファブリックの形成

Brocade VCS ファブリックテクノロジでは、ID 重複などのファブリック作成時の問題を発見するために RBridge ID を使用しています。クラスタ単位の RBridge ID は、FC スイッチのドメイン ID と同じです。RBridge ID の割り当ては、FC SAN のドメイン ID 割り当てプロトコルを活用することで実装されています。Request for Domain ID (RDI)と Domain ID Assignment (DIA)プロトコルは、一つのスイッチ(principal switch)がファブリック内の全ての RBridge に対するドメイン ID の集中的な割当とファブリック内で重複するドメイン ID の検出を保証します。重複がある場合、重複したノードはファブリックから分離されますので、この重複を解決する必要があります。

NOTE
Network OS v3.0 のファブリックは、一つの VCS ファブリック内で最大 239 の RBridge を持つことが出来ますが、ファブリックあたり 24 RBridges で使用することを推奨します。

次のイベントシーケンスは、VCS ファイブリックの構成手順を示しています。

- 各 VCS ファブリックは、VCS ファブリック ID により特定されます。
- 全ての VCS ファブリックが利用可能なスイッチは、デフォルトで VCS ID が 1 となっています。
- スイッチソフトウェアは、"VCS enable"に設定されているかをチェックします。

NOTE
もしソフトウェアが"VCS enable"に設定されていなかった場合、スイッチはスタンドアロンモードに移

行し、通常の 802.1x イーサネットスイッチとして動作します。

- スイッチで VCS ファブリック有効な状態と判断されると、スイッチソフトウェアは一連の手順を実行します。
  - Brocade Link Discovery Process (BLDP)により、VCS ファブリックが利用可能なスイッチがエッジポートと接続されているかを検出しようとします。更に詳細は、92 ページの『9.2.2 隣接デバイスの検出』を参照下さい。
  - BLDP はリンク状態にある VCS ファブリック環境に隣接のスイッチを組み込もうとします。
- 一連の Fibre Channel fabric formation protocols (RDI, DIA, and FSPF)の手順が実行され、２つの隣接スイッチ間でリンクレベルの関係が構築されます。更に詳細は、92 ページの『9.2.4 ファブリックの形成』を参照下さい。
- マージと結合プロトコルにより、クラスタユニット間のコンフィグレーションがマージされ、ファブリックが形成されます。

9.2.1 RBridge の動作

RBridge は、FSPF Hello フレームを交換することで互いを検出します。全ての TRILL IS-IS フレームのように、Hello フレームは、透過的に RBridges によって転送されて、RBridge ISL ポートで処理されます。Hello フレームで交換された情報を使って、各リンク上の RBridge はそのリンクに対する指定 RBridge を選びます。

RBridge リンク状態は、VLAN やマルチキャストリスナー、マルチキャストルーターアタッチメント、ニックネーム、サポートされている送受信オプションというような情報を含みます。指定 RBridge は、リンク上の各 VLAN に対して指定されたフォワーダーと RBridge 間の通信用に指定 VLAN を決定します。指定されたフォワーダーは、その VLAN のリンクのネイティブフレームを制御します。

RBrdige の受信機能は、TRILL データフレームにリンクから受信したフレームをカプセル化します。RBridge の送信機能は、TRILL データフレームから行先が決定しているネイティブフレームに分解します。学習済みユニキャストの TRILL データフレームは、RBridge により転送されます。

ブロードキャストやマルチキャスト及び未学習のユニキャストのような複数に転送されるフレームは、RBridge をルートとするツリーに転送されます。

- ユニキャスト転送は、FSPF によって生成されるドメインルーティング情報と MAC 学習及び分配された MAC テーブルによって生成される MAC-to-RBridge 学習情報を組み合わせて制御されます。
- マルチキャスト転送は、普通最も小さい RBridge ID をもつスイッチをルートとする一つのツリーが使われます。しかし、マルチキャストルートツリーの選択には、幾つかのルールがあります。常に、最も小さい RBridge ID が使われるわけではありません。

もし、リンク確立中に重複する RBridge ID が検出されると、リンクは分離されます。両サイドのスイッチは、エラーを認識しリンクを分離します。もし、新しいスイッチがオフラインからファブリックに組み込まれたケースで ISL のリンク確立時に RBridge ID の重複が検出されない場合は、ファブリック形成中に検出され、重複したスイッチが隔離されます。

RBridge は、コーディネータスイッチから特定の RBridge ID をリクエストします。もし、コーディネータスイッチが、この RBridge ID が既に使われていることを検出した場合、次の未使用の RBridge ID

を応答します。リクエストした RBridge は、別の RBridge ID を使用することは許されず、ファブリックから自ら分離します。このケースでは、ISL を起動することは出来ません。ISL は、明示的に無効化された後、重複した RBridge ID を持つ RBridge を取り除くために再度有効化される必要があります。

9.2.2 隣接デバイスの検出

VCS ファブリックが利用可能な隣接デバイスの検出は、次の手順で実行されます。

- 隣接デバイスが Brocade スイッチかどうかを検出します。
- Brocade 隣接スイッチが VCS ファブリック利用可能かを検出します。

同じ VCS ID を持った VCS ファブリック利用可能なスイッチだけが、仮想クラスタスイッチを構成します。内蔵 DCB スイッチの出荷設定は、VCS ファイブリックは無効ですが、VCS ID は"1"となっています。

9.2.3 Brocade トランク

Network OS v3.0.0 は、ハードウェアベースのリンクアグリゲーショングループ、または LAG などの Brocade トランクをサポートしています。これらの LAG は動的に 2 つの隣接スイッチとの間に形成されます。トランクの形成は FC スイッチ上のトランクの形成を制御するのと同じ FC のトランキングプロトコルによって制御されるので、有効化または無効化を除いてユーザーの介入や設定は必要ありません。設定は、グローバルレベルもしくはインタフェースレベルでトランクを形成するようスイッチのソフトウェアに指示します。手順については、96 ページの『9.4.3 ファブリックトランクの有効化』を参照してください。

NOTE

同一の隣接 Brocade スイッチに接続された全ての ISL ポートは、トランクを形成しようとします。トランクの形成を成功させるために、スイッチの全てのポートは、同じスピードで設定されなければなりません。これらトランクに対するルールは、Brocade ファイバチャネルスイッチのトランクに似ています。一つのトランクグループは８ポートまでです。

9.2.4 ファブリックの形成

Brocade VCS ファブリックテクノロジは、TRILL ファブリックを構築するため実績のあるファイバチャネルファブリックプロトコルを拡張したものです。ファブリック形成プロトコルのメインの機能は次の通りです。

- VCS ファブリック全体でユニークな RBridge ID(ドメイン ID)を割り当てる。
- Fabric Shortest Path First(FSPF)のようなリンクステートルーティングプロトコルを使って、ネットワークトポロジデータベースを生成する。FSPF は目的の RBridge までの最短ルートを計算します。
- ファブリックのマルチキャストトラフィックを分散します。

(1) Principal スイッチの選択

すべての Brocade VCS ファブリックが有効なスイッチは、ブートアップ時やファブリックポートを形成した後、それ自体が Principal スイッチであることを宣言し、すべてのファブリックポートでは、こ

のインテントを広告します。インテントには、優先順位とそのスイッチの WWN が含まれています。すべてのスイッチが同時に起動した場合は、デフォルトの優先順位は同じで、すべてのスイッチが、それらの相互のインテントを比較します。この比較で最も低い WWN を持つスイッチが Principal スイッチになります。WWN は、業界標準のスイッチに割当てられた識別子で、８バイトであることを除いて、MAC と似ています。Principal スイッチの役割は、ファブリックに参加した新しい RBridge が、ファブリックに既に存在するどの RBridge ID とも重複しないことを判断することです。

NOTE
内蔵 DCB スイッチは、工場出荷時にユニークな WWN（WWN）が割り当てられています。

Principal スイッチ選択プロセスの終了時には、クラスタ内のすべてのスイッチがルートに Principal スイッチでツリーを形成します。

(2) RBridge ID の割り当て
RBridge ID の割り当ては、FC SAN のから実績のあるドメイン ID 割り当てプロトコルを活用することで実装されています。ドメイン ID（RDI）、およびドメイン ID の割り当て（DIA）のプロトコルのための要求は、単一の Principal スイッチが集中的に、ファブリック内のすべての RBridge のドメイン ID を割り当てて、ファブリック内の任意のドメイン ID の競合を検出・解決することを保証します。VCS ファブリックは、24 までの RBridge ID をサポートします。
Principal スイッチだけが、ファブリック内の他のすべてのスイッチに対して RBridge の ID（ドメイン ID）を割り当てることができます。Principal スイッチは、ユーザーにより設定された ID を使って、自身の RBridge ID を割当てることによって、割当て処理を開始します。そして、DIA メッセージを全てのポートに送信します。
Principal スイッチ以外のスイッチは、DIA のフレームを受信したときに Principal スイッチに向かって RDI のメッセージで応答し、ファブリック内のすべてのスイッチにユニークな ID が割り当てられているまで、このプロセスを繰り返します。

9.2.5 ファブリックルーティングプロトコル
スイッチにドメイン ID が割り当てられた後、Fabric Shortest Path First (FSPF)リンクステートルーティングプロトコルは、隣接とのファブリックを形成し始めて、トポロジと接続性情報を収集します。VCS ファブリックは、最も小さい RBridge ID を持ったスイッチをルートとするループフリーなマルチキャストツリーを計算し選択するために、FSPF を使います。マルチキャストツリーは、ユニキャストルートが計算された後、計算されます。

NOTE
Principal スイッチ及びマルチキャストルートは、自動的に決定されます。このため、両方の機能が一つのスイッチに集中する場合があります。しかし、ファブリック管理の重要機能が一つのスイッチに集中することは好ましくありません。可能な限り、複数のスイッチに分散されるように構成することを推奨します。一旦設定された後でも、故障などでスイッチが交換された場合、Principal スイッチが

切替る場合があるため、ご注意下さい。Principal スイッチとマルチキャストルートを分散するには、下記要領で行います。

show fabric all コマンドにより、Principal スイッチを確認する。

show fabric route multicast コマンドにより、マルチキャストルートを確認する。

上記の結果より、同一スイッチ(RBridge ID)となっていた場合は、新たにマルチキャストルートとしたいスイッチに、fabric route mcast コマンドを使って、デフォルトの１より大きなプライオリティ値を設定します。

9.3 Brocade VCS ファブリックの構成管理

ファブリックに新たなスイッチを追加するため、次の設定手順を実行してください。

1. 管理者ロールに割り当てられたアカウントを使用してスイッチに接続します。
2. スイッチ上の RBridge ID プロパティを設定するために'vcs rbridge-id id enable'コマンドを使用します。
3. システムをリブートします。スイッチはリブート前に手動で設定された値をリブート後に割り当てられ、RBridge ID アロケーションプロトコルに参加します。

スイッチは、競合があるとファブリックに参加できません。例えば、同じ RBridge ID をもった別のスイッチが存在しファブリック上で動作中である場合です。この場合、同じ CLI 操作で使って新しい RBridge ID を選択してください。
一旦、ファブリックプロトコルにより ID が割当てられると、これらの ID は数値として RBridge ID と等しく、その後は RBridge ID として取り扱われます。
VCS ID や RBridge ID のような VCS ファブリックパラメータを設定したり、VCS ファブリックモードを有効にするため、'vcs'コマンドを使用します。VCS ファブリックパラメータの設定と VCS ファブリックモードの有効化は、同時にも別々にも行うことは可能です。詳細については、表 9-1 を参照してください。
VCS ファブリックの設定を変更後、スイッチは変更を適用し、リブートします。
スイッチの無効化状態は、リブート後まで保持されません。もし、リブート前に無効化されていた場合は、ブートが完了した後、有効化状態で復帰します。

9.3.1 VCS ファブリック設定作業

表 9-1 に VCS ファブリック環境をセットアップするために入力する追加のコマンドを示します。

表 9-1　VCS ファブリック設定作業の例

VCS ファブリック設定作業	VCS ファブリックコマンド例
スイッチの無効化、RBridge ID の設定、VCS ファブリックモードの有効化を行う	`switch# vcs rbridgeId 3 enable`

スイッチの無効化、VCS ID と RBridge ID の設定、VCS ファブリックモードの有効化を行う	`switch# vcs rbridgeId 3 vcsId 1 enable`
スイッチの無効化、RBridge ID と VCS ID 設定を別々に行う	`switch# vcs rbridge-id 3 enable` `switch# vcs vcs-id 1`
VCS ファブリックモードからスタンドアロンモードに切替える場合	`switch# no vcs enable`
現在のスイッチとファブリッククラスタ内の指定スイッチを交換する場合	`switch# vcs rbridge-id 5`

9.4 ファブリックインタフェースの構成管理

仮想スイッチクラスタ内の物理インタフェースは、エッジポートまたはファブリックポートにすることはできますが、両方はできません。物理インタフェースの switch-port の設定と同様に、'fabric ISL enable'および'fabric trunk enable'コマンドを使用して、物理インタフェース上のファブリックポート・コンフィギュレーションを変更することができます。以下に説明します。

9.4.1 ファブリック ISL の有効化

'fabric ISL enable'コマンドは、２つのスイッチ間の ISL の管理状態を制御します。ISL 検出が auto で ISL 形成モードが enable のデフォルト設定では、２つのクラスタスイッチ間では自動的に ISL が形成されます。ISL が動作中ならば'fabric isl enable'コマンドは、機能しません。しかし、'no fabric isl enable'コマンドはリンクステータスを切り替えた後、ISL が無効化されます。加えて、'no fabric isl enable'コマンドは、スイッチの ISL が無効になった事を隣接スイッチに通知することになります。その情報を受信すると、隣接スイッチは現在のインタフェース状態に係らず ISL の形成を中止します。

NOTE

任意のセグメント化または無効化した ISL ポートを修復した後、変更を隣接スイッチに通知するために、ファブリック ISL を切り替えます。

NOTE

動作中の ISL インタフェースへの'shutdown'コマンドは、物理リンクだけでなく FSPF の隣接情報もダウンさせます。'shutdown'コマンドと'no fabric isl enable'コマンドの違いは、'no fabric isl enable'後はリンクアップのままですが、'shutdown'後はリンクダウンします。

NOTE

ECMP ファブリックーISL パスを含むトポロジの変更により、ファブリックの再コンバージェンス時に、既知のユニキャストトラフィックによる数秒間のフラッディングがあるかもしれません。

9.4.2　ファブリック ISL の無効化

トランクの一部であるインタフェースに対して、'no fabric isl enable 'コマンドを使用し、トランクグループからこのインタフェースを取り除きます。スイッチ上のエッジとファブリックのポート割り当てを修正したい場合は、このコマンドを使用すると、完全に ISL の形成ロジックをオフにして、エッジポートでの任意のリンク立ち上げ遅延を短縮することができます。

1．管理者ロールに割り当てられたアカウントを使用してスイッチに接続します。
2．'no fabric isl enable'コマンドを入力します。

9.4.3　ファブリックトランクの有効化

1．管理者ロールに割り当てられたアカウントを使用してスイッチに接続します。
2．'fabric trunk enable'コマンドを入力します。

9.4.4　ファブリックトランクの無効化

ファブリックトランキングはデフォルトで有効です。２つの VCS ファブリックスイッチ間で ISL をスタンドアロンに戻すために、'no fabric trunk enable'コマンドを入力します。

9.4.5　ブロードキャスト、未学習ユニキャスト、マルチキャスト転送

Brocade VCS ファブリッククラスタ内の全てのスイッチは、最も小さい RBridge ID を持った RBridge をルートとする一つのマルチキャストツリーを共有します。２つのエッジ RBridge 間の全てのブロードキャスト、未学習ユニキャスト、マルチキャストは、Brocade VCS ファブリック内のこのマルチキャストツリーに転送されます。マルチキャストツリーは、VCS ファブリックの全ての RBridge を含んでいます。

(1) マルチキャスト分配ツリールートの選択

Network OS v3.0.0 は、次の分配ツリーの動作をサポートしています。

- デフォルトでは、分配ツリーのルートは、最も低い RBridge ID を持ったスイッチになります。自動選択のプロセスでは、ユーザーの介入は不要です。
- クラスタにある各スイッチは、任意にマルチキャストルートプライオリティを転送します。プライオリティ設定は、自動的に選択されたマルチキャストルートを上書きします。最も低い RBridge ID を持たない特定のスイッチがマルチキャストルートになることが必要な場合、スイッチのプライオリティ設定は、ルート選択を上書きします。同じプライオリティの２つのスイッチがあると、最も小さい RBridge ID を持ったスイッチが優先されます。
- バックアップマルチキャストルートがあらかじめ選択され、そしてそれは、その次に低い RBridge ID を持つスイッチです。現在のマルチキャストルートに障害が発生した場合、バックアップマルチキャストルートは、自動的にすべてのスイッチで選択されます。

9.4.6 プライオリティ

ツリーのルートには、最も小さい RBridge ID を持ったスイッチが自動的に選択されます。例えば、RBridge ID が 5,6,7,8 を持ったスイッチでクラスタが構成されていると、5 がルートに選択されます。もし、このファブリックに RBridge ID が 1 のスイッチを追加すると、ツリーは 1 をルートとして再計算します。

この振る舞いを避けるために、プライオリティ(デフォルトは 1)を設定することが出来ます。最も高いプライオリティは、最も小さい RBridge ID を上書きし、ルートになります。

例えば、ルートとして RBridge ID が 7 か 8 のファブリックを構成するために、1（プライオリティ値は 1～255 である）よりも高いものにプライオリティを設定します。例えば、RBridge ID 7 と 8 が両方ともプライオリティ 1 に設定されていれば、7 がルートになります。

(1) プライオリティの変更

1．スイッチに接続し、管理者権限のアカウントでログインします。

2． 'fabric route mcast rbridge-id'コマンドを入力します。

```
switch(config)# fabric route mcast rbridge-id 12 priority 10
```

9.4.7 running configuration の表示

'show running-config fabric route mcast'コマンドは、ファブリックルートマルチキャストの構成情報を表示します。スイッチで有効な現在のコンフィグレーションは、running configuration として参照されます。スイッチがオンラインの間にコンフィグレーションに行われた全ての変更は、 running configuration に行われます。running configuration は、恒久的ではありません。

NOTE

コンフィグレーションの変更を格納するために、running configuration をファイルへ格納するか、running configuration を startup configuration をコピーすることによって変更を適用します。

1．スイッチに接続し、管理者権限のアカウントでログインします。

2． ' show running-config fabric route mcast priority'コマンドを入力します。

```
switch# show running-config fabric route mcast priority
fabric route mcast rbridge-id 12 priority 10
```

9.4.8 VCS 仮想 IP アドレスの設定

仮想 IP アドレスは、各 VCS クラスタに割り当てられています。この仮想 IP アドレスは、クラスタ内の Principal スイッチに関連付けられています。Principal スイッチの管理インタフェースは、この仮想 IP アドレスを使用してアクセスできます。Principal スイッチがダウンした場合、仮想 IP アドレスはファブリッククラスタおよび管理クラスタの特性ですので次の Principal スイッチに割り当てられます。

仮想 IP アドレスを設定するために、'vcs virtual ip address'コマンドを使用します。

```
switch(config)# vcs virtual ip address 10.0.0.23
```

このコマンドは、ファブリッククラスタモードの管理クラスタで唯一、使用することができます。最初に仮想 IP アドレスが設定されている場合、クラスタ内の現在の Principal スイッチは、この IP アドレスが割り当てられています。
仮想 IP のコンフィグレーションは本質的にグローバルであり、クラスタ内のすべてのノードは、同じ仮想 IP アドレスを使用して構成されますが、アドレスは、現在の Principal スイッチに割当られます。
割り当てられた仮想 IP アドレスは、クラスタまたはネットワーク内の他の管理ポートに割り当てられたアドレスと重複しないことを確認してください。
管理インタフェースの IP アドレスと同じサブネットを使用することをお勧めします。
現在設定されている仮想 IP アドレスを確認するには、'show vcs'コマンドを使用します。

```
switch# show vcs virtual-ip
Virtual IP                : 10.21.87.2/20
Associated rbridge-id     : 2
```

現在設定されている仮想 IP アドレスを削除するには、'no vcs virtual ip address'コマンドを使用します。

```
switch(config)# no vcs virtual ip address
switch# show running-config vcs virtual ip address
% No entries found.
```

NOTE
仮想 IP アドレスとして、”10.255.x.x”のクラス A プライベートアドレスは使用できません。

NOTE
仮想 IP アドレスを使用してスイッチにログインしたときには、'no vcs virtual ip address'コマンドを使用してはいけません。仮想 IP アドレスを削除する場合、Principal スイッチの管理ポートの IP アドレス、または Principal スイッチのシリアルコンソール接続を使用します。

アドレス重複検出機能により、仮想 IP アドレスが Principal スイッチの管理インタフェースに割当てられない場合があります。この場合、管理インタフェースに仮想 IP アドレスを割当てたい場合は、現在設定されている仮想 IP アドレスを削除して、再設定してください。
独立したゲートウェイに仮想 IP アドレスを設定することはできません。デフォルトゲートウェイは、同じスイッチの管理ポートのゲートウェイアドレスと同じです。
Principal スイッチがリブート中は、仮想 IP アドレスを新たな Principal スイッチに割当てることはできません。

(1) 仮想 IP アドレスの構成シナリオ
クラスタ内の Principal スイッチには、仮想ＩＰアドレスが割り当てられます。その場合の構成シナリオを表 9-2 に示します。

表 9-2　構成のシナリオ

シナリオ	概要
最初のクラスタ形成	クラスタが最初に形成されている時と仮想 IP アドレスが既に設定されている場合、Principal スイッチは、仮想 IP アドレスが割り当てられています。もし、仮想 IP アドレス設定が存在しないならば、Principal スイッチは、管理ポートの IP アドレスを使用してアクセスすることができます。
仮想 IP の設定	最初にクラスタの仮想 IP アドレスを設定すると、仮想 IP アドレスが Principal スイッチの管理インタフェースにバインドされます。
Principal スイッチのフェイルオーバー	仮想 IP アドレスが管理インタフェースに割り当てられている間に Principal スイッチがセカンダリスイッチになった場合、仮想 IP アドレスは新しい Principal スイッチに再割り当てされます。
Principal スイッチのダウン	クラスタ内の Principal スイッチがダウンした場合、仮想 IP アドレスは、その管理インタフェースから解放されます。仮想 IP アドレスは、Principal スイッチになる次のスイッチに割り当てられます。
Principal スイッチのシャーシ無効化	Principal スイッチで'chassis disable'コマンドが実行されると、仮想 IP アドレスは、その管理インタフェースから解放されます。仮想 IP アドレスは、Principal スイッチになる次のスイッチに割り当てられます。
仮想 IP の削除	コンフィギュレーションから仮想 IP アドレスを削除する場合は、仮想 IP アドレスが Principal スイッチの管理インタフェースからアンバインドされます。この場合、Principal スイッチは引き続き管理ポートの IP アドレスを使用してアクセスできます。
些細なマージ	2 つのクラスタが一緒にマージした場合には、より小さい（クラスタ A）のグローバル･コンフィギュレーションは、大規模なクラスタ（クラスタ B）で上書きされます。この時間に、仮想 IP アドレスは、クラスタ A の Principal スイッチからアンバインドされます。クラスタ B の仮想 IP アドレスは、新しいマージされたクラスタの Principal スイッチにアクセスするために使用できます。クラスタ B の仮想 IP アドレスが設定されていない場合は、マージされたクラスタに仮想 IP アドレスが設定されません。
クラスタのリブート	クラスタを再起動すると、仮想 IP アドレスは、永続的で、新しい Principal スイッチにバインドされます。
クラスタの単独運転	ISL のリンクが形成している 2 つ以上のクラスタ間でダウンした場合、元のクラスタ内の Principal スイッチは、仮想 IP アドレスを保持します。第２クラスタ内の新しい Principal スイッチは、仮想 IP アドレスが使用中でないことを確認するためにチェックを実行します。使用中である場合、アドレスがスイッチに割り当てられないと意味するエラーが RASlog に記録されます。
スタンドアロンノードの動作	仮想 IP アドレスは、VCS モードでのスタンドアロンノード上に構成することができません。
仮想 MAC アドレス	仮想 MAC アドレスは、仮想 IP アドレスでサポートされません。
管理ポートのプライマリ IPv4 アドレス	仮想 IP アドレスが正常に機能するためには、管理ポートの IPv4 アドレスが割り当てられ、機能する必要があります。

9.4.9　ファブリックの ECMP 負荷分散

ECMP パスのトラフィックは、Vlan ID、MAC DA/SA、L3_ULP、L3 DA/SA、および、L4 Dst/Src の 8 つのフィールドをキーに負荷分散されます。ストリームのいくつかのパターンでは、トラフィックの大

部分は 1 つの ECMP パスにながれこみ、ECMP パスの残りの部分は十分に活用されません。この結果、トラフィックを分散させるために利用可能な ECMP パスが複数あっても、データトラフィックの損失となります。'fabric ecmp load-balance'コマンドを使用して、ファブリック内の ECMP パスの選択方法を設定することができます。このコマンドのオペランドを表 9-3 のリストに示します。

表 9-3　VCS ファブリック設定作業の例

オペランド	概要
dst-mac-vid	宛先 MAC アドレスと VID ベースの負荷分散
src-dst-ip	送信元および宛先 IP アドレスベースの負荷分散
src-dst-ip-mac-vid	送信元 IP アドレス、宛先 IP アドレス、MAC アドレスおよび VID ベースの負荷分散
src-dst-ip-mac-vid-port	送信元 IP アドレス、宛先 IP アドレス、MAC アドレス、VID および TCP / UDP ポートベースの負荷分散
src-dst-ip-port	送信元 IP アドレス、宛先 IP アドレスおよび TCP / UDP ポートベースの負荷分散
src-dst-mac-vid	送信元 MAC アドレス、宛先 MAC アドレスおよび VID ベースの負荷分散
src-mac-vid	送信元 MAC アドレスと VID ベースの負荷分散

また、'fabric ecmp load-balance-hash-swap'コマンドを使用して、ハッシュキーの隣接するビットを交換することができます。これは、トラフィックの分布が一様でないことが原因となる場合、ハッシュキーの組み合わせを選択するのに有用です。
'fabric ecmp load-balance-hash-swap command'コマンドは、ハッシュ関数に供給する前の入力フィールドの交換を設定するために使用されます。整数は、212 ビットキーとして解釈されます。各ビットは、キーの 2 つの隣接したビットを交換するかどうかを制御します。この 32 ビットの制御値は、すべての 4 つのハッシュ交換制御レジスタに書き込まれます。この値は、106 ビットの値を形成するために 32 ビットのブロック単位で複製されます。0x0 の値は、0xffffffff の値が全 106 の入力ビットペアを交換する間、入力フィールドを交換しません。

ECMP 負荷分散機能を設定するには、グローバルコンフィギュレーションモードで次の手順を実行します。

1．RbridgeID コンフィグレーションモードに遷移します。

```
switch(config)# rbridge-id 2
switch(config-rbridge-id-2)#
```

2．'fabric ecmp load-balance'コマンドを実行します。

以下の例では、宛先 MAC アドレスと VID ベースの負荷分散を設定します。

```
switch(config-rbridge-id-2)# fabric ecmp load-balance dst-mac-vid
```

3．オプション：'fabric ecmp load-balance-hash-swap'コマンドを使用してハッシュ関数に次に供給する前に、入力フィールドを交換します。

```
switch(config-rbridge-id-2)# fabric ecmp load-balance-hash-swap 4
```

4．'show fabric ecmp load-balance'コマンドを使用してハッシュフィールドの選択とハッシュ交換の現在のコンフィギュレーションを表示します。

```
switch# show fabric ecmp load-balance
Fabric Ecmp Load Balance Information
-----------------------------------
Rbridge-Id                  : 2
Ecmp-Load-Balance Flavor    : Destination MAC address and VID based load
balancing
Ecmp-Load-Balance HashSwap  : 0x4
```

9.5 VCS ファブリック上での操作

VCS ファブリックは、単一の論理シャーシを実現するよう設計されていますが、NOS 3.0.0_dcb ではスイッチ，ファブリックに対する操作に制約があります。以下に、スイッチ(rbridge)及びファブリックに対して可能な操作を示します。

表 9-4　VCS ファブリック上での操作

	対 象	操 作
情報参照	rbridge 個別情報	個々の rbridge 上でコマンドを実行する必要があります。'all'オプションが指定された場合でも、コマンドを実行している rbridge の情報のみ表示します。
	ファブリック情報 (例：マルチキャストルート)	ファブリック全体の構成に関する情報は、いずれかの rbridge でコマンドを実行することで参照可能です。
	キャッシュ情報 (MAC アドレステーブル)	本情報はファブリック全体で共有されており、いずれか一つの rbridge での実行結果が、ファブリック全体の情報を示すことになります。
情報設定	rbridge 個別情報	個々の rbridge に対して設定が必要です。
	ファブリック情報	ファブリック構成情報は、自動的に形成されますが、ファブリックを有効にする設定(`vcs enable')は、個々の rbridge に必要です。
	キャッシュ情報 (MAC アドレステーブル)	動的に学習される MAC アドレスは、自動的にファブリック全体で共有されますので、特別な設定操作は不要です。更に、動的に学習される MAC アドレスを削除する場合は、いずれか一つの rbridge で実行された結果が、自動的にファブリック全体で共有されます。 静的に登録する MAC アドレスも、いずれか一つの rbridge で設定した結果が、自動的にファブリック全体で共有されます。但し、静的に登録した MAC アドレスは、登録した rbridge 上でしか削除できません。

NOTE

動的に学習された MAC アドレスを削除する場合、`clear mac-address-table dynamic'は、いずれか一つの rbridge で実行してください。複数の rbridge で実行すると MAC アドレステーブルに不整合が発生し、一時的にフラッディングが発生することがあります。

10 Network OS システムモニタ

10.1 システムモニタの概要

システムモニタは、カスタマイズ可能なモニタリング閾値を提供し、スイッチの各コンポーネントの状態を監視することが可能となります。スイッチのコンポーネントが閾値を超えるたびに、システムモニタは、設定に応じて RASlog メッセージを使用し、自動的に通知を行います。閾値と通知の設定手順は、次のセクションで説明します。

10.1.1 スイッチヘルス監視

表 10-1 に示すように、サポートされているスイッチ上の監視対象の FRU は、次のとおりです。

- Temperature sensor - 温度センサコンポーネントの閾値を表示します。
- Compact-flash - コンパクトフラッシュデバイスの閾値を表示します。

10.1.2 ハードウェアプラットフォームのデフォルト閾値の設定

表 10-1 は、サポートされているスイッチのデフォルト閾値の設定を示します。

表 10-1 ハードウェアプラットフォームのデフォルト設定

プラットフォーム	ハードウェア コンポ-ネント	デフォルト設定	限界の閾値	ダウンの閾値
内蔵 DCB スイッチ	Temperature sensor	3	1	2
	Compact flash	1	1	0

10.1.3 システム設定の閾値

各コンポーネントは、工場出荷時の定義または、ユーザーが設定した閾値に基づいて、ダウンとマージナルの 2 つのいずれかの状態となります。デフォルトの閾値は、表 10-1 に示します。

NOTE

ダウンの閾値および限界の閾値にゼロを設定して、各コンポーネントの監視を無効にすることができます。

1．グローバルコンフィグレーションモードを開始するには、'configure terminal'コマンドを発行します。

2．ダウンの閾値および限界の閾値を設定するには、次のコマンドを入力します。

```
switch(config)# system-monitor {fan | power | temp | cid-card | compact-flash| MM
| LineCard | SFM } threshold [down-threshold value] [marginal-threshold value]
```

・temp は、温度センサ用の閾値設定を構成します。

・compact-flash はコンパクトフラッシュコンポーネントの閾値を設定します。

NOTE
'fan','power','cid-card' ,'MM','LineCard','SFM'オプションは、内蔵 DCB スイッチではサポートしていません。(設定しても機能しません。)

10.1.4 スイッチヘルスステータスの表示

スイッチヘルスステータスを表示するには、特権実行モードで'show system monitor'コマンドを入力します。

```
switch# show system monitor
```

10.1.5 システムモニタ構成の表示

システムモニタ構成を表示するには、特権実行モードで'show running-config system-monitoring'コマンドを入力します。

```
switch# show running-config system-monitor
```

10.2 リソース監視

システムモニタは、CPU とシステムのメモリ使用量を監視し、設定した閾値を超過しているユーザーに警告します。

CPU 監視を設定する場合は、1 から 100 の範囲の値を指定します。CPU 使用率が制限を超えると、システムモニタのアラートが発行されます。デフォルトの CPU の限界は 75%です。メモリ監視を設定する場合、閾値は使用可能なリソースのパーセンテージとして使用限度を指定します。メモリ監視の設定に使用する監視の閾値は、下限値より大きく、上限値より小さくなければなりません。

- High_limit
- 使用可能なメモリのパーセンテージとして、上限使用量を指定します。この値は、-limit パラメータで設定した値より大きくなければなりません。デフォルトは、80 パーセントで最大は、90 パーセントです。メモリ使用量がこの制限を超えると、システムモニタは、CRITICAL RASlog メッセージを生成します。
- Limit
- デフォルトの CPU 制限を指定します。制限を超えると、システムモニタが RASlog 警告メッセージを送信します。使用量が限界以下に戻ると、システムモニタが RASlog INFO メッセージを送信します。有効な値は 0 から 80 パーセントの間の範囲でデフォルト値は、別々のシステムのために異なります。
- Low_limit
- 使用可能なメモリのパーセンテージとして、下限使用量を指定します。この値は、-limit パラメータで設定した値よりも小さくなければなりません。メモリ使用量がこの制限を下回ると、システムモニタでは、INFO RASlog メッセージを生成します。すべてのプラットフォームのデフォルトは、50 パーセントです。

NOTE
メモリと CPU の閾値に対しては、下限値は最低値でなければならず、上限は最高値でなければなりません。

表 10-2 は、CPU およびメモリの閾値の工場出荷時のデフォルト一覧を示します。

表 10-2　CPU およびメモリの閾値の工場出荷時のデフォルト

オペランド	メモリ	CPU
Low-limit	40%	なし
Limit	60%	75%
High-limit	70%	なし
Poll	120 秒	120 秒
Retry	3	3
Action	なし	なし

10.2.1　メモリ監視の設定

NOTE
電子メールは、閾値監視のアクションとしてサポートされていません。

1．グローバルコンフィグレーションモードを開始するには、'configure terminal'コマンドを発行します。
2．'switch(config)#'プロンプトで rbridge-id を指定します。
3．次のパラメータを使用して、'threshold-monitor memory'コマンドを入力します。

```
switch(config-rbridge-id-1)# threshold-monitor memory ?
```

・actions
　閾値を超えた時、システムモニタトリガが指定するアクション。
・high-limit
　使用可能なメモリのパーセンテージ（0-80）などのメモリの上限使用量の制限。
・limit
　使用可能なリソースのパーセンテージ（0-80）と同様な使用量の制限。
・low-limit
　使用可能なメモリのパーセンテージ（0-80）などのメモリの下限使用量の制限。
・poll
　ポーリング間隔(秒単位)は、システムモニタがリソースの使用状況をポーリングする間隔。
・retry
　システムモニタがアクションをトリガする前に取るリトライ回数（0-100）。

10.2.2 CPU 監視の設定

NOTE
電子メールは、閾値監視のアクションとしてサポートされていません。

1．グローバルコンフィグレーションモードを開始するには、'configure terminal'コマンドを発行します。
2．'switch(config)#'プロンプトで rbridge-id を指定します。
3．次のパラメータを使用して'threshold-monitor cpu'コマンドを入力します。

```
switch(config-rbridge-id-1)# threshold-monitor cpu ?
```

・poll
ポーリング間隔(秒単位)は、システムモニタがリソースの使用状況をポーリングする間隔。
・retry
システムモニタがアクションをトリガする前に取るリトライ回数（0-100）。
・limit
使用可能なリソースのパーセンテージ（0-80）と同様な使用量の制限。

10.2.3 閾値監視設定の表示

次のパラメータを使用して'show running-config threshold-monitor'コマンドを入力します。

```
switch# show running-config rbridge-id 1 threshold-monitor
```

10.3 セキュリティ監視

NOTE
電子メールは、閾値監視のアクションとしてサポートされていません。

システムモニタは、セキュリティ対策を微調整するのを援助し、セキュリティを侵害するすべての試みを監視します。システムモニタはセキュリティ違反がある場合、RASlog アラートを送信します。次のセキュリティエリアは監視されています。

- telnet 違反 - telnet 接続要求が許可されていない IP アドレスからのセキュアなスイッチに到達した場合に発生します。
- ログイン違反 - セキュアなファブリックは、ログイン失敗を検出した場合に発生します。

セキュリティ監視における、閾値などの監視条件は変更できません。

10.4 インタフェース監視

システムモニタは、インタフェース監視として、show defaults threshold interface type Ethernet コマンドにより閾値及びアラートオプションのデフォルト値は表示されますが、本バージョンでは本機能は未サポートです。

11 ユーザーアカウントの管理

11.1 ユーザーアカウント

ユーザーアカウントは、認証されたユーザーにスイッチ CLI へのアクセスを許可します。ユーザーアカウントには、アカウントのアクセス権限を指定するロールを割り当てる必要があります。ユーザーアカウントは、ユーザーがスイッチにログインするのを防止するため、任意の時点で無効にすることができます。ユーザーがログイン試行の失敗で設定された閾値を超えると、アカウントが自動ロックされます。このロックは、ユーザーのみが解除することができます。また、認可されたユーザーのみがユーザーアカウントの作成、変更、ロック解除または削除をすることができます。

11.1.1 ローカルスイッチユーザデータベースのデフォルトアカウント

デフォルトのアカウントとして、工場出荷時 2 つのユーザーアカウントを定義しています。各スイッチの初期インストールおよび設定時にすべてのデフォルトアカウントのパスワードを変更することをお勧めします。

デフォルトユーザーアカウントは "admin"と"user"で、これらのアカウントは、スイッチのローカルユーザデータベース内の"admin"と"user"のロールに関連付けられています。"admin"と "user"のユーザーのみが CLI にアクセスすることができ、アカウントのパスワードを除いて、デフォルトユーザー（"admin"と"user"）のその他の属性を変更することはできません。

デフォルトでは、すべてのアカウント情報は、スイッチのローカルユーザデータベースに保管されています。スイッチへのログインユーザの認証と追跡は、デフォルトでローカルです。

NOTE

デフォルトアカウントを含むユーザーアカウントの最大数は、64 です。デフォルトロールを含むロールの最大数は、64 です。64 以上のユーザーを必要とする環境では、ユーザー管理のための認証、認可、アカウンティング（AAA）サービスを採用しなければなりません。詳細については、126 ページの『12 外部 AAA サーバの認証』を参照してください。スイッチ毎にサポートされるアクティブな telnet または CLI セッションの最大数は 32 です。

11.1.2 ユーザーアカウントの作成と変更

ユーザーアカウントを作成するときは、アカウントのログイン名、ロールおよび、パスワードの 3 つの必須属性を指定する必要があります。残りの属性は省略可能です。

表 11-1　ユーザーアカウントの属性

パラメータ	説明
Name	ユーザー名です。ユーザー名は大文字小文字を識別し、文字で始まり 40 文字以内でなければなりません。使用できる文字は、文字、数字、アンダースコア(_)、ピリオド(.)です。指定されたユーザー名が既に存在する場合は、'username'コマンドは、既存のロールを変更します。
role	ユーザーに割り当てられているロールは、アカウントの RBAC のアクセス権限を定義します。
password	アカウントパスワードは、すべての現在適用中のパスワード規則を満たさなければなりません。詳細については、120 ページの『11.4 パスワードポリシー』を参照してください。
encryption-level	パスワードの暗号化レベル。パスワードを暗号化（7）か、クリアテキスト（0）を選択できます。暗号化レベルを指定しない場合、クリアテキスト（0）がデフォルト設定です。
desc	アカウントのディスクリプション。ディスクリプションは、最長 64 文字まで指定でき、シングルクォテーション(')、ダブルクォーテーション(")、エクスクラメーション(!)、コロン(:)、セミコンマ(;)文字を除く、出力可能な任意の ASCII 文字を含めることができます。 ディスクリプションに空白が含まれている場合、ダブルクォテーション(")でテキストを囲む必要があります。
enable true | false	アカウントが有効か無効かを示します。アカウントが無効にされているユーザーはログインできません。デフォルトのアカウント状態は有効になっています。

11.1.3 ユーザーアカウントの作成

次の例では、最低限必要な属性（ユーザ名、ロール、パスワード）を持つ新しいユーザーアカウントを作成します。アカウント名"brcdUser"は、特権実行モードでアクセスするコマンドのデフォルトユーザー権限を所有しています。

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。

2．指定されたパラメータで'username'コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# username brcdUser role user password welcome
```

ユーザーアカウント情報の表示

ユーザーアカウント情報は、スイッチコンフィギュレーションファイルに保存されています。

- 設定されているすべてのユーザーを表示するには、特権実行モードで'show running-config username'コマンドを使用します。

```
switch# show running-config username
username admin password "BwrsDbB+tABWGWpINOVKoQ==¥n" encryption-level 7 role admin
desc Administrator
username user password "BwrsDbB+tABWGWpINOVKoQ==¥n" encryption-level 7 role
user desc User
```

- 単一のユーザーを表示するには、特権実行モードで'show running-config username username'コマンドを使用します。

```
switch# show running-config username admin
username admin password "BwrsDbB+tABWGWpINOVKoQ==¥n" encryption-level 7 role admin
desc Administrator
```

- アカウントが有効か無効かを表示するには、特権実行モードで'show running-config username username enable'コマンドを使用します。

```
switch# show running-config username admin enable
username admin enable true
```

11.1.4 既存ユーザーアカウントの変更

アカウントの作成および変更する操作の構文は似ています。違いは、既存アカウントを変更する場合は、必須パラメータが存在しないことです。システムが内部の構成データベースにユーザーアカウントが既に存在するかどうかをチェックすることにより、新しいアカウントを作成するか、既存のアカウントの変更操作をするかを認識します。
次の例では、以前に作成した "brcdUser"アカウントにディスクリプションを追加します。

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。
2．指定されたパラメータで'username'コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# username brcdUser
switch(config-username-brcdUser)# desc "Brocade guest account"
```

次の例では、アカウント"testuser"のためのパスワードを変更します。ユーザーのパスワードまたはロールを変更した場合、ユーザーのすべてのアクティブなログインセッションを終了します。

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。
2．指定されたパラメータで'username'コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# username testUser
switch(config-username-testUser)# password hellothere
```

11.1.5 ユーザーアカウントの無効化

enable パラメータに"false"を設定することにより、ユーザーアカウントを無効化することができます。

ユーザーアカウントが無効化された時、ユーザーのすべてのアクティブなログインセッションが終了します。

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。
2．指定されたパラメータで'username'コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# username testUser enable false
```

11.1.6 ユーザーアカウントの削除

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。
2．'no username'コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# no username testUser enable false
```

ユーザーアカウントを削除した時、ユーザーのすべてのアクティブなログインセッションが終了します。

11.1.7 ユーザーアカウントのロック解除

ログインリトライの閾値に達すると、ユーザーアカウントはシステムによって自動的にロックされます。アカウントのロックアウトの閾値は、設定可能なパラメータです。詳細については、122 ページの 『11.4.3 アカウントロックアウトポリシー』を参照してください。

NOTE

'username'コマンドと'no username'コマンドは、グローバルコンフィギュレーションコマンドですが、'unlock username'コマンドは、特権実行コマンドです。

1．現在アクティブなセッションとロックアウトしたユーザーを表示するには、特権実行モードで'show users'コマンドを入力します。
2．ロックされたユーザーアカウントのロックを解除するには、特権実行モードで'unlock username'のコマンドを入力します。
3．ユーザーがロック解除されたことを確認します。'show users'コマンドは、ロックされていないユーザーを表示します。

```
switch# show users
**USER SESSIONS**
RBridge
ID  Username    Host Ip       Device Time Logged In
2   user       10.70.4.105    vty/0  2012-04-30 01:59:35
1   user       10.70.4.105    vty/0  2012-04-30 01:57:41
```

```
1   admin      10.70.4.105    vty/2  2012-04-30 01:58:41
1   user       10.70.4.105    vty/3  2012-09-30 02:04:42
**LOCKED USERS**
RBridge
ID     username
1      testUser
switch# unlock username testUser
Result: Unlocking the user account is successful
switch# show users
**USER SESSIONS**
RBridge
ID  Username    Host Ip       Device Time Logged In
2   user       10.70.4.105    vty/0  2012-04-30 01:59:35
1   user       10.70.4.105    vty/0  2012-04-30 01:57:41
1   admin      10.70.4.105    vty/2  2012-04-30 01:58:41
1   user       10.70.4.105    vty/3  2012-09-30 02:04:42
**LOCKED USERS**
RBridge
ID     username
no locked users
```

11.2　ロールベースアクセス制御

Network OS は、許可メカニズムとして、ロールベースアクセス制御(RBAC)を使います。ロールは動的に作成することができ、個別のロールに適用できる権限を定義するためのルールに関連付けることができます。ユーザーアカウントは、いずれかのロールに関連付ける必要があり、ユーザーアカウントに関連付けられるのは、一つのロールだけです。

RBAC はリソースへのアクセス権を指定する機能です。ユーザーがコマンドを実行する時、ユーザーのロールに基づき、コマンドが使用可能かを判別されます。

11.2.1　デフォルトロール

内蔵 DCB スイッチは、2 つのデフォルトロール（"user"と "admin"）をサポートしています。デフォルトロールの属性を変更することはできませんが、デフォルト以外のユーザーアカウントにデフォルトロールを割り当てることができます。デフォルトロールは、次のアクセス権限を持っています。

- ユーザロールは、特権実行モードで show コマンドを実行する権限だけでなく、'ping'、'ping6'、'ssh'、'telnet'、'traceroute'のような運用上のコマンドに制限された権限を持ちます。ユーザロールに関連付けられているユーザーアカウントでは、グローバルコンフィギュレーションモードでのみ使用可能なコンフィグレーションコマンドにはアクセスできません。

- admin ロールは、最高の権限を持っています。admin ロールに関連付けられているユーザーは、特権実行モードとグローバルコンフィギュレーションモードのコマンドにアクセスできます。

新しいスイッチで admin ユーザーアカウントのみが、ユーザーとロールの管理操作を実行するためのアクセス権を持っています。admin ユーザーは、任意のロールの作成、アクセスのためのロールのユーザーへの設定および、ロールの管理操作ができます。

11.2.2 ユーザー定義ロール

デフォルトロールに加えて、Network OS は、ユーザー定義のロール作成をサポートします。ユーザー定義ロールは、特別なルールを追加することによって、洗練された特権の基本セットから始まります。ロールを作成したら、ロールに名前を割り当て、1 つ以上のユーザーアカウントへのロールを関連付けることができます。以下のツールは、ユーザー定義されたロールを管理するために利用できます。

- 'role'コマンドは、新しいルールの定義とユーザー定義ルールの削除をします。
- 'rule'コマンドを使用すると、特定の操作に対するアクセスルールを指定し、指定されたロールにこれらのルールを割り当てることができます。
- 'username'コマンドは、所定のユーザー定義ロールを特定のユーザーアカウントと関連付けます。

11.2.3 ユーザー定義ロールの作成

ユーザー定義ロールは表 11-2 に示すように、必須の名前とオプションの説明があります。

表 11-2　ロールの属性

パラメータ	説明
Name	ロール名が一意である必要があり、英字で始まり、英数字とアンダースコアを含めることができます。ロール名の長さは 4～32 文字の間でなければなりません。ロール名は、既存のユーザー、既存のデフォルトロール、または既存のユーザー定義ロールと同じにすることはできません。
desc	ロールのオプショナルディスクリプション。ディスクリプションは、最長 64 文字まで指定でき、シングルクォテーション(')、ダブルクォーテーション(")、エクスクラメーション(!)、コロン(:)、セミコンマ(;)文字を除く、出力可能な任意の ASCII 文字を含めることができます。 ディスクリプションに空白が含まれている場合、ダブルクォテーション(")でテキストを囲む必要があります。

ロールを作成は、以下の基準を満たさなければなりません。

- サポートするロールの最大数は 64 です。
- コマンドは、動作の権限があるアカウントから実行する必要があります。
- 'role'コマンドは、グローバルコンフィギュレーションモードで使用可能です。
- 指定されたロールが既に存在する場合、role コマンドは、既存のロールを変更します。

11.2.4 ロールの作成または変更

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモ

ードに入ります。

2．パラメータを指定して、'role'コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# role name VLANAdmin desc “Manages security CLIs”
switch(config-name-VLANAdmin)#
```

11.2.5 ロールの表示

特権実行モードで'show running-config role'コマンドを入力します。

```
switch# show running-config role

role name VLANAdmin desc “Manages security CLIs”
role name NetworkAdmin desc “Manages Network CLIs”
role name ClusterAdmin desc “Manages Cluster CLIs”
```

11.2.6 ロールの削除

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。

2．パラメータを指定して'no role'コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# no role name VLANAdmin
```

11.3 コマンドアクセスルール

コマンド認可はロールに関連付けられているルールの順序付き集合のかたちで定義されています。ルールは、ロールのアクセスモード(読み取り専用または読み書き用のアクセス)を定義し制限したり、特定のコマンドグループや個別のコマンドの実行権限を定義したりできます。定義済みのユーザー定義ロールに対して複数のルールを関連付けることができますが、ユーザーアカウントに関連付けられルロールはひとつだけです。

ルールを指定するには、少なくとも以下の 3 つの必須属性を指定する必要があります。

・ルールのインデックス番号

・ルールを適用するロール

・ルールによって定義されたコマンド

表 11-3 は、ルールの属性の詳細を説明します。

表 11-3 ルールの属性

パラメータ	説明
index	1～512 の範囲内のルールの識別子。

role	ルールが定義されているロール名。
command	アクセスが定義されているコマンド。
operation	オプション。ルールによって付与された一般的なアクセスモードを定義します。アクセスは、読み取り専用（read-only）または読み書き（read-write）にすることができます。デフォルト値は、" read-write "です。
action	オプション。一般的なアクセスモードを制限している修飾子。指定されたアクセスは受け入れる（accept）か、拒絶されます（reject）。デフォルト値は、"reject" です。

11.3.1 複数オプションで指定するコマンド

コマンド階層構造を示している複数の単語からなるコマンドは、スペースで区切られます。次に例を示します。

```
switch(config)# rule 70 action accept operation read-write role NetworkAdmin
command copy running-config
switch(config)# rule 71 action accept operation read-write role NetworkAdmin
command interface management
switch(config)# rule 72 action accept operation read-write role NetworkAdmin
command clear arp
```

NOTE

ルールはコマンド階層の最上位レベルではないコマンドに対して追加することはできません。適格なコマンドのリストを表示するには、コマンドプロンプトでヘルプ機能（?）を入力します。

11.3.2 コンフィギュレーションコマンドのルール

コマンド個別の構成データは、'show running-config'コマンドを使って表示されます。デフォルトでは、どのロールも'show running-config'を使用できます。非デフォルトロールでは、'show running-config'コマンドの使用権限でさえ、権限を与えられたユーザ(admin)のみ使用可能となるように変更することが出来ます。どのコンフィグコマンドでも実行できるようにするには、ユーザーが'configure'コマンドに対して read-write 権限を持っている必要があります。

次のルールは、コンフィギュレーションコマンドを規定します。

- ロールに read-write 権限とコンフィグレーションコマンドに対する accept action を持ったルールを適用している場合、このロールに関連付けられたユーザーはコマンドの実行とコンフィグレーションデータの参照が可能である。
- ロールに read-only 権限とコンフィグレーションコマンドの accept action を持ったルールを適用している場合、このロールに関連付けられたユーザーはコマンドのコンフィグレーションデータを参照することしか出来きません。
- ロールに read-write 権限とコンフィグレーションコマンドの reject action を持ったルールを適用している場合、このルールに関連付けられたユーザーはコマンドの実行ができないが、コマンドのコンフィグレーションデータを参照することができる。

11.3.3 運用コマンドのためのルール

指定された運用コマンドにしてルールを作成することができます。デフォルトでは、どのロールも運用コマンドを表示することはできますが、実行することは出来ません。show コマンドは全てのユーザーが使用可能です。

次のルールは運用コマンドを規定します。

- ロールに read-write 権限と運用コマンドに対する accept action を持ったルールが適用されていると、このロールに関連付けられたユーザーはコマンドを実行できます。
- ロールに read-only 権限と運用コマンドの accept action を持ったルールを適用している場合、このロールに関連付けられたユーザーはコマンドへアクセスできますが、実行することができません。
- ロールに read-write 権限と運用コマンドへの reject action を持ったルールを適用している場合、このルールに関連付けられたユーザーはコマンドへアクセスも実行もできません。

11.3.4 インタフェース関連コマンドのためのルール

デフォルトでは、すべてのロールが'show running-config interface interface_name rbridge-id/slot/port' コマンドを使用して、インタフェースのすべてのインスタンスに関連するコンフィギュレーションデータの読み出す権限を持っています。

インタフェース関連のコンフィギュレーションコマンドの特定インスタンスに対してルールを作成することができます。

次のルールはインタフェース関連コマンドを規定します。

- ロールに、read-write 権限とインタフェースの特定のインスタンスに対する accept action を持つルールが関連付けられてある場合、このロールに関連付けられているユーザーは、その属性を変更することができます。
- ロールに、read-only 権限とインタフェースの特定のインスタンスに対する accept action を持つルールが関連付けられてある場合、このロールに関連付けられているユーザーは、show running-config コマンドを使用してそのインタフェースに関連したデータの読み取りのみできます。
- ロールに、read-write 権限とインタフェースの特定のインタフェースに対する reject action を持つルールが関連付けられてある場合、このロールに関連付けられているユーザーは、そのインタフェースのコンフィグレーションデータの実行も読み取りもできません。

次の例では、規則は指定されたインタフェースの特定のインスタンスだけに適用できます。

```
switch(config)# rule 60 action accept operation read-write role NetworkAdmin
command interface tengigabitethernet 0/4
```

- ロールに、read-only または read-write 権限とインタフェースまたはインタフェースのインスタンスの reject action を持つルールが関連付けられてある場合、このロールに関連付けられているユーザーは、これらのインタフェースまたはインタフェースのインスタンスに関連する clear / show 操作ができません。clear / show 操作をするには、ユーザーのロールは、少なくとも read-only 権限と

accept 許可を持たなければなりません。デフォルトでは、すべてのロールは、すべてのインタフェースのために read-only 権限と accept 権限を持っています。

次に示す例では、NetworkAdmin ロールに関連付けられているユーザーが、全ての tengigabitethernet に関する clear / show 操作を実行できません。

```
switch(config)# rule 30 action accept operation read-write role NetworkAdmin
command interface tengigabitethernet
```

- ロールが read-write 権限および dot1x コマンドとインタフェースインスタンスへの accept 許可の両方を持っている場合、インタフェースインスタンスのサブモードで DOT1X オプションを設定することができます。

次の例では、CfgAdmin ロールに関連付けられているユーザーは、指定された tengigabitethernet インスタンスで dot1x コマンドにアクセスして実行することができます。

```
switch(config)# rule 16 action accept operation read-write role cfgadmin
command interface tengigabitethernet
switch(config)# rule 17 action accept operation read-write role cfgadmin
command dot1x
```

- インタフェース tengigabitethernet インスタンスのサブモードで'no vlan'および、'no spanning-tree'コマンドを実行するには、ユーザーが'vlan 'および'protocol spanning-tree'コマンドの read-write 権限および accept 許可を持つ必要があります。ユーザーが、少なくとも 1 つのインタフェースに対する read-write 権限および、'vlan'、'spanning-tree'コマンドへの accept 許可を持つならば、ユーザーが持っているデフォルトの許可(read-only 権限、accept 許可)でその他のインタフェースインスタンスに対して'no vlan'および、'no spanning-tree'の操作を実行できます。

11.3.5 プレースホルダルールの設定

'no-operation'オペランドで作られたルールは認証ルールに従いません。'no-operation'オペランドは、次の例のように有効なオペランドが後で追加できるようプレースホルダとして使用します。

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。
2．パラメータと’ no-operation’プレースホルダを指定して' rule'コマンドを入力します。
3．プレースホルダを置き換えるために、'rule'コマンドと指定したコマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# rule 75 action reject operation read-write role NetworkAdmin
command no-operation
switch(config)# rule 75 command firmware
```

11.3.6 ルールの処理

ユーザーがコマンドを実行する時、ルールは合致したインデックスで昇順に検索されます。そして、最初に合致したアクションが適用されます。ルールがマッチしない場合は、そのコマンドは実行されません。異なるインデックスでロールの権限が重複していた場合は、インデックスの小さいものが使われます。

read-only かつ accept 権限のルールに一致した場合は、システムは read-write かつ accept 権限のルールがないか更に検索します。その後、read-write および accept 権限で以降にみつかったルールが適用されます。

次の例では、ルール 11 で NetworkAdmin ロールが'aaa'コマンドにアクセスできるようにしたものです。

```
switch(config)# rule 9 operation read-only action accept role NetworkAdmin
command aaa
switch(config)# rule 11 operation read-write action accept role NetworkAdmin
command aaa
```

11.3.7 ルールの追加

適切なオプションを使用して、'rule'コマンドを入力して、ロールにルールを追加します。許可ルールを更新すると、ユーザーのアクティブなセッションには適用されません。ユーザーが、現在のセッションからログアウトして、新しいセッションにログインするときに変更が適用されます。

次の例では、ユーザーアカウントを作成および管理するために、セキュリティ管理者ロールを認可するルールを作成します。

1. 特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。
2. グローバルコンフィギュレーションモードへの read-write アクセスを指定するルールを作成します。
3. 'username'コマンドへの read-write アクセスを指定する 2 番目のルールを作成します。指定されたパラメータを使用して、'rule'コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# rule 150 action accept operation read-write role SecAdminUser command
config
switch(config)# rule 155 action accept operation read-write role SecAdminUser command
username
```

4. ルールを作成した後、SecAdminUser アカウントのユーザーがスイッチにログインして、'username'コマンドを使用してユーザーアカウントを作成または変更できます。

```
switch login: SecAdminUser
Password:******
Welcome to the ConfD CLI
```

```
SecAdminUser connected from 127.0.0.1 using console on switch


switch# configure terminal
Entering configuration mode terminal
Current configuration users:
admin console (cli from 127.0.0.1) on since 2010-08-16 18:35:05 terminal mode
switch(config)# username testuser role user password (<string>): ********
```

11.3.8 ルールの変更

次の例では、コマンド"username"が "role"で置換されるように、以前に作成したルール（インデックス番号 155）を変更します。

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。

2．既存のルール（インデックス No.155）を指定し、'role'コマンドのコマンド属性を変更するための'rule'コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# rule 150
switch(config)# rule 155 command role
```

インデックス番号 155 のルールを変更した後、SecAdminUser がスイッチにログインして、'username'コマンドではなく、'role'コマンドを実行することができます。

```
switch login: SecAdminUser
Password:
Welcome to the ConfD CLI
SecAdminUser connected from 127.0.0.1 using console on sw0
switch# configure terminal
Entering configuration mode terminal
Current configuration users:
admin console (cli from 127.0.0.1) on since 2010-08-16 18:35:05 terminal mode
switch(config)# role name NetworkAdmin
```

11.3.9 ルールの削除

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。

2．'no rule'コマンドに削除したいルールのインデックス番号を続けて入力します。

```
switch# configure terminal
Entering configuration mode terminal
```

```
switch(config)# no rule 155
```

ルール 155 を削除した後、SecAdminUser は、role コマンドにアクセスすることはできません。

11.3.10 ルールの表示

設定されたすべてのルールを表示するには、特権実行モードで'show running-config rule'コマンドを入力します。追加のパラメータを指定してコマンドを使用して出力をフィルタリングすることができます。

```
switch# show running-config rule
rule 30 action accept operation read-write role NetworkSecurityAdmin
rule 30 command role

rule 31 action accept operation read-write role NetworkSecurityAdmin
rule 31 command rule

rule 32 action accept operation read-write role NetworkSecurityAdmin
rule 32 command username

rule 33 action accept operation read-write role NetworkSecurityAdmin
rule 33 command aaa

rule 34 action accept operation read-write role NetworkSecurityAdmin
rule 34 command radius-server

rule 35 action accept operation read-write role NetworkSecurityAdmin
rule 35 command configure
```

11.3.11 コンフィギュレーション例

次の例は、頻繁に使用される管理者アカウント（Brocade VCS ファブリックセキュリティ管理者）の設定を一つ一つ示しています。

(1) Brocade VCS ファブリックセキュリティ管理者アカウントの設定

1．Brocade VCS ファブリックセキュリティ管理者のロールを作成します。

```
switch(config)# role name NetworkSecurityAdmin desc “Manages security CLIs”
```

2．新しく作成されたロールに関連付けるユーザーアカウントを作成します。

```
switch(config)# username SecAdminUser role NetworkSecurityAdmin password
testpassword
```

3．NetworkSecurityAdmin のロールのための RBAC アクセス許可を指定するルールを作成します。

```
switch(config)# rule 30 action accept operation read-write role
NetworkSecurityAdmin command role
switch(config-rule-30)# exit
switch(config)# rule 31 action accept operation read-write role
NetworkSecurityAdmin command rule
switch(config-rule-31)# exit
switch(config)# rule 32 action accept operation read-write role
NetworkSecurityAdmin command username
switch(config-rule-32)# exit
switch(config)# rule 33 action accept operation read-write role
NetworkSecurityAdmin command aaa
switch(config-rule-33)# exit
switch(config)# rule 34 action accept operation read-write role
NetworkSecurityAdmin command radius-server
switch(config-rule-34)# exit
switch(config)# rule 35 action accept operation read-write role
NetworkSecurityAdmin command config
switch(config-rule-35)# exit
```

SecAdminUser アカウントは、'configuration-level'コマンドのロール、ルール、ユーザー名、AAA、および radius-server への運用アクセスを付与されています。NetworkSecurityAdmin ロールに関連付けられたすべてのアカウントは、ユーザーアカウントの作成および、変更することができ、ロールを管理してルールを定義することができます。また、ロールは RADIUS サーバを設定可能にし、ログインシーケンスを設定します。

11.4　パスワードポリシー

パスワードポリシーは、グローバルな規制をすべての新しいパスワードに付与することにより、パスワードをより安全にするルールのセットを定義して、実施します。このセクションで説明するパスワードポリシーは、スイッチのローカルユーザデータベースに適用されます。設定したパスワードポリシー（すべてのユーザーアカウントの属性、およびパスワード状態情報）は、管理モジュール間で同期化して、HA フェイルオーバー後も維持されます。以下に、設定可能なパスワードポリシーのリストを示します。

- パスワード強度ポリシー
- パスワード暗号化ポリシー
- アカウントロックアウトポリシー

11.4.1 パスワード強度ポリシー

表 11-4 に設定可能なパスワードポリシーのパラメータを示します。

表 11-4 パスワードポリシーのパラメータ

パラメータ	説明
character-restriction lower	パスワードに使われなければならない小文字アルファベットの最小数を指定します。最大値は MinLength 値以下でなければなりません。デフォルトは 0 で、小文字の制約はありません。
character-restriction upper	パスワードに使われなければならない大文字アルファベットの最小数を指定します。最大値は MinLength 値以下でなければなりません。デフォルトは 0 で、大文字の制約はありません。
character-restriction numeric	パスワードに使われなければならない数字の最小数を指定します。最大値は MinLength 値以下でなければなりません。デフォルトは 0 で、数字の制限はありません。
character-restriction special-char	パスワードに使われなければならない句読文字を指定します。コロン(:)を除く全ての印刷可能な非英数字が使用できます。値は MinLength 値以下で無ければなりません。デフォルトは 0 で、句読文字の制約はありません。
min-length	パスワードの最小長を指定します。パスワードは 8 から 32 文字でなければなりません。デフォルトは 8 文字です。上記の４つのパラメータ(lowercase, uppercase, digits, punctuation)は MinLength 値以下でなければなりません。
max-retry	ユーザーがロックアウトされる前にログインが許す失敗パスワード数を指定します。ロックアウトの閾値は、0 から 16 までの範囲で指定することができます。デフォルトは 0 です。パスワードが強さ属性の 1 つ以上に失敗すると、エラーは一度に属性の 1 つのために報告されます。

11.4.2 パスワード暗号化ポリシー

Network OS は、スイッチレベルでのパスワードの暗号化を有効にすることによって、すべての既存のユーザーアカウントのパスワードを暗号化することをサポートします。デフォルトでは、暗号化サービスが無効になっており、パスワードはクリアテキストで格納されます。パスワードの暗号化を有効化または無効化するには、'service password-encryption'コマンドを使用します。次のルールは、パスワードの暗号化に適用します。

- パスワードの暗号化を有効にすると、すべての既存のクリアテキストのパスワードが暗号化され、その後、クリアテキストに加えられたすべてのパスワードが暗号化形式で保存されます。
  次の例では、パスワードの暗号化が有効になった後、testuser のアカウントのパスワードはクリアテキストで作成されます。グローバル暗号化ポリシーは、コマンドレベルの暗号化の設定を上書きしたパスワードは暗号化して格納されます。

```
switch(config)# service password-encryption
switch(config)# do show running-config service password-encryption
service password-encryption
switch(config)# username testuser role testrole desc "Test User"
encryption-level 0 password hellothere
switch(config)# do show running-config username
```

```
username admin password "BwrsDbB+tABWGWpINOVKoQ==¥n" encryptionlevel
7 role admin desc Administrator
username testuser password "cONW1RQ0nTV9Az42/9uCQg==¥n"
encryption-level 7 role testrole desc "Test User"
username user password "BwrsDbB+tABWGWpINOVKoQ==¥n" encryptionlevel
7 role user desc User
```

- パスワード暗号化サービスを無効化すると、クリアテキストに加えられる新しいパスワードでもスイッチ上でクリアテキストとして保存されます。既存の暗号化されたパスワードは暗号化されたままです。

  次の例では、パスワードの暗号化が無効になった後で、testuser のアカウントのパスワードがクリアテキストで保存されています。デフォルトのアカウント、"user"と admin "は暗号化されたままです。

```
switch(config)# no service password-encryption
switch(config)# do show running-config service password-encryption
no service password-encryption
switch(config)# username testuser role testrole desc "Test User"
encryption-level 0 password hellothere enable true.
switch(config)# do show running-config username
username admin password "BwrsDbB+tABWGWpINOVKoQ==¥n" encryptionlevel
7 role admin desc Administrator
username testuser password hellothere encryption-level 0 role
testrole desc "Test User"
username user password "BwrsDbB+tABWGWpINOVKoQ==¥n" encryptionlevel
7 role user desc User
```

11.4.3 アカウントロックアウトポリシー

アカウントロックアウトポリシーは、ログイン試行回数が指定した回数を超えた時、ユーザーアカウントを無効にするものです。アカウントロックされたユーザーは、ログインができません。ロックされたユーザー証明書を使っている SSH ログイン試行は、ユーザーに否定の理由を通知することなく拒否されます。

明示的に管理アクションでアカウントのロックを解除するまで、アカウントはロックされたままです。ユーザーアカウントを手動でロックすることはできません。ロックされていないアカウントのロックを解除することはできません。

失敗したログイン試行は、ローカルスイッチ上でのみ追跡されます。VCS モードでは、ユーザーアカウントはロックアウトが発生したスイッチだけでロックされ、同じユーザーで、VCS ファブリック内の別のスイッチにログインすることはできます。

アカウントロックアウトポリシーは、admin ロールを持つ root アカウント以外のすべてのユーザーアカウントに適用されます。

11.4.4 サービス妨害の拒否

アカウントロックアウト機構は、不正なパスワードを使用して繰り返しログインするアカウントに対し、サービス拒否の状態を作れるようになります。選ばれた特権アカウントの root や admin などは、サービス攻撃の拒否によりロックアウトされるのを防ぐために、アカウントロックアウトのポリシーから免除されています。しかし、これらの特権アカウントもパスワードの推測攻撃の標的になるかもしれません。定期的にこのような攻撃が試行されたかどうかを判断するためにセキュリティ監査ログを調べることをお勧めします。

セキュリティ監査ロギングに関する情報については、『Network OS Message Reference』を参照してください。

11.4.5 アカウントロックアウト閾値の設定

'password-attributes max-retry maxretry'コマンドでロックアウト閾値を設定することができます。maxretry の値は、ユーザーのアカウントがロックされる前に、誤ったパスワードでログインを試みることができる回数を指定します。失敗ログイン試行回数は、直前のログイン成功からカウントされます。maxretry は 0～16 の値に設定することができます。値が 0 の場合、ロックアウトメカニズムを無効にします（デフォルト）。

次の例では、ロックアウトの閾値を 5 に設定します。

1. 特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。
2. 指定したパラメータで、'password-attributes'コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# password-attributes max-retry 4
```

ユーザーアカウントがロックされている場合、それは 110 ページの『ユーザーアカウントのロック解除』で説明する手順を使用してロックを解除することができます。

11.4.6 リモート AAA サーバを使用したパスワード相互作用

パスワードポリシーは、ローカルスイッチの認証に適用されます。RADIUS、または TACACS+などの外部 AAA サーバは、サーバ固有のパスワード施行メカニズムを提供します。Network OS のパスワード管理コマンドは、スイッチが認証のために外部の AAA サービスを使用するように構成されている場合でも、スイッチローカルパスワードデータベースのみを操作します。リモートサーバによる認証はログインだけに適用されます。

リモート AAA サーバ認証が有効になっている場合でも、管理者は、ユーザーとローカルパスワードデータベースのパスワードの管理機能を実行できます。

リモート AAA サーバ認証の詳細については、126 ページの『12 外部 AAA サーバの認証』を参照してください。

11.4.7 パスワードポリシーの管理

既存のパスワードポリシーを定義または変更するために指定されたパラメータで、'password-attributes'コマンドを使用します。

(1) パスワードポリシーの作成

次の例では、最小長と強制文字の制限やアカウントのロックアウトに制約を課すパスワードポリシーを定義します。

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。
2．指定したパラメータで、’password-attributes’コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# password-attributes min-length 8 max-retry 4
character-restriction lower 2 upper 1 numeric 1 special-char 1
```

(2) デフォルトパスワードポリシーの復元

次の例では、最小長と強制文字の制限やアカウントのロックアウトに制約を課すパスワードポリシーを定義します。オペランドなしで使用した場合、コマンドはすべてのパスワード属性をリセットします。

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。
2．指定したパラメータで、’password-attributes’コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# no password-attributes min-length
switch(config)# password-attributes max-retry 4
switch(config)# no password-attributes
```

(3) パスワード属性の表示

特権実行モードで設定されたパスワード属性を表示するには、'show running-config password-attributes'コマンドを入力します。

```
switch(config)# password-attributes max-retry 4
switch(config)# password-attributes character-restriction lower 2
switch(config)# password-attributes character-restriction upper 1 numeric 1
special-char 1
switch(config)# exit
```

```
switch# show running-config password-attributes
password-attributes max-retry 4
password-attributes character-restriction upper 1
password-attributes character-restriction lower 2
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1
switch# configure terminal
switch(config)# no password-attributes character-restriction lower
switch(config)# no password-attributes character-restriction upper
switch(config)# exit
switch# show running-config password-attributes
password-attributes max-retry 4
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1
switch# configure terminal
switch(config)# no password-attributes
switch(config)# exit
switch# show running-config password-attributes
% No entries found.
```

11.5　セキュリティイベントのロギング

セキュリティイベントログは、セキュリティ関連の監査イベントを記録する RASLog 監査インフラストラクチャを利用しています。任意のユーザーが開始したセキュリティイベントは、監査可能なイベントを生成します。監査対象のイベントは、すべての管理インタフェース用に生成されます。VCS ファブリックモードでは、クラスタ全体のイベントのために、監査はクラスタ内のすべてのスイッチで発生します。
設定およびセキュリティ監査ログを監視する方法については、『Network OS Message Reference』を参照してください。

12 外部 AAA サーバの認証

12.1 リモートサーバ認証の概要

Network OS は、Brocade デバイスの外部認証、認可、アカウンティング（AAA）サービスを提供するために、様々なプロトコルをサポートしています。サポートされるプロトコルは、次のものがあります。

- RADIUS
  リモート認証ダイヤルインユーザーサービス
- TACACS+
  ターミナルアクセスコントローラアクセス制御システムプラス

リモート AAA サービスを使用するように設定すると、スイッチは、ネットワークアクセスサーバ（NAS）クライアントとして動作します。スイッチは、すべての認証、許可および、アカウンティング（AAA）サービス要求をリモート RADIUS、または TACACS+サーバへ送信します。リモート AAA サーバは、受信した要求を検証し、スイッチに応答を送信します。
RADIUS、または TACACS+とサポートされた管理アクセスチャネルは、シリアルポート、telnet、または SSH を含みます。
リモート RADIUS、または TACACS+サーバを使用するように設定した時、スイッチは、RADIUS、または TACACS+のクライアントになります。これらの構成では、認証レコードがリモートホスト／サーバのデータベースに格納されます。ログインとログアウトのアカウント名、割り当てられた権限、および時間アカウンティングレコードは、各ユーザー用の AAA サーバ上に格納されます。
障害が発生した場合に冗長性を提供するために、少なくとも 2 つのリモート AAA サーバを設定することを推奨します。各々のサポートされた AAA プロトコルのために、スイッチで最高 5 台の外部サーバを設定することができます。各スイッチは、それぞれのサーバ構成を維持します。

12.2 ログイン認証モード

認証モードは、AAA サービスがログインプロセスの間にユーザー認証のためにスイッチで使用される順序として定義されます。Network OS は、認証のプライマリおよびセカンダリの 2 つのソースをサポートしています。認証の二次ソースは、一次ソースのフェイルオーバーが発生した場合に使用して構成するためのオプションです。認証を行うための 4 つの可能性のあるソースを設定できます。

- Local
  デフォルトスイッチローカルデータベースを使用します。（デフォルト）
- RADIUS
  外部 RADIUS サーバを使用します。
- TACACS+
  外部 TACACS+サーバを使用します。

デフォルトでは、外部 AAA サービスは無効化され、AAA サービスがスイッチローカルユーザデータベースに既定されています。一次ソース（プライマリ）が外部の AAA サービス（RADIUS または TACACS+）に設定されていて、二次ソースが設定されていない場合、以下のイベントが起こります。

- telnet ベースおよび SSH 接続ベースのログインは、設定した一次ソースの AAA サーバがどれも応答しない、または、ログインを拒絶する場合、ログイン認証は失敗します。
- シリアルポート接続ベースのユーザログインは、何らかの理由でプライマリソースとの認証が失敗した場合、フェイルオーバーが発生し、同じユーザー資格情報がローカルソースでのログイン認証に使用されます。このフェイルオーバーは明白ではありません。
- 一次ソース（プライマリ）は外部 AAA サービスに設定されており、二次ソースは（たとえば、AAA 認証ログインの RADIUS ローカルのような）ローカルになるように構成されている場合、設定されたサーバのいずれもが応答しないか、またはログインがサーバによって拒否されたかの要因により、一次ソース（プライマリ）のログインが失敗すると、フェイルオーバーが発生し、認証が二次ソース（ローカル）を介して再度発生します。

12.2.1 適合の条件

一次ソースをデフォルトとして指定されている場合は、二次ソースを指定しないでください。二次ソースはログイン認証モードをデフォルト値に設定するための要求を出し、それはローカル認証です。一次ソースがローカルの場合、フェイルオーバーが発生することはありませんので、二次ソースは、任意の値に設定することはできません。
認証のソース（ローカル除く）と対応するサーバタイプの設定は、互いに依存しています。したがって、サーバタイプがソースとして指定される前に、少なくとも一つの構成済みのサーバが存在しなければなりません。
ソースがサーバタイプになるように構成されて、リストに唯一登録されているサーバである場合は、そのタイプのサーバを削除することはできません。TACACS+サーバのリストにエントリがない場合は、認証モードを TACACS+サーバまたは TACACS+ローカルに設定することはできません。同様に、認証モードが RADIUS または RADIUS ローカルで、リストに 1 つしかない場合、RADIUS サーバを削除することはできません。

(1) ログイン認証モードの設定と検証

以下の手順は、認証の一次ソース（プライマリ）の TACACS+と二次ソースとしてスイッチローカルユーザデータベースを構成します。

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。
2．指定したパラメータで、’ aaa authentication login’コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
```

```
switch(config)# aaa authentication login tacacs+ local
Broadcast message from root (pts/0) Tue Apr 5 16:34:12 2011...
AAA Server Configuration Change: all accounts will be logged out
```

3．構成を表示するために、'do show running-config aaa'コマンドを入力します。

```
switch(config)# do show running-config aaa
aaa authentication login tacacs+ local
```

4．TACACS+がユーザーを認証するために使用されているか確認するために、TACACS+のみの資格情報を持つアカウントを使用してスイッチにログインします。

(2) ログイン認証モードの解除

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。

2．設定した認証シーケンスを削除し、デフォルト値（ローカルのみ）を復元するためには、'no aaa authentication login'コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# no aaa authentication login
```

3．'do show running-config aaa'コマンドで構成を確認します。

```
switch(config)# do show running-config aaa
aaa authentication login local
```

4．TACACS+のみの資格情報を持つアカウントを使用してスイッチにログインします。ログインは、"アクセス拒否"のエラーで失敗します。

5．ローカルのみの資格情報を持つアカウントを使用してスイッチにログインします。ログインは、成功します。

(3) ログイン認証モードの変更

'aaa authentication login'コマンドを使用して、認証モードを設定することができますが、同じコマンドで既存の認証モードを変更または削除することはできません。'no aaa authentication login'のコマンドを使用してデフォルト値にリセットし、正しい値に認証シーケンスを再設定してください。

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。

2．デフォルト値に設定をリセットするには、'no aaa authentication login'コマンドを入力します。

3．'aaa authentication login'コマンドを入力し、希望する認証モードを指定します。

4．'do show running-config aaa'コマンドで構成を確認します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# no aaa authentication login tacacs+ local
switch(config)# aaa authentication login radius local
```

```
Broadcast message from root (pts/0) Tue Apr 5 16:34:12 2011...

AAA Server Configuration Change: all accounts will be logged out
switch(config)# do show running-config aaa
aaa authentication login radius local
```

5．TACACS+の資格情報を持つアカウントを使用して、スイッチにログインします。ログインは、"アクセス拒否"のエラーで失敗します。
6．RADIUS の資格情報を持つアカウントを使用して、スイッチにログインします。ログインは、成功します。

リモート認証ダイヤルインユーザーサービス（RADIUS）プロトコルは、一元的に認証、許可、およびアカウンティング（AAA）サービスを管理します。RADIUS と融和するサポート管理アクセスチャンネルは、シリアルポート、telnet と SSH です。

12.3 RADIUS

12.3.1 認証とアカウンティング

内蔵 DCB スイッチが認証に使用する RADIUS サーバのセットで構成されている場合、スイッチは、暗黙的に RADIUS サーバにアカウンティングデータを送信します。RADUS を使用するように設定された内蔵 DCB スイッチでサポートされる唯一のアカウンティングイベントは、RADIUS ユーザーのログイン成功とログアウトです。
ユーザー認証プロセスの間に、スイッチはその IP アドレスを送ります。Brocade VCS ファブリックモードでスイッチが仮想 IP アドレスを持っている場合、一意的な IP アドレスだけを RADIUS サーバに送信します。

NOTE
RADIUS サーバはアカウンティングをサポートするように構成されていない場合は、スイッチによってサーバへ送信されるアカウンティングイベントはドロップされます。

12.3.2 認可

RADIUS プロトコルを介してのユーザー認証は、サポートされていません。RADIUS アクセス制御のユーザーは、スイッチレベルで Brocade ロールベースアクセス制御（RBAC）プロトコルによって実施されます。すなわち、RADIUS サーバは、Vender Specific Attribute(VSA)である"Brocade-Auth-Role"を使うことで、スイッチに設定されたロールを割り当てられます。RADIUS ユーザーの認証が成功すると、サーバで設定されているユーザーのロールが得られます。ロールを得ることができない、または、得られたロールがスイッチに存在しない場合、”user”ロールが割り当てられ、セッションは"user"権限を持つユーザーに付与されます。

12.3.3 アカウントパスワードの変更

スイッチ上のローカルなユーザーアカウント及びパスワードの管理のための全てのメカニズムは、スイッチが RADIUS を使用するように設定された場合も、機能的に残されたままです。スイッチローカルなデータベースの変更は、RADIUS サーバに伝わらないだけでなく、RADIUS サーバのあらゆるアカウントに影響を与えません。すなわち、RADIUS ユーザーのパスワード変更は、RADIUS サーバ上での行われることになります。

12.3.4 管理インタフェースを介した RADIUS 認証

管理インタフェースまたはデータポート(TE インタフェースまたはインバンド)のいずれかから、telnet または SSH を使用してスイッチにアクセスすることができます。スイッチは、いずれかのアクセス方法を使って RADIUS ベースの同様の認証を行います。

12.3.5 クライアント側の RADIUS サーバの設定

それぞれのスイッチクライアントを個別の RADIUS サーバを使用するように設定する必要があります。サーバの IP アドレス、認証プロトコル、およびその他のパラメータを指定するには、'radius-server' コマンドを使用します。AAA サービスの内蔵 DCB スイッチで 5 つの RADIUS サーバの最大値を設定することができます。

表 12-1　RADIUS サーバのパラメータ

パラメータ	説明
Host	IP アドレス(IPv4 または IPv6)または RADIUS サーバのホスト名。ホスト名は、先に DNS 設定が必要となります。ホスト名でサポートされる最大長は 40 文字です。
auth-port	認証のために RADIUS サーバと接続する UDP ポート。0 から 65535 まで指定可能。デフォルトは 1812。
Protocol	使用する認証プロトコル。CHAP、PAP、PEAP が指定可能。デフォルトは CHAP。PEAP が設定されたプロとコツの場合、IPv6 ホストはサポートされません。
Key	スイッチと RADIUS サーバ間の公開秘密鍵。デフォルトは"sharedsecret"。キーはスペースを含まず、8 から 40 文字以内でなければなりません。空のキーはサポートしません。
Retransmit	RADIUS サーバに接続する場合のリトライ回数。0 から 100 まで指定可能。デフォルトは 5 回。

NOTE

キー属性を設定しない場合、認証セッションが暗号化されません。キー属性の値は、RADIUS コンフィギュレーションファイルで設定された値と一致する必要があり、そうでなければ、サーバとスイッチ間の通信は失敗します。

(1) クライアントサーバーリストへの RADIUS サーバの追加

RADIUS サーバをドメイン名またはホスト名で追加する前に、スイッチ上のドメインネームシステム

（DNS）サーバを設定する必要があります。DNS サーバがないと RADIUS サーバの名前解決が失敗し、追加操作は失敗します。DNS サーバを設定するには、'ip dns'コマンドを使用します。

NOTE
サーバのリストがスイッチで構成されるとき、RADIUS サーバが応答することができない場合にだけ、1 台のサーバから別のサーバへのフェイルオーバーは起こります。ユーザー認証が失敗するときには起こりません。

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。
2．指定したパラメータで、' radius-server'コマンドを入力します。
コマンドの実行と同時に、さらに追加パラメータを指定することができる AAA サーバのコンフィギュレーションサブモードに入ります。
3．'exit'コマンドを入力して、グローバルコンフィグレーションモードに戻ります。
4．設定を確認するには、'do show running-config radius-server host'コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# radius-server host 10.38.37.180 protocol pap key
“new#virgo*secret” timeout 10
switch(config-host-10.38.37.180)# exit
switch# show running-config radius-server host 10.38.37.180
radius-server host 10.38.37.180
protocol   pap
key        “new#v
timeout    10
```

(2) RADIUS サーバ構成の変更

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。
2．設定された RADIUS サーバを表示するには、ヘルプオプション（？）で'radius-server host'コマンドを入力します。
3．変更したいサーバの IP アドレスを指定して'radius-server host'コマンドを入力します。
コマンドの実行と同時に、さらに変更したいパラメータを指定することができる radius-server コンフィギュレーションサブモードに入ります。
4．変更したいパラメータと値を入力します。
5．設定を確認するには、'do show running-config radius-server'のコマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# radius-server ?
```

```
Possible completions:
<hostname: IP Address or Hostname of this RADIUS server>
10.38.37.180
10.24.65.6
switch(config)# radius-server host 10.38.37.180
switch(config-host-10.38.37.180 )# key “changedsec”
switch(config-host-10.38.37.180 )# timeout 3
switch(config)# do show running-config radius-server host 10.24.65.6
radius-server host 10.24.65.6
protocol    pap
key         changedsec
timeout     3
```

'no radius-server host'コマンドは、設定された RADIUS サーバのリストからサーバ設定を削除します。指定されたパラメータで使用すると、コマンドはそのパラメータのデフォルト値を設定します。

(3) RADIUS を使用ログイン認証のクライアントの設定
クライアント側の RADIUS サーバのリストを設定した後、RADIUS が認証の主要ソースとして使用されるように、認証モードを設定する必要があります。
ログイン認証モードを設定する方法については、126 ページの『12.2 ログイン認証モード』を参照してください。

12.3.6 サーバ側の RADIUS の設定

RADIUS サーバを使用すると内蔵 DCB スイッチで作成されたアカウント名ではなく、真のネットワーク全体の識別子でユーザーアカウントを設定する必要があります。各アカウント名と一緒に、適切なスイッチアクセスロールを割り当てる必要があります。ユーザーアカウントは、同時にスイッチのユーザーと同じ名前で、RADIUS サーバに存在することができます。
RADIUS を設定するスイッチにログインする際プロンプトが表示されたときに、ユーザーは割り当てられた RADIUS アカウント名とパスワードを入力します。一旦、RADIUS サーバがユーザーを認証すると、Brocade Vendor-Specific Attribute（VSA）を使っているユーザーアカウント情報と関連付けられたスイッチロールと情報で応答します。ロールの割り当てがなくても、認証受け付け応答は自動的に"user"ロールを付与します。

(1) Linux を使用した RADIUS サーバの設定
FreeRADIUS は Linux のすべてのバージョン、FreeBSD、NetBSD および Solaris 上で動作するオープンソースの RADIUS のサーブです。www.freeradius.org からパッケージをダウンロードし、FreeRADIUS の Web サイトでのインストール手順に従います。
Brocade 固有の属性を設定するには、次の情報が必要になります。

RADIUS サーバの設定と起動方法については、RADIUS の製品マニュアルを参照してください。

(2) RADIUS サーバ設定へのブロケード属性の追加

Linux FreeRADIUS サーバの構成のために、表 12-2 の dictionary.brocade という名前のベンダ辞書ファイルで説明された値を定義します。

表 12-2　dictionary.brocade ファイルエントリ

Include	Key	Value
VENDOR	Brocade	1588
ATTRIBUTE	Brocade-Auth-Role	1 string Brocade

1．以下の情報を使用してファイル $PREFIX/etc/raddb/dictionary.brocade を作成し、保存します。

```
#
# dictionary.brocade
#
VENDOR Brocade 1588


#
# attributes
#
ATTRIBUTE    Brocade-Auth-Role       1     string  Brocade.
```

2．テキストエディタでマスタ辞書ファイル $PREFIX の/etc/raddb/dictionary を開き、行を追加します。

```
$INCLUDE dictionary.brocade
```

その結果、ファイル dictionary.brocade は、RADIUS マスタ構成ディレクトリに配置され、RADIUS サーバで使用するためにロードされます。

(3) Brocade ユーザーアカウントの設定

Linux FreeRadius サーバの構成のために、表 12-2 の dictionary.brocade という名前のベンダ辞書ファイルで説明された値を定義します。

1．テキストエディタでファイル $PREFIX/etc/raddb/users を開きます。
2．ユーザー名を追加して、権限を関連付けます。
ユーザーは、Brocade-AUTH-role で指定されたアクセス許可を使用してログインします。有効な権限は、"user"と "admin"が含まれています。パスワードおよびロールの前後に二重引用符(")を使用する必要があります。

次の例では、"jsmith"というアカウントに管理者権限とパスワード "jspassword"を設定します。

```
jsmith          Auth-Type := Local,
                User-Password == "jspassword",
                Brocade-Auth-Role = "admin"
```

認証のためのネットワーク情報サービス（NIS）を使用する場合、パスワードファイルを使用して認証を有効にする唯一の方法は、内蔵 DCB スイッチがパスワード認証プロトコル（PAP）を使用して認証するように設定することです。これは、'radius-server host'コマンドで PAP オプションが必要です。

(4) Windows サーバを使用した RADIUS サーバサポートの設定
マイクロソフト Windows server 2008（または以前の Windows 2003 または 2000）でてインターネット認証サービス（IAS）をインストールして、構成するための手順は、www.microsoft.com またはあなたのマイクロソフト・ドキュメンテーションから得ることができます。ネットワーク環境を設定する前に、システム管理者またはネットワーク管理者に相談してください。
内蔵 DCB スイッチのためのインターネット認証サービスを設定するために、以下の情報を使ってください。
新しい RADIUS クライアントウィンドウのクライアントベンダーメニューから RADIUS 標準を選択します。次のようにダイヤルインプロファイルのウィンドウを設定します。

1．[Advanced]タブを選択します。
2．RADIUS の標準リストの一番下までスクロールして、[Vendor-Specific]を選択し、[Add]をクリックします。
Multivalued Attribute Information ダイアログが表示されます。
3．Multivalued Attribute Information ウィンドウで[Add]をクリックします。
Vendor-Specific Attribute Information ダイアログボックスが表示されます。
4．1588 の Brocade ベンダーコード値を入力します。
5．[Yes]を選択し、ラジオボタンに従い、[Configure Attribute]をクリックします。
Configure VSA (RFC compliant)ダイアログが表示されます。
6．Configure VSA (RFC compliant)ウィンドウで、次の値を入力し、[OK]をクリックします。
[Vendor-assigned attribute number]に、1 を入力します。
[Attribute format]に、String を入力します。
[Attribute value]に、'admin'または'user'を入力します。

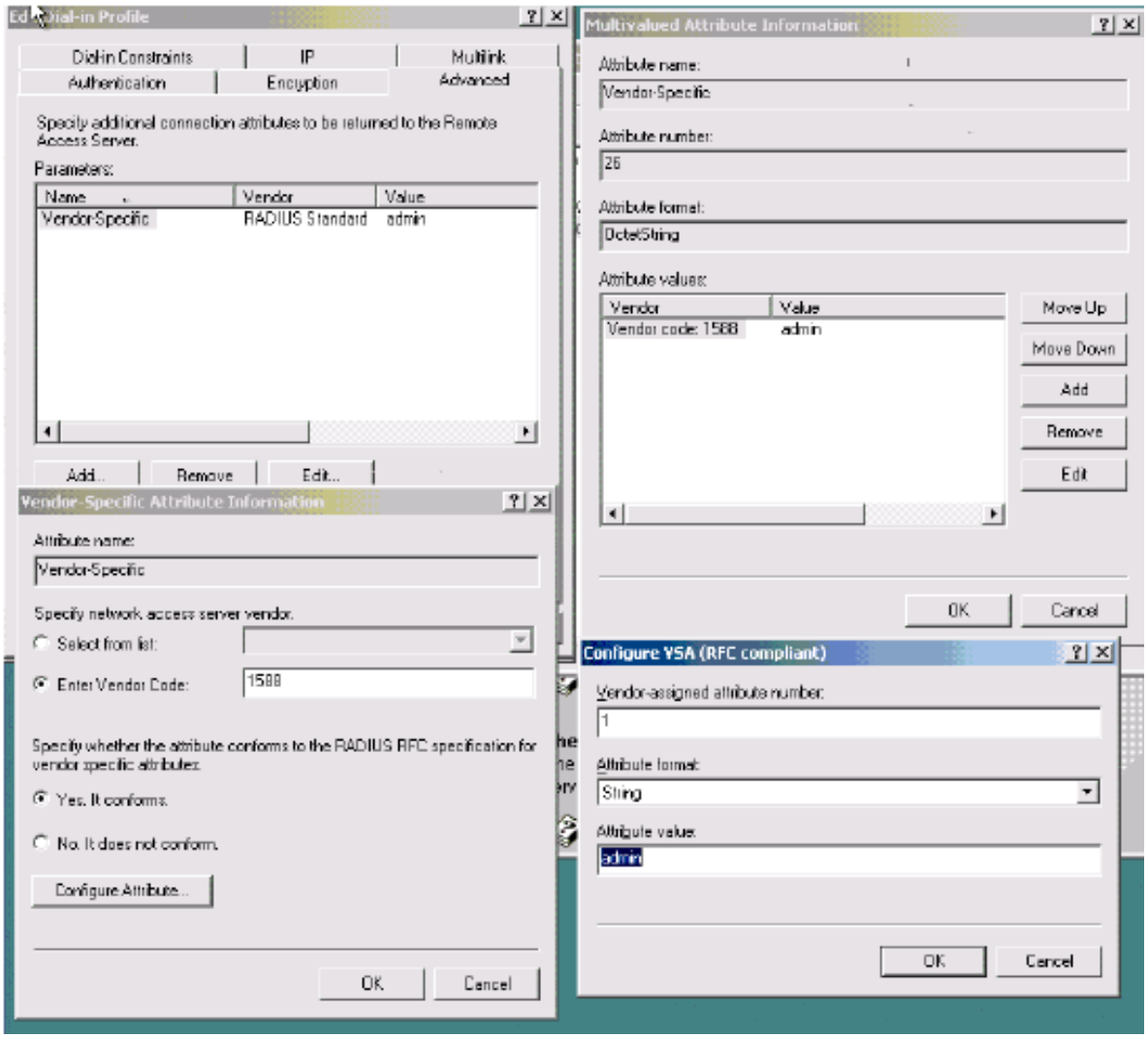

図 12-1 Windows サーバ VSA の設定

12.4　TACACS+

Terminal Access Controller Access-Control System Plus (TACACS+)は、集約された認証サーバや複数の Network Access Servers (NAS)もしくはクライアントで構成される AAA サーバ環境で使用されるプロトコルです。TACACS+をサポートすることで、スイッチをこれらの環境にシームレスに統合することが可能となります。一旦、TACACS+を使用するように設定すると、スイッチは Network Access Servers (NAS)として機能します。

12.4.1　認可

TACACS+サーバが認証とアカウンティングにのみ使用されます。認可は、スイッチレベルでの Brocade role-based access control（RBAC）プロトコルによって実施されます。同じロールは、TACACS+サーバで設定し、スイッチ上で設定されたユーザーに割り当てる必要があります。スイッチの認証が成功した後に、TACACS+サーバからユーザロールの取得で失敗した場合、または、ロールがスイッチで提示されたロールと一致しない場合、ユーザロールは、デフォルトで割り当てられます。その後、TACACS+サーバから得られたロールまたはデフォルトのロールは、RBAC のために使用されます。

12.4.2　管理インタフェースを介した TACACS+認証

シリアルポートを介して、または、管理インタフェースかデータポート（TE インタフェースまたはインバンド）から telnet または SSH を介してスイッチにアクセスすることができます。スイッチは、どちらのアクセス方式ででも同じ TACACS+ベースの認証を行います。

12.4.3　サポートするパッケージとプロトコル

次の TACACS+パッケージを実行するためにリモート AAA サーバで TACACS+デーモンをサポートしています。

- フリーTACACS+ daemon(tacacs-plus 4.0.4.23-3)
  このパッケージを http://www.shrubbery.net/tac_plus/からダウンロードすることができます。
- ACS 5.3
- ACS 4.2

TACACS +プロトコル v1.78 は、内蔵 DCB スイッチのクライアントおよび TACACS +サーバの間の AAA サービスに使用されます。
ユーザー認証のためにサポートされている認証プロトコルは、Password Authentication Protocol（PAP）と Challenge Handshake Authentication Protocol（CHAP）です。

12.4.4　クライアント側の TACACS+サーバ設定

それぞれの内蔵 DCB スイッチクライアントは個別の TACACS+サーバを使用するように設定する必要があります。サーバの IP アドレス、認証プロトコル、およびその他のパラメータを指定するには、

'tacacs-server'コマンドを使用します。内蔵 DCB スイッチの AAA サービスでは、最大 6 つの TACACS+サーバを設定することができます。
表 12-3 のパラメータは、スイッチ上で設定された TACACS+サーバに関連付けられています。

表 12-3　RADIUS サーバのパラメータ

パラメータ	説明
Host	IP アドレス(IPv4 または IPv6)または TACACS+サーバのドメイン／ホスト名。ホスト名は、先に DNS 設定が必要になります。ホスト名でサポートされる最大長は 40 文字。
Port	認証のために TACACS+サーバと接続する TCP ポート。ポート範囲は、1～65535 で、デフォルトは 49。
Protocol	使用する認証プロトコル。CHAP または PAP が指定可能で、デフォルトは CHAP。
Key	安全にメッセージ交換をするためのスイッチと RADIUS サーバ間の公開秘密鍵。デフォルトは"sharedsecret"。キーはスペースを含まず、8 から 40 文字以内でなければなりません。空のキーはサポートしません。
retries	ACACS+サーバに接続する場合のリトライ回数。0 から 100 まで指定可能で、デフォルトは５回。
Timeout	サーバが応答するまでの待ち時間。1 から 60 秒が指定可能で、デフォルトは 5 秒。

NOTE
キー属性を設定しない場合、認証セッションが暗号化されません。キーの値は、TACACS+コンフィギュレーションファイルで設定された値と一致する必要があり、そうでなければ、サーバとスイッチ間の通信は失敗します。

(1) クライアントサーバーリストに TACACS+サーバを追加
ドメイン名またはホスト名で TACACS+サーバを追加する前にスイッチのドメインネームシステム（DNS）サーバを設定する必要があります。DNS サーバがないと、TACACS+サーバの名前解決が失敗するため、追加操作は失敗します。DNS サーバを設定するには、'ip dns'コマンドを使用します。

NOTE
サーバのリストがスイッチで構成されるとき、TACACS+サーバが応答することができない場合にだけ、1 台のサーバから別のサーバへのフェイルオーバーは起こります。ユーザー認証が失敗するときには起こりません。

次の手順では、IPv6 形式で TACACS+サーバホストを追加します。

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。
2．'tacacs-server'コマンドを入力し、サーバの IP アドレスを指定します。
コマンドの実行時に、追加のパラメータを指定することができる tacacs-server コンフィギュレーションサブモードに入ります。
3．設定を確認するには、'do show running-config tacacs-server host'コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
```

```
switch(config)# tacacs-server host fec0:60:69bc:94:211:25ff:fec4:6010
switch(config-tacacs-server-fec0:60:69bc:94:211:25ff:fec4:6010)# protocol chap key
“new#hercules*secret”
switch(config-tacacs-server-fec0:60:69bc:94:211:25ff:fec4:6010)# exit
switch(config)# do show running-config tacacs-server
fec0:60:69bc:94:211:25ff:fec4:6010
tacacs-server host fec0:60:69bc:94:211:25ff:fec4:6010
key new#Hercules*secret
!
```

(2) TACACS+サーバ構成の変更

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。
2．設定されているサーバの IP アドレスを表示するには、ヘルプオプション（？）で'tacacs-server host'コマンドを入力します。
3．変更したいサーバの IP アドレスで、'tacacs-server host'コマンドを入力します。
コマンドの実行時に、変更したいパラメータを指定することができる tacacs-server コンフィギュレーションサブモードに入ります。
4．グローバルコンフィグレーションモードに戻るため、'exit'コマンドを入力します。
5．設定を確認するには、'do show running-config tacacs-server host'コマンドを入力します。
このコマンドは、デフォルト値が表示されません。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# tacacs-server host ?
fec0:60:69bc:94:211:25ff:fec4:6010
switch(config)# tacacs-server host fec0:60:69bc:94:211:25ff:fec4:6010
switch(config-tacacs-server-fec0:60:69bc:94:211:25ff:fec4:6010)# key “changedsec”
retries 100
switch(config-tacacs-server-fec0:60:69bc:94:211:25ff:fec4:6010)# exit
switch(config)# do show running-config tacacs-server
fec0:60:69bc:94:211:25ff:fec4:6010
tacacs-server host fec0:60:69bc:94:211:25ff:fec4:6010
key       changedesc
retries    100
!
```

'no tacacs-server host'コマンドは、設定された RADIUS サーバのリストからサーバ設定を削除します。削除される tacacs-server がリストの最後のものであり、認証モードが設定されている TACACS+の場合、スイッチコンフィグレーションからのサーバの削除は、拒否されます。指定されたパラメータと一緒

に使用すると、コマンドはそのパラメータのデフォルト値を設定します。

(3) TACACS+のログイン認証のためのクライアント設定
クライアント側の TACACS+サーバのリストを設定した後、その TACACS+が認証のプライマリソースとして使われるように認証モードを設定する必要があります。
ログイン認証モードを設定する方法については、126 ページの『12.2 ログイン認証モード』を参照してください。

12.5 TACACS+アカウンティング

TACACS+プロトコルは、認証とは明確に独立した関数としてアカウンティングをサポートします。認証またはアカウンティングのためにだけ、または、両方とものために TACACS+を使うことができます。TACACS+サーバで、ログインアカウンティング、コマンドアカウンティングまたは両方とも有効にすることによって、ユーザーがログインセッションの間に実行するユーザログインとコマンドを調査することができます。

- ログインアカウンティングが有効の場合、ユーザーがログインするとスイッチは設定された TACACS+サーバに関連した属性で、TACACS+開始アカウンティングパケットを送信します。セッションが終了すると停止アカウンティングパケットを送信します。
- コマンドアカウンティングを有効にすると、スイッチはコマンドの実行が終了した時、サーバに、TACACS+アカウンティング停止パケットを送信します。TACACS+アカウンティング開始パケットは、コマンドアカウンティングのために送信されません。ほとんどのコンフィギュレーションコマンド、show コマンドとファームウェアのダウンロードなどの非コンフィギュレーションコマンドは追跡されます。
  アカウンティングされないコマンドのリストについては、357 ページの『31 TACACS+ Accounting の例外』を参照してください。

TACACS+サーバが認証およびアカウンティングの両方に使用されている場合、TACACS+サーバにアカウンティングパケットを送信するときに正常に認証のために使用されたサーバに、スイッチは最初に接続しようとします。TACACS+サーバに到達できない場合、スイッチはリストの次のサーバにパケットを送信しようとします。この場合にフェイルバックがないことに注意してください。最初の TACACS+サーバが再び到達可能にたった時でも、アカウンティングパケットは、第二の TACACS+サーバに送信され続けます。
例えば、認証がスイッチのローカルデータベース、または RADIUS サーバなどのいくつかの他のメカニズムを介して実行された場合、スイッチは最初の設定済みの TACACS+サーバにアカウンティングパケットを送信しようとします。そのサーバに到達できない場合、スイッチは設定された順序で後続のサーバにアカウンティングパケットを送信しようとします。

12.5.1 適合の条件

- ログインとコマンドアカウンティングのみサポートされています。システムイベントのアカウンティングはサポートされていません。
- 認証が RADIUS、TACACS+またはスイッチ-ローカルユーザデータベースを介して実行されるか否かに関わらず、アカウンティングのために TACACS+サーバを使用することができます。唯一の前提条件は、1 つまたは複数の TACACS+スイッチ上で構成されたサーバが存在することです。
- 認証が失敗した場合、アカウンティングを行うことができません。
- コマンドアカウンティングでは、不完全なタイムスタンプを持ったコマンドは、ログに記録することができません。たとえば、再起動オプションを指定して発行された、'firmware download'コマンドは、このコマンドの完了に使用可能なタイムスタンプがありませんので、記録されません。
- ログイン情報の Port は常に'tty0'と記録されます。
- ユーザーがログイン中に reload などでスイッチが再起動した場合、ログアウトイベントは記録されません。

12.5.2 クライアントでの TACACS+アカウンティング設定

デフォルトによるアカウンティングは、TACACS+クライアント（スイッチ）が無効になっており、明示的に機能を有効にする必要があります。コマンドアカウンティングの有効化と TACACS+クライアントでのログインアカウンティングの有効化は、2 つの異なる操作です。ログインおよびコマンドアカウンティングを有効化するには、少なくとも 1 つの TACACS+サーバを設定する必要があります。同様に、ログインまたはコマンドアカウンティングが有効になって、リスト内にある唯一のサーバである場合、TACACS+サーバを削除することはできません。

(1) ログインアカウンティングの有効化

次の手順は、アカウンティングが無効にされたサーバで、ログインアカウンティングを有効にします。

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。
2．ログインアカウンティングを有効化するには、'aaa accounting exec default start-stop tacacs+'コマンドを入力します。
3．設定を確認するには、'do show running-config aaa accounting'コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# aaa accounting exec default start-stop tacacs+
switch(config)# do show running-config aaa accounting
aaa accounting exec default start-stop tacacs+
aaa accounting commands default start-stop tacacs+
```

(2) コマンドアカウンティングの有効化

次の手順では、ログインアカウンティングが有効でコマンドアカウンティングが無効になっているス

イッチでログインアカウンティングを有効にします。

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。

2．ログインアカウンティングを有効化するには、'aaa accounting command default start-stop tacacs+'コマンドを入力します。

3．設定を確認するには、'do show running-config aaa accounting'コマンドを入力します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# aaa accounting command default start-stop tacacs+
switch(config)# show running-config aaa accounting
aaa accounting exec default start-stop
aaa accounting commands default start-stop tacacs+
```

(3) アカウンティングの無効化

アカウンティングをディセーブルにするには、'aaa accounting'コマンドで none オプションを使用する方法と、コマンドの no 形式を使用する方法の 2 つのオプションがあります。両方の設定方法は機能的に同等です。ログインアカウンティングとコマンドアカウンティングのため別々に無効化操作を実行する必要があります。操作は、グローバルコンフィギュレーションモードで実行します。

次の例は、コマンドアカウンティングを無効にする 2 つの方法を示します。コマンドは、グローバルコンフィギュレーションモードで実行します。

```
switch(config)# aaa accounting commands default start-stop none
switch(config)# no aaa accounting commands default start-stop
```

次の例では、ログインアカウンティングを無効にする 2 つの方法を示します。

```
switch(config)# aaa accounting exec default start-stop none
switch(config)# no aaa accounting exec default start-stop
```

12.5.3 TACACS+アカウンティングログの表示

次の TACACS +アカウンティングログの例は、コマンドやログインアカウンティングに対する典型的な成功例と失敗例を示します。これらの例は、フリーの TACACS+サーバで取得しました。属性の順序は、サーバパッケージに依存して変わることがありますが、値は同じです。アカウンティングログの格納場所は、サーバの構成によって異なります。

(1) コマンドアカウンティング

次のレコードは、admin ユーザーによる'username'コマンドの実行が成功したことを示しています。

```
<102> 2012-04-09 15:21:43 4/9/2012 3:21:43 PM NAS_IP=10.17.37.150 Port=0
rem_addr=Console User=admin Flags=Stop task_id=1 timezone=Etc/GMT+0 service=shell
priv-lvl=0 Cmd=username Stop_time=Mon Apr 9 09:43:56 2012
```

```
Status=Succeeded
```

次のレコードが、無効なホスト名またはサーバの IP アドレスが原因で、admin ユーザーによる 'radius-server'コマンドの実行が失敗したことを示しています。

```
<102> 2012-04-09 14:19:42 4/9/2012 2:19:42 PM NAS_IP=10.17.37.150 Port=0
rem_addr=Console User=admin Flags=Stop task_id=1 timezone=Etc/GMT+0 service=shell
priv-lvl=0 Cmd=radius-server Stop_time=Mon Apr 9 08:41:56 2012
 Status=%% Error: Invalid host name or IP address
```

(2) ログイン(EXEC)アカウンティング

次のレコードは、トライアルユーザのログイン成功を示しています。

```
<102> 2012-05-14 11:47:49 5/14/2012 11:47:49 AM NAS_IP=10.17.46.42
Port=/dev/tty0 rem_addr=Console User=trial Flags=Start task_id=1
timezone=Asia/Kolkata service=shell
```

次のレコードは、成功したトライアルユーザのログアウトを示しています。

```
<102>2012-05-14 11:49:52 5/14/2012 11:49:52 AM NAS_IP=10.17.46.42 Port=/dev/ttyS0
rem_addr=console User=trial Flags=Stop task_id=1 timezone=Asia/Kolkata
service=shell elapsed_time=123 reason=admin reset
```

12.5.4 ファームウェアのダウングレードに関する注意事項

TACACS +アカウンティングをサポートしていないバージョンにダウングレードする前に、ログインとコマンドアカウンティングを無効にするか、またはファームウェアダウンロードが適切なエラーメッセージと共に失敗するでしょう。

12.6 TACACS+サーバ側の設定

インストールと設定のステップバイステップの手順は、www.cisco.com から入手することができます。ネットワーク環境の設定する前に、システム管理者またはネットワーク管理者に相談してください。

12.6.1 ユーザーアカウントの管理

TACACS+サーバを使用すると、内蔵 DCB スイッチで作成されたアカウント名ではなく、真のネットワーク全体のアイデンティティでユーザーアカウントを設定する必要があります。各アカウント名と一緒に、適切なスイッチアクセスロールを割り当てる必要があります。ユーザーアカウントは、同時にスイッチのユーザー名と同じ名前で TACACS+サーバに存在できます。

TACACS+サーバを設定するスイッチにログインする際プロンプトが表示されたときに、ユーザーは割り当てられた TACACS+アカウント名とパスワードを入力します。一旦、TACACS+サーバがユーザーを認証すると、Brocade Vendor-Specific Attribute（VSA）を使っているユーザーアカウント情報と関連付

けられたスイッチロールと情報で応答します。ロールの割り当てがなくても、認証受け付け応答は自動的に"user"ロールを付与します。
ユーザーアカウント、プロトコルのパスワード、および関連の設定は、サーバコンフィグレーションファイルを編集することによって設定されます。次の設定例は、そのTACACS+デーモンユーザ向けに、Cisco 社が提供している資料に基づいています。

12.6.2 ユーザーアカウントの設定

次の例では、ユーザー"Mary" CHAP または PAP プロトコルが使用されているかどうかに応じて、"vlanadmin"と異なるパスワードの Brocade ロールを割り当てます。次の例では、brcd-role 属性は必須で Brocade-only 環境で動作します。混合ベンダ環境では、brcd-role 属性をほとんどのオプションに設定する必要があります。詳細については、144 ページの『12.6.7 混在ベンダ環境のための TACACS+の設定』を参照してください。

```
user = Mary {
chap = cleartext "chap password"
pap = cleartext "pap password"
service = exec {
brcd-role = vlanadmin;
}
}
```

次の例では、ユーザー"Agnes"に、ログイン認証のすべてのタイプのための単一パスワードを割り当てます。

```
user = Agnes {
global = cleartext "Agnes global password"
}
```

次の例では、ユーザーが/etc/passwd ファイルを使用して認証することができるようにアカウントを設定します。

```
user = fred {
login = file /etc/passwd
}
```

12.6.3 TACACS+アカウントパスワードの変更

TACACS+ユーザーのためのパスワードの変更は、TACACS+サーバコンフィグレーションファイルの編集によって、サーバ上で行われます。

12.6.4 アカウント有効期限の設定

TACACS+サーバコンフィグレーションファイルの "expires"属性を使用して、アカウントの有効期限を

設定することができます。有効期限は、 "MMM DD YYYY"の形式で保持します。

```
user = Brocade {
member = admin
expires = "Jan 1 2011"
pap = cleartext "pap password"
}
```

12.6.5 TACACS+サーバキー

TACACS+サーバキーは、内蔵 DCB スイッチと TACACS+サーバ間で交換されるメッセージを保護するために使用される共有秘密鍵です。TACACS+サーバキーは、TACACS+サーバとクライアント（内蔵 DCB スイッチ）の両方で設定する必要があります。1 つだけのキーは TACACS+サーバコンフィグレーションファイル内にサーバごとに定義されます。キーの定義は次のとおりです。

```
key = "vcs shared secret"
```

12.6.6 TACACS+グループの定義

TACACS+グループまたはロールは、ユーザーと同じ属性を含めることができます。グループのすべての属性は、グループが割り当てられている任意のユーザーに割り当てることができるでしょう。TACACS+グループは、Brocade ロール概念と機能的に類似していますが、"brcd-role"属性の値とは関係がありません。

次の例では、TACACS +グループを定義します。

```
group = admin {
# group admin has a cleartext password which all members share
# unless they have their own password defined
chap = cleartext “my$parent$chap$password”
}
```

次の例では、ユーザー "Brocade"にグループ"admin"を割り当てます。

```
user = Brocade {
member = admin
pap = cleartext "pap password"
}
```

12.6.7 混在ベンダ環境のための TACACS+の設定

認証されたユーザーによってシステムオブジェクトへのアクセスを認可するために、Network OS は、Role Based Access Control（RBAC）を使用しています。AAA 環境では、ユーザーは Brocade と非 Brocade のプラットホーム間で許可される必要があるかもしれません。集中化した AAA サービスを複数の Network Access Servers（NAS）またはクライアントに提供するために、TACACS+を使うことができます。マルチベンダ環境で TACACS+サービスを利用するために、例で示すようにオプションの

Attribute-Value Pair（AVP）引数を設定する必要があります。

```
brcd-role*admin
```

Network OS デバイスが TACACS+サービスへの許可要求にオプションの引数 'brcd-role が'を送信します。ほとんどの TACACS+サーバは、認証要求の応答として、同じ引数を返すようにプログラムされています。もし、'brcd-role'がオプションの引数として設定されていると、それが認証要求に含まれて送信され、Network OS ユーザーは、混合ベンダ環境で正常にすべての TACACS+サービスで認証することができます。

(1) tac_plus でオプション引数の設定

以下は tac_plus パッケージ用の具体的な例です。他のパッケージの Syntac は異なる場合があります。この例では、必須属性の PRIV-lvl=15 は、Cisco が認証を許可するように設定されています。オプションの brcd-role=admin の引数は、tac_plus.conf ファイルに加えられて、認証する内蔵 DCB スイッチを許可します。

次の例では、オプションの属性値ペア、role = admin を持つユーザーを設定します。Brocade ユーザーが正常に認証するためのユーザー名とユーザーグループの両方に一致させる必要があります。

```
user = <username> {
      default service = permit
      service = exec {
         priv-lvl=15
   optional brcd-role = admin
   }
}
Or
group = <usergroup> {
      default service = permit
      service = exec {
         priv-lvl=15
         optional brcd-role = admin
   }
}
user = <username> {
   Member = <usergroup>
   }
```

13 エッジループ検出の管理

13.1 エッジループ検出の概要

Edge-loop detection（ELD）は、ブロードキャストストームを引き起こす 2 つのループを検出してレイヤを無効にします。通常、これらのループは設定ミスによって引き起こされます。
ELD は、Brocade VCS ファブリッククラスタ上で構成され有効にできます。二つ以上の Brocade VCS ファブリッククラスタを含む任意のトポロジで、レイヤ 2 ループを検出しブロードキャストストームを防ぐため ELD を利用できます。スタンドアロンスイッチも、クラスタに含めることができますが、ループの検出は、Brocade VCS ファブリッククラスタ上で働き、スタンドアロンスイッチ上で動作するわけではありません。スタンドアロンスイッチで構成されるネットワークでは、ELD を使用することができません。

具体的には、次のトポロジでレイヤ 2 ループに起因するブロードキャストストームを防止するため、ELD を使用することができます：

- スタンドアロンスイッチに接続した Brocade VCS ファブリッククラスタ
- 複数のノードのネットワークに接続した Brocade VCS ファブリッククラスタ。
- 他の Brocade VCS ファブリッククラスタに接続した Brocade VCS ファブリッククラスタ。

図 13-1 は、レイヤ 2 ループが発生する可能性がある Brocade VCS ファブリッククラスタとスタンドアロンスイッチ間の誤った構成例を示しています。このケースでは、Brocade VCS ファブリッククラスタをスタンドアロンスイッチに接続する 2 つの ISL に対して、Brocade VCS ファブリッククラスタのエッジデバイス上に VLAG が構成されています。このケースでは、ISL の接続先であるスタンドアロンスイッチ上に LAG が作成されていません。ELD は、この潜在的なレイヤ 2 ループを検出し、切断します。

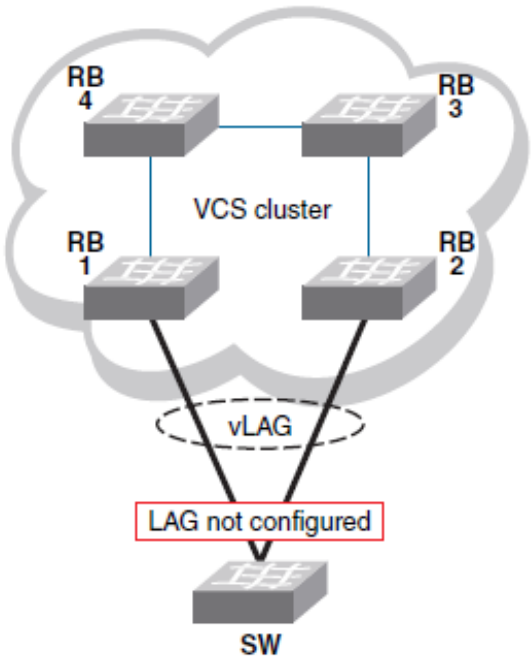

図 13-1 LAG を失ったことが原因のループ

図 13-2 は、ELD がレイヤ 2 ループを検出し、切断できる別の例を示します。このケースでは、レイヤ 2 ループを生み出す構成で複数の Brocade VCS ファブリッククラスタが相互接続されています。

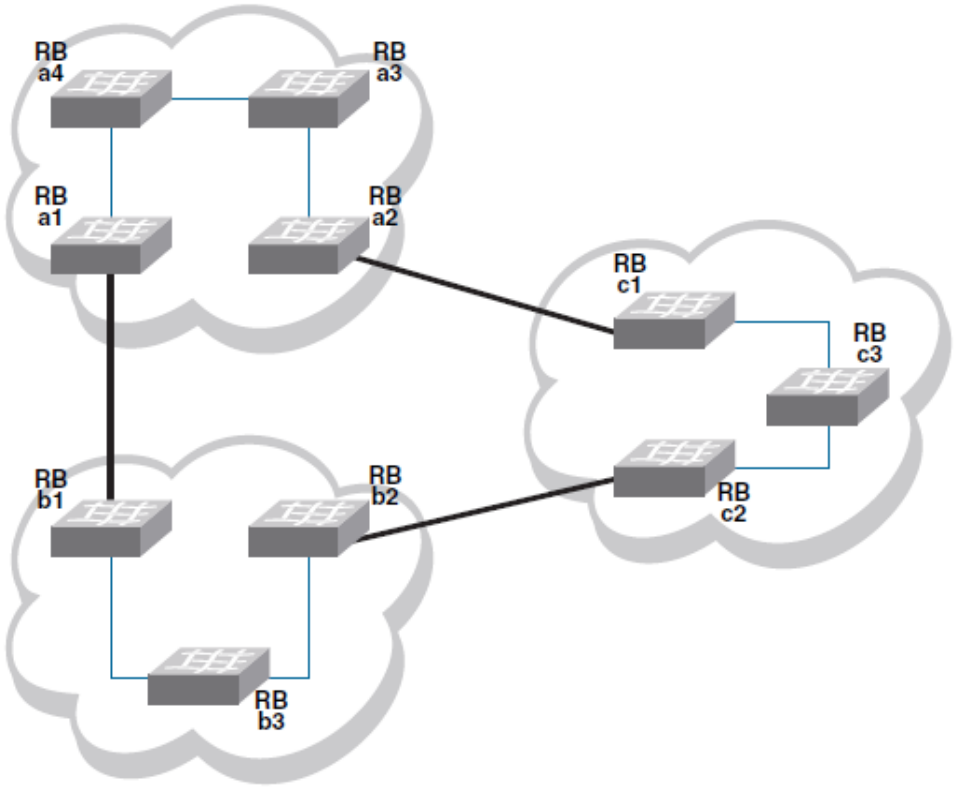

図 13-2 相互接続した Brocade VCS ファブリッククラスタが原因となるループ

NOTE

エッジループが発生した場合、VCS ファブリッククラスタ内で共用する MAC アドレステーブルに不整

合が発生する場合があります。ループ発生時は、いずれかひとつの Rbridge で’clear mac-address-table dynamic’ を必ず実行して MAC アドレステーブルが正常に同期するまでお待ち下さい。

13.2　ELD がループを検出する方法

ELD は、エッジポート上の Multicasting Protocol Data Unit（PDU）パケットによって動作します。ELD が送信する PDU を受けると、デバイスはループを認識します。デバイスは、レイヤ 2 ループが存在することを認識すると、そのポートを無効にし、レイヤ 2 ループを切断することができます。

無効なポートの数を最小限に抑えるには、ELD は、各ポートに優先順位と各々の Brocade VCS ファブリッククラスタに固有の受信制限（pdu-rx-limit）を割り当てます。ポートプライオリティは、クラスタの送信または受信エッジポートが無効になっているかどうかを決定します。pdu-rx-limit は、アクションが行われる Brocade VCS ファブリック上で決定します。これらの設定されなければ、レイヤ 2 ループが同時に複数のクラスタ内で検出される可能性があります。その結果、複数のポートが無効になり、Brocade VCS ファブリッククラスタ間トラフィックが停止します。

図 13-3 は、147 ページの図 13-2 と同様の相互接続を示していますが、ELD は、各エッジポート上で有効なっておりポートプライオリティと pdu-rx-limit が割り当てられています。

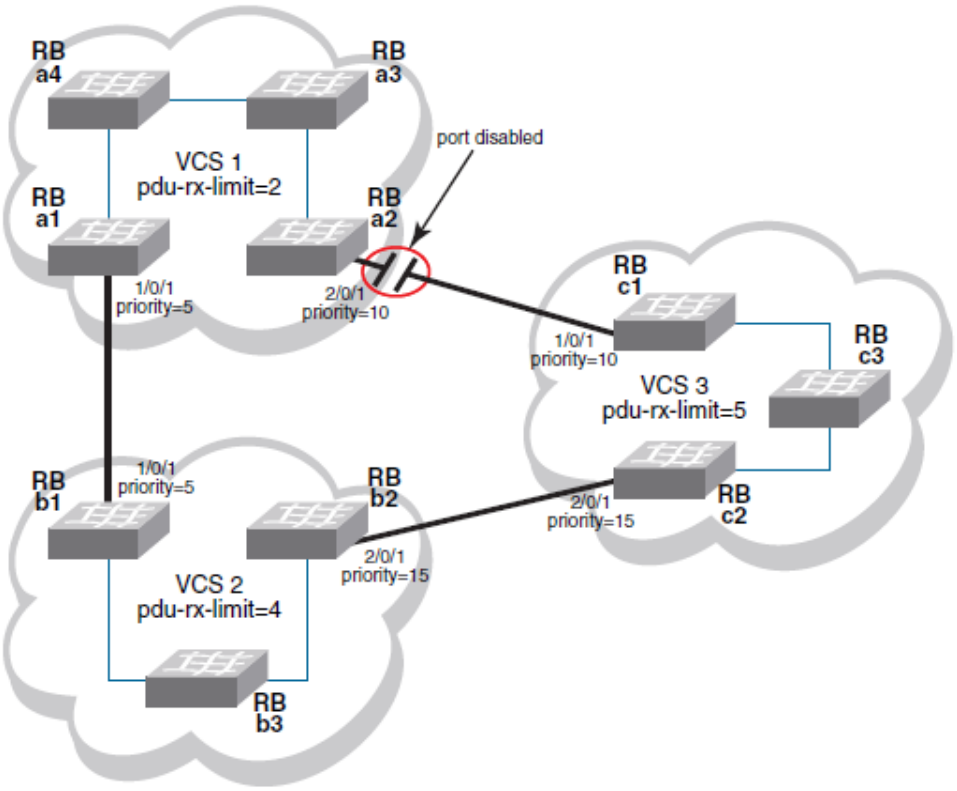

図 13-3 ELD が有効な相互接続の Brocade VCS ファブリッククラスタ

すべて ELD 有効エッジポートが同じ速度で PDU を送信すると、VCS1 は最初に pdu-rx-limit に到達します。ポート 2/0/1、ポート 1/0/1 よりも低い優先順位（優先順位の高い番号）を持っているため、無効にすることが選択されています。両方のポートが同じプライオリティの場合、ポート ID が高いポートが無効にされます。
ELD によってシャットダウンされたポートが LAG の一部である場合、LAG のすべてのメンバポートもシャットダウンされます。シャットダウンされたポートが VLAG の一部である場合は、その RBridge 上の VLAG のすべてのメンバポートもシャットダウンされます。
ELD は、ポートを無効にすると、任意の設定ミスが修復されるまで、ポートの通常の動作は、無効のままです。修復が完了すると、ポートを手動で再度有効にする必要があります。

NOTE
ELD がポートを無効にすると、ポートは運用上のステータスはダウンですあるが、管理上のステータスはアップです。ポートが STP またはいくつかの他の L2 プロトコルによって無効にされている場合、ELD はそのポートに対して PDU を処理しません。

13.3　エッジループ検出の設定

エッジループの検出は、グローバルレベルおよびインタフェースレベルで設定を行う必要があります。グローバルレベルの設定に対して、Brocade VCS ファブリッククラスタはループが存在していることを判定する前に、任意のポート上で受信する PDU の数を設定する必要があります。この値が、pdu-rx-limit です。また、'hello-interval'コマンドを使用して PDU を送信する間隔を設定しなければなりません。pdu-rx-limit および、hello インターバルタイマの組み合わせは、ELD がレイヤ 2 ループを検出し、切断するのに要する時間を決定します。
インタフェースレベルでは、ポートプライオリティを設定したい各ポートで ELD を有効にする必要があります。また、ELD を有効にする VLAN を指定する必要があります。
ひとつの Brocade VCS ファブリッククラスタのみがポートを無効できるように、各 Brocade VCS ファブリッククラスタに異なる数値を制限に設定するには、'pdu-rx-limit'コマンドを入力します。隣接した２つの Brocade VCS ファブリッククラスタ上のポートが無効となる競合状態を防ぐために 2 増加させた値で設定することをお勧めします。
PDU 間の間隔を設定するには、'hello-interval'コマンドを入力します。この間隔は ELD が構成されているすべての Brocade VCS ファブリック･クラスタ上で同じ値に設定する必要があり、そうでなければ、エッジループ検出の結果が予測不能になります。
必要に応じて、10 分～24 時間の間で指定した期間の経過後に、ポートを再度有効にするように設定するには、'shutdown-time'コマンドを入力します。この機能の典型的な使い方は、テスト環境のようにネットワークの再構成が一般的な環境においてです。典型的な使い方はデフォルト値のゼロのままでの使用であり、ポートが自動的に再度有効にすることを許可しません。

NOTE
'shutdown-time'への変更は、設定の変更後 ELD によって無効にされたポートに対してのみ有効です。'shutdown-time'の変更前に、ELD によって既に無効になっていたすべてのポートは、変更前の'shutdown-time'の値のままです。これらのポートは、現在実行中のタイマーが切れると、ELD は再度ループを検出し、ポートをシャットダウンした後、新しい'shutdown-time'時間に従い動作します。

ELD が実行されているインタフェースごとに、ELD を有効にするには、'edge-loop-detection vlan'コマンドを入力します。また、ポートプライオリティを指定するには、'edge-loop-detection port-priority'コマンドを入力します。

13.3.1 Brocade VCS ファブリッククラスタのためのグローバル ELD パラメータの設定

ELD を構成する Brocade VCS ファブリッククラスタの上で、この手順を実行してください。

1. Brocade VCS ファブリッククラスタ内の任意のスイッチにログインします。
2. グローバルコンフィギュレーションモードで、エッジループ検出コンフィギュレーションモードを開始するには、'protocol edge-loop-detection'コマンドを入力します。
3. レイヤ 2 ループを切断する前に受信された PDU の数を設定するには、'pdu-rx-limit *number*'コマンドを入力します。
   number オペランドは、1 から 5 の値でなければなりません。デフォルト値は 1 です。
4. PDU 間の間隔を設定するには、'hello-interval number'コマンドを入力します。
   number オペランドは、1 ミリ秒の単位を持っています。*number* オペランドの範囲は、100 ミリ秒から 5000 ミリ秒でなければなりません。デフォルト値は 1000 ミリ秒です。
5. シャットダウンポートが再度有効になった後の時間を分単位で設定するには、 'shutdown-time *number*'コマンドを入力します。
   number オペランドは、10 から 1440（10 分から 24 時間）までの範囲でなければなりません。デフォルト値は、0 でポートが自動的に再有効化されないことを示します。

例：この例では、5 つの PDU の受領の上でループを検出し、切断する Brocade VCS ファブリッククラスタを設定します。PDU の間隔は 2000 ミリ秒（2 秒）に設定されているため、任意のループは 10 秒後に中断されます。選ばれたポートは、ループ検出が自動的に再有効化された後、24 時間は無効のままです。

```
(config)# protocol edge-loop-detection
(config-eld)# pdu-rx-limit 5
(config-eld)# hello-interval 2000
(config-eld)# shutdown-time 1440
```

13.3.2 ポートでのインターフェースパラメータの設定

ELD で監視したいすべてのポートに対して、この手順を実行します。

1．Brocade VCS ファブリッククラスタ内の任意のスイッチにログインします。
2．グローバルコンフィギュレーションモードで、エッジループの検出を有効にする RBridge/スロット/ポートを選択するには、interface コマンドを入力します。
3．インターフェースコンフィギュレーションモードで、ELD がこのポート上で監視する VLAN を指定するには、'edge-loop-detection vlan'コマンドを入力します。
VLAN を指定しない場合、コマンドは失敗します。
4．選択した VLAN の指定されたポートの ELD ポート優先度を指定するには、'edge-loop-detection port-priority'コマンドを入力します。しかし、スイッチングを可能にすることは、ポートプライオリティを割り当てるための必須条件ではありません。

NOTE
優先順位の値の範囲は 0 から 255 までです。優先順位 0 のポートは、このポートのシャットダウンが無効になっていることを意味します。デフォルト値のポートプライオリティは 128 です。

例：この例では、ポート 1/0/7 VLAN 10 およびポート 4/0/6 VLAN 10 の 2 つのポート/ VLAN ペアに ELD ポートプライオリティを設定します。これらのポートの両方が同じループで検出される場合、Brocade VCS ファブリッククラスタに対する pdu-rx-limit に到達すると、ELD は、ポート 4/0/6 をシャットダウンします。それが次にプライオリティのより低い（より大きい番号）ポート 1/0/7 を割り当てられているため、ポート 4/0/6 がシャットダウンに選択されます。

```
(config)# interface TenGigabitEthernet 1/0/7
(conf-if-te-1/0/7)# edge-loop-detection vlan 10
(conf-if-te-1/0/7)# edge-loop-detection port-priority 5
(conf-if-te-1/0/7)# top
(config)# interface TenGigabitEthernet 4/0/6
(conf-if-te-4/0/6)# edge-loop-detection vlan 10
(conf-if-te-4/0/6)# edge-loop-detection port-priority 7
```

13.4　エッジループのトラブルシューティング

誤った設定を表示し、修正するために'edge-loop detection'コマンドを使用します。
1．Brocade VCS ファブリッククラスタ内の任意のスイッチにログインします。
2．グローバルコンフィギュレーションモードで、Brocade VCS ファブリッククラスタのエッジループ検知の統計情報を表示するには、'show edge-loop-detection'コマンドを入力します。
コマンド出力には、ELD でディセーブルとなったポートを示しています。
3．手順 2 で検出されたすべての設定の誤りを修正してください。
4．グローバルコンフィギュレーションモードで次のいずれかの操作を実行します。
・ELD によって無効にされた 1 つのポートを再可能にします。
- ELD によって無効にされたポートで、'shutdown'コマンドを入力します。
- ELD によって無効にされたポートで、'no shutdown'コマンドを入力します。

NOTE
リモートポートの VCS ID が変更され、エッジポートが ISL ポートになった場合、既に ELD によってシャットダウンされたポートは、ISL ポートとして検出させるためには、'shutdown'コマンド入力後'no shutdown'コマンドを使用する必要があります。

・再度有効に ELD では無効になってすべてのポートは、'clear edge-loop-detection'コマンドを入力します。

14 AMPP の設定

14.1 AMPP 概要

サーバ仮想化インフラは、サーバ側の Virtual Ethernet Bridge (VEB)ポートプロファイルを、VEB ポートを介してネットワークにアクセスする Virtual Machine (VM)が使用するイーサネット MAC アドレスに関連付けています。
VM がある物理サーバから別のサーバにマイグレーションすると、VM に関連付けられたサーバの VEB ポートの自動的なポートプロファイルマイグレーションを提供することで、VEB ポートプロファイルは VM にあわせてマイグレーションします。
サーバ仮想化インフラが十分な制御を提供する環境では、ポートプロファイルが自動的にマイグレーションするアプローチは優れています。そのような環境の例は、ファイやウォールやセキュリティアプライアンスを介して外部ネットワークから分離されたレイヤ２ネットワークを使う高性能クラスタになります。
しかしながら、外部のレイヤ２スイッチでサポートされるアクセス制御及び QoS とサーバ仮想化インフラの間にはギャップがあります。外部のレイヤ２スイッチはサーバの VEB の実装に比べて、高度な制御機能を持っています。
幾つかの環境では、外部のネットワークスイッチで提供される更に高度な制御を必要とします。その例としては、異なる最新のネットワーク制御のもと、同じレイヤ２ネットワークの上で各種アプリケーションが動作するような多階層のデータセンタです。この種の環境では、ネットワーク管理者は外部ネットワークスイッチで利用可能な高度なアクセス制御を使うことを好みます。
レイヤ２ネットワークは、エンドポイントデバイスが一つのスイッチから別のスイッチに移動するとき、そのデバイスに関連したスイッチのアクセス制御及びトラフィック制御を自動的に移動するメカニズムを持っていません。マイグレーションは、例えばあるシステムのベアメタル OS で動作していて別のシステムに移動する(アプリケーション、ミドルウェア、OS 及び状態を意味する)OS イメージのような、物理的なものかもしれません。または、マイグレーションは、あるシステム上の VMware 上で動作していて、別のシステムの VMware で移動する OS イメージのように、仮想的なものかもしれません。
Brocade Auto Migrating Port Profile (AMPP)機能は、VM が物理サーバ間を移動するとき、ポートプロファイルの関係付けを管理や移動に対応して高度な制御を提供します。

14.1.1 AMPP over vLAG

Virtual Link Aggregation Group (vLAG)は、1 つまたは複数の物理スイッチまたはサーバに接続することができる Brocade VCS ファブリックとのリンクを示す Brocade 独自の LAG の名前です。冗長性と高い帯域幅のために、vLAG は、Brocade VCS ファブリック技術の重要なコンポーネントです。AMPP は、物理ポートと同様に vLAG と標準 LAG でもサポートされています。

vLAG の詳細については、205 ページの『17 リンクアグリゲーションの設定』を参照してください。
次の例の下線付きのテキストは、ポートプロファイルの vLAG 情報であること示しています。

```
switch# show port-profile status
Port-Profile                PPID     Activated    Associated MAC    Interface
auto-dvPortGroup             1        Yes         None              None
auto-dvPortGroup2            2        Yes         None              None
auto-dvPortGroup3            3        Yes         None              None
auto-dvPortGroup_4_0         4        Yes         0050.567e.98b0    None
auto-dvPortGroup_vlag        5        Yes         0050.5678.eaed    None
auto-for_iscsi               6        Yes         0050.5673.85f9    None
                                                  0050.5673.fc6d    None
                                                  0050.5674.f772    None
                                                  0050.5675.d6e0    Te 234/0/54
                                                  0050.567a.4288    None
auto-VM_Network              9        Yes         000c.2915.4bdc    None
                                                  0050.56a0.000d    None
                                                  0050.56a0.000e    None
                                                  0050.56a0.000f    None
                                                  0050.56a0.0010    Po 53
                                                  0050.56a0.0011    Po 53
                                                  0050.56a0.0012    Po 53
                                                  0050.56a0.0013    None
                                                  0050.56a0.0025    None
                                                  0050.56a0.0026    None
                                                  0050.56a0.0027    None
                                                  0050.56a0.0028    None
                                                  0050.56a0.0029    Po 53
                                                  0050.56a0.002a    Po 53
                                                  0050.56a0.002b    Po 53
                                                  0050.56a0.002c    None
                                                  0050.56a0.002d    None
                                                  0050.56a0.002e    None
                                                  0050.56a0.002f    None
                                                  0050.56b3.0001    Po 53
                                                  0050.56b3.0002    Po 53
                                                  0050.56b3.0004    Po 53
                                                  0050.56b3.0005    None
auto-VM_kernel               10       Yes         0050.5671.4d06    None
```

```
                                                0050.5672.862f    Po 53
                                                0050.5678.37ea    None
                                                0050.567a.ddc3    None
auto-VM_NW_1G                 11       Yes          0050.56b3.0000    None
                                                0050.56b3.0003    Po 82
                                                0050.56b3.0007    None
                                                0050.56b3.0008    Po 82
                                                0050.56b3.0009    Po 82
auto-VMkernel                 12       Yes          0050.567a.fdcf    Po 82
                                                0050.567c.c2e3    None
auto-VMkernel_VS              13       Yes          0050.567d.16b9    None
                                                0050.567e.e25b    None
auto-Management+Network       14       Yes          5cf3.fc4d.ca88    None
auto-Virtual+Machine+Network  15       Yes          000c.2941.27e2    None
                                                000c.2980.335d    None


switch# show port-profile int all
Interface      Port-Profile
Gi 234/0/1     None
Gi 234/0/13    None
Gi 234/0/25    None
Gi 234/0/26    None
Te 234/0/54    auto-for_iscsi
Po 82          auto-VM_NW_1G
               auto-VMkernel
Po 53          auto-VM_Network
               auto-VM_kernel
```

14.1.2 AMPP とスイッチドポートアナライザー

Switched Port Analyzer（SPAN）、またはポートミラーリングは、ネットワークアナライザによる分析のためのネットワークトラフィックを指定します。特定のポートを通過するトラフィックを観測したりスヌーピングしたい場合、人為的にアナライザに接続されたポートにパケットをコピーするため、ポートをミラーリングする必要があります。

AMPP でのポートミラーリングは、プロファイリングポートとしてミラーポートを使うために必要な機能を提供しています。プロファイルポートを宛先ポートとして、またその逆に設定することはできません。SPAN は、プロファイルポートで学習されたトラフィックをミラーリングすることができます。

SPAN の詳細については、277 ページの『24 スイッチドポートアナライザ(SPAN)設定』を参照してください。

14.1.3 スケーラビリティ

表 14-1 は、Network OS v3.0.0 でサポートされているスケーラビリティ値を示します。

表 14-1　AMPP スケーラビリティ値

測定基準	スタンドアロンモード	ファブリッククラスタモード
プロファイル数	256	256
ポートプロファイル内の VLAN 数	2000	2000
QoS プロファイル	1 cee-map 1 mutation-map	1 cee-map 1 mutation-map
セキュリティプロファイル内の ACLs 数	レイヤ 2 ACL と同じ	レイヤ 2 ACL と同じ
MAC 関連付け数	8000	8000

表 14-1 の MAC と VLAN スケーリング数は、MAC 関連付けと vlan プロフィールスケーリングに基づいています。さらに、AMPP は、スイッチでサポートされている vLAG と LAG の最大数に従います。このケースでは、256 です。

14.2　AMPP ポートプロファイルの構成

図 14-1 に示す通り、デフォルトのポートプロファイルには、LAN および SAN へのアクセスを取得するために VM に必要な全体の構成が含まれています。

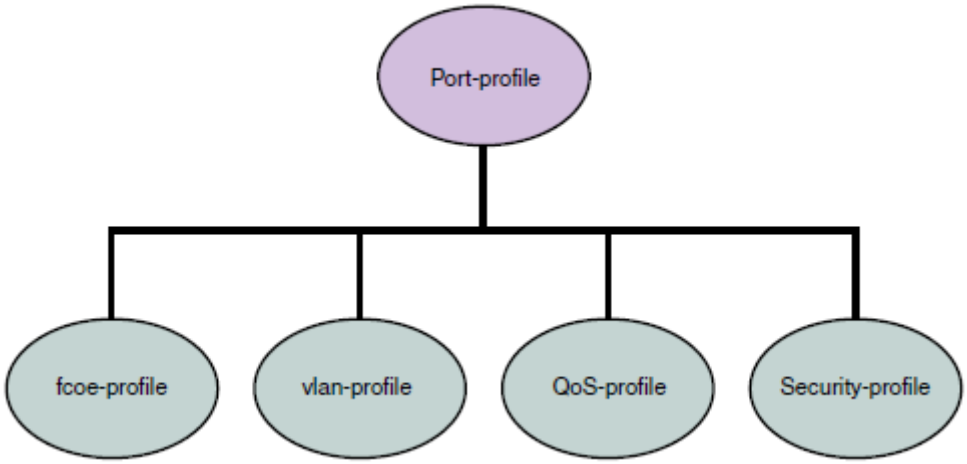

図 14-1 ポートプロファイルの内容

NOTE

ポートプロファイルは、LLDP や SPAN や LAG などの幾つかのインタフェースレベルのコンフィグレーションは含みません。

ポートプロファイルは、自己完結のコンフィグレーションコンテナとして動作します。言い換えれば、もしポートプロファイルが何も設定されていない新しいスイッチに提供された場合、インタフェースのローカル設定を構成し、トラフィックを通し始めることが可能となるということです。ポリシーに

対するどのような変更もデータプレーンへ即座に適用されます。
セキュリティプロファイルは、プロファイルまたは PolicyID に基づく ACL に適用されます。したがって、複数のセキュリティプロファイルを同じプロファイル化されたポートに適用することができます。しかし、一旦ポートプロファイルを有効にするとポートプロファイルの編集は出来ません。ポートへプロファイルを適用する場合は、ポートプロファイルの有効化が必須です。

14.2.1 ポートプロファイルの状態

生成中のポートプロファイルは、多数の状態に遷移します。ポートプロファイルの状態は下記の通りです。

- Created - この状態は、ポートプロファイルが作成・修正されたが、完成してない状態を示します。
- Activated - この状態は、ポートプロファイルが有効化されて、MAC とポートプロファイルの関連が有効になっている状態です。もし、作成されたポートプロファイルが完成せず有効化できない場合は、あらゆる競合や依存関係を解決し、ポートプロファイルを再度有効化する必要があります。
- Associated - この状態は、ファブリック内で一つ以上の MAC アドレスがこのポートプロファイルと関連付けられている状態です。
- Applied - この状態は、ポートプロファイルが MAC アドレスと関連付けられた profiled ポートに適用された状態です。なんのプロトコルも動作してない状態では、関連付けられた MAC アドレスがプロファイルポートに現れないかを検出するためシステムはパケットを覗き見します。２つの異なるポートプロファイル構成は、ひとつのプロファイルポートに共存できます。しかし、競合があると後から適用されるポートプロファイルが適用失敗となります。

表 14-2 に、AMPP イベントおよび該当障害の動作について説明します。

表 14-2　AMPP の動作および障害の説明

AMPP イベント	該当する動作と障害内容
Create port-profile	•ポートプロファイルが存在しない場合、新たに生成されます。存在していて有効化されてない場合、created となります。
Activate port-profile	•ポートプロファイルの構成が完全でなければ、有効化は失敗します。もし、ポートプロファイルが有効化されなければ、どのポートにも適用されません。 •すべての依存関係の検証が成功した場合、ポートプロファイルは ACTIVE 状態にあり、関連付けの可能な状態となります。 •VLAN プロファイルは、すべてのポートプロファイルのために必須です。
De-activate port-profile	•このイベントは全てのプロファイルポートの適用済みポートプロファイルの構成を削除します。 •ポートプロファイルに関連付けられた MAC アドレスがあっても無効化されます。
Modify port-profile	•ポートプロファイルは有効化される前だけ編集可能です。 •ポートプロファイルは、属性に競合があったり、依存関係が不完全ならば、INACTIVE 状態となります。 •ポートプロファイルは INACTIVE 状態となると、プロファイルの MAC アドレスへの関連付けはできません。
Associate MAC addresses to a port-profile	•別のポートプロファイルと既にマッピングされていると、MAC アドレスが複数のポートプロファイルへマッピングされません。 •マッピングされていない場合、ポートまたはスイッチの MAC アドレスに適用されるポートプロファイルに指定された全てのポリシーを MAC アドレスに許可するようにポートを構成します。
De-associate MAC addresses from a port-profile	•マッピングされている場合、特定の MAC アドレスに構成された全てのポリシーは、ポートもしくはスイッチから削除されます。
Deleting a port-profile	•ポートプロファイルが有効化状態ならば、IN USE エラーが発生します。AMPP は削除する前にプロファイルを強制的に無効化します。 •ポートプロファイルが有効化されている場合、プロファイルを削除すると全ての MAC との関係は削除されます。
Modifying port-profile content when in an associated state	•ポートプロファイルが既に有効化されている場合、IN USE エラーが発生します。
Moving the VM MAC and notifying the fabric	•ポートプロファイル ID に関連付けられた全てのポリシーが MAC アドレスにマッピングされ、ファブリックの新しいポートに適用されます。
Unused port-profile	•MAC との関連を削除するため、手動で MAC アドレスとのマッピングを削除しなければなりません。

14.2.2　新しいポートプロファイルの構成

VM MAC アドレス学習をサポートするため、デフォルトポートプロファイルが使用されます。デフォルトポートプロファイルは、他のユーザー定義の AMPP プロファイルとは異なります。

- ポートプロファイルＩＤ(ppid)を変更することは出来ません。
- VLAN サブプロファイルは修正できません。
- QoS サブプロファイルとセキュリティプロファイルは追加できません。
- デフォルトポートプロファイルは無効化できません。

要求に合わせるために新しいポートプロファイルを作成することを推奨します。新しいポートプロフ

ァイルを作成するために、特権実行モードで次の手順を実行してください。

1．物理インタフェースは、ポートプロファイルを作成する前に設定する必要があります。

2．新しいポートプロファイルの名称を作成・設定します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-profile vm1-port-profile
switch(config-port-profile-vm1-port-profile)# vlan-profile
switch(config-pp-vlan)# switchport trunk native-vlan 300
switch(config-pp-vlan)# switchport trunk allowed vlan add 300
```

3．VLAN プロファイルコンフィグレーションモードを終了します。

```
switch(confg-pp-vlan)# exit
```

4．プロファイルを有効化します。

```
switch(config)# port-profile vm1-port-profile activate
```

5．各ホストに対してプロファイルを MAC アドレスに関連付けます。

```
switch(config)# port-profile vm1-port-profile static 0050.56bf.0001
switch(config)# port-profile vm1-port-profile static 0050.56bf.0002
switch(config)# port-profile vm1-port-profile static 0050.56bf.0003
switch(config)# port-profile vm1-port-profile static 0050.56bf.0004
switch(config)# port-profile vm1-port-profile static 0050.56bf.0005
```

14.2.3 VLAN プロファイルの設定

VLAN プロファイルは、ポートプロファイル全体の VLAN 構成を定義します。それは、tagged と untagged VLAN の両方を含みます。

NOTE

Network OS v3.0.0 は VLAN classifier をサポートしていません。

VLAN プロファイルを設定するために、グローバルコンフィグレーションモードで次の手順を実行してください。

1．AMPP プロファイルは有効な間は修正できません。VLAN プロファイルを修正する前にポートプロファイルを無効化してください。

```
switch(config)# no port-profile vm1-port-profile activate
```

2．VLAN プロファイルコンフィグレーションモードに移行します。

```
switch(config)# port-profile vm1-port-profile
switch(config-port-profile-vm1-port-profile)# vlan-profile
```

3．モードをレイヤ２に変更しスイッチング特性をデフォルトに設定します。

```
switch(config-pp-vlan)# switchport
```

4．正しい VLAN に対して VLAN プロファイルモードにアクセスします。

```
switch(config-pp-vlan)# switchport access vlan 200
```

５．trunk コンフィグレーションモードに移行します。

```
switch(config-pp-vlan)# switchport mode trunk
```

６．allowed VLAN ID を指定して trunk モードを設定します。

```
switch(config-pp-vlan)# switchport trunk allowed vlan add 10, 20, 30-40
```

７．native VLAN にするため trunk モードを設定します。

```
switch(conf-pp-vlan)# switchport trunk native-vlan 300
```

８．VLAN プロファイルコンフィグレーションモードを終了します。

```
switch(conf-pp-vlan)# exit
```

９．プロファイルを有効化します。

```
switch(config)# port-profile vm1-port-profile activate
```

１０．プロファイルを MAC アドレスに関連付けます。

```
switch(config)# port-profile vm1-port-profile static 0050.56bf.0001
switch(config)# port-profile vm1-port-profile static 0050.56bf.0002
switch(config)# port-profile vm1-port-profile static 0050.56bf.0003
switch(config)# port-profile vm1-port-profile static 0050.56bf.0004
switch(config)# port-profile vm1-port-profile static 0050.56bf.0005
```

１１. 変更したいインタフェースのインターフェースコンフィギュレーションモードをアクティブにします。次の例は、スロット 0/ポート 0 の 10 ギガビットイーサネットインターフェース用のモードをアクティブにします。

```
switch(config)# interface tengigabitethernet 1/0/1
```

１２．物理インタフェース上でポートプロファイルポートを設定します。

```
switch(conf-if-te-1/0/1)# port-profile-port
switch(conf-if-te-1/0/1)#
```

14.2.4 QoS プロファイルの設定

QoS プロファイルは次の値を定義します。

- 入力の 802.1p プライオリティが内部のキュープライオリティに設定されます。ポートが QoS 非トラストモードの場合、全ての入力のプライオリティはデフォルトのベストエフォートプライオリティにマッピングされます。
- 入力のプライオリティが出力のプライオリティに設定されます。
- 入力プライオリティのマッピングが絶対優先または WRR トラフィッククラスに設定されます。
- 絶対優先または WRR トラフィッククラスでのフロー制御を有効化

QoS プロファイルは、CEE QoS とイーサネット QoS の２つの特色を持ちます。QoS プロファイルは CEE QoS かイーサネット QoS のいずれかを含みます。サーバ側のポートは、通常、コンバージドトラフィックを運んでいます。

QoS プロファイルを設定するため、グローバルコンフィグレーションモードで次の手順を実行します。

1．AMPP プロファイルは有効な間は修正できません。VLAN プロファイルを修正する前にポートプロファイルを無効化します。

```
switch(config)# no port-profile vm1-port-profile activate
```

2．QoS プロファイルモードに移行します。

```
switch(config)# port-profile vm1-port-profile
switch(config-port-profile-vm1-port-profile)# qos-profile
switch(config-qos-profile)#
```

3．CEE マップを適用します。

```
switch(config-qos-profile)# cee default
```

4．デフォルト CoS 値を設定します。

```
switch(config-qos-profile)# qos cos 7
```

5．CoS に対する QoS トラスト属性を設定します。

```
switch(config-qos-profile)# qos trust cos
```

6．プロファイルへのマップを適用します。以下のいずれかを行います。

- 存在する CoS-to-CoS ミューテイションマップを適用する

```
switch(config-qos-profile)# qos cos-mutation vm1-cos2cos-map
```

- 存在する CoS-to-Traffic クラスマップを適用する。

```
switch(config-qos-profile)# qos cos-traffic-class vm1-cos2traffic-map
```

7．以下のいずれかの Pause 機能を有効にします。

- PFC なし

```
switch(config-qos-profile)# qos flowcontrol tx on rx on
```

- 各 CoS 値に対する PFC 付

```
switch(config-qos-profile)# qos flowcontrol pfc 1 tx on rx on
switch(config-qos-profile)# qos flowcontrol pfc 2 tx on rx on
```

8．QoS プロファイルモードを終了します。

```
switch(config-qos-profile)# exit
```

9．プロファイルを有効化します。

```
switch(config)# port-profile vm1-port-profile activate
```

１０．プロファイルを MAC アドレスに関連付けます。

```
switch(config)# port-profile vm1-port-profile static 0050.56bf.0001
switch(config)# port-profile vm1-port-profile static 0050.56bf.0002
switch(config)# port-profile vm1-port-profile static 0050.56bf.0003
switch(config)# port-profile vm1-port-profile static 0050.56bf.0004
switch(config)# port-profile vm1-port-profile static 0050.56bf.0005
```

１１．変更したいインタフェースのインターフェースコンフィギュレーションモードをアクティブにします。次の例は、スロット 0/ポート 0 の 10 ギガビットイーサネットインターフェース用のモードをアクティブにします。

```
switch(config)# interface tengigabitethernet 1/0/1
```

１２．物理インタフェース上でポートプロファイルポートを設定します。

```
switch(conf-if-te-1/0/1)# port-profile-port
switch(conf-if-te-1/0/1)#
```

14.2.5 セキュリティプロファイルの設定

セキュリティプロファイルは、サーバが接続されたポートに必要な全てのセキュリティルールを定義します。典型的なセキュリティプロファイルは MAC ベースの標準または拡張 ACL の属性値を含みます。セキュリティプロファイルは、プロファイルまたは PolicyID に基づく ACL に適用されます。したがって、複数のセキュリティプロファイルを同じプロファイル対象のポートに適用することができます。セキュリティプロファイルを設定するため、グローバルコンフィグレーションモードで次の手順を実行します。

１．AMPP プロファイルは有効な間は修正できません。セキュリティプロファイルを修正する前にポートプロファイルを無効化します。

```
switch(config)# no port-profile vm1-port-profile activate
```

２．セキュリティポートプロファイルコンフィグレーションモードに移行します。

```
switch(config)# port-profile vm1-port-profile
switch(config-pp)# security-profile
switch(config-pp-security)#
```

３．ACL セキュリティ属性を修正します。

詳細は 231 ページの『20 アクセスコントロールリスト(ACL)の設定』を参照下さい。

４．セキュリティプロファイルに ACL を適用します。

```
switch(config-pp-security)# mac access-group vm1-acl in
```

５．セキュリティプロファイルコンフィグレーションモードを終了します。

```
switch(config-pp-security)# exit
```

６．プロファイルを有効化します。

```
switch(config)# port-profile vm1-port-profile activate
```

７．各ホストの MAC アドレスにプロファイルを関連付けます。

```
switch(config)# port-profile vm1-port-profile static 0050.56bf.0001
switch(config)# port-profile vm1-port-profile static 0050.56bf.0002
switch(config)# port-profile vm1-port-profile static 0050.56bf.0003
switch(config)# port-profile vm1-port-profile static 0050.56bf.0004
switch(config)# port-profile vm1-port-profile static 0050.56bf.0005
```

８．各ホストの MAC アドレスとプロファイルの関連付けを削除します。

```
switch(config)# no port-profile vm1-port-profile static 0050.56bf.0001
switch(config)# no port-profile vm1-port-profile static 0050.56bf.0002
switch(config)# no port-profile vm1-port-profile static 0050.56bf.0003
switch(config)# no port-profile vm1-port-profile static 0050.56bf.0004
switch(config)# no port-profile vm1-port-profile static 0050.56bf.0005
```

９. 変更したいインタフェースのインターフェースコンフィギュレーションモードをアクティブにし

ます。次の例は、スロット 0/ポート 0 の 10 ギガビットイーサネットインターフェース用のモードをアクティブにします。

```
switch(config)# interface tengigabitethernet 1/0/1
```

１０．物理インタフェース上でポートプロファイルポートを設定します。

```
switch(conf-if-te-1/0/1)# port-profile-port
switch(conf-if-te-1/0/1)#
```

14.2.6 ポートプロファイルポートの削除

ポートプロファイルポートを削除するには、グローバルコンフィギュレーションモードで次の手順を実行します。

1. 変更したいインタフェースのインターフェースコンフィギュレーションモードをアクティブにします。次の例は、スロット 0/ポート 0 の 10 ギガビットイーサネットインターフェース用のモードをアクティブにします。

```
switch(config)# interface tengigabitethernet 1/0/1
```

2．物理インタフェース上でポートプロファイルポートの設定を削除します。

```
switch(conf-if-te-1/0/1)# no port-profile-port
```

14.2.7 ポートプロファイルの削除

ポートプロファイルを削除するために特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#
```

2．ポートプロファイルを非アクティブにします。

```
switch(config)# no port-profile vm1-port-profile activate
switch(config)# no port-profile vm1-port-profile
```

3．カスタムプロファイルを削除するためポートプロファイルコマンドの'no'付を使います。デフォルトポートプロファイルは削除できません。

```
switch(config)# no port-profile vm1-port-profile
```

14.2.8 サブプロファイルの削除

サブプロファイルを削除するには、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#
```

2．ポートプロファイルを非アクティブにします。

```
switch(config)# no port-profile vm1-port-profile activate
```

3．ポートプロファイルモードに移行します。

```
switch(conf-vm1-port-profile)# port-profile vm1-port-profile
```

4．VLAN サブプロファイルを削除するには：

```
switch(conf-vm1-port-profile)# no vlan-profile
```

5．セキュリティサブプロファイルを削除するには：

```
switch(conf-vm1-port-profile)# no security-profile
```

6． QoS サブプロファイルを削除するには：

```
switch(conf-vm1-port-profile)# no qos-profile
```

14.3 AMPP プロファイルの監視

AMPP プロファイルを監視するには、特権実行モードで次の手順を実行します。

1．現在の MAC の詳細を表示するため、'show'コマンドを使います。

```
switch# show mac-address-table port-profile
Legend: Untagged(U), Tagged (T), Not Forwardable(NF) and Conflict(C)
VlanId   Mac-address      Type     State      Port-Profile     Ports
1       0050.5679.5351   Dynamic    Active     Profiled(U)      Te 111/0/10
1       0050.567b.7030   Dynamic    Active     Profiled(U)      Te 111/0/12
1       005a.8402.0000   Dynamic    Active     Profiled(T)      Te 111/0/24
1       005a.8402.0001   Dynamic    Active     Profiled(NF)     Te 111/0/24
1       005a.8402.0002   Dynamic    Active     Not Profiled     Te 111/0/24
1       005a.8402.0003   Dynamic    Active     Not Profiled     Te 111/0/24
1       005a.8402.0004   Dynamic    Active     Not Profiled     Te 111/0/24
1       005a.8402.0005   Dynamic    Active     Profiled(NF)     Te 111/0/24
1       005a.8402.0006   Dynamic    Active     Not Profiled     Te 111/0/24
1       005a.8402.0007   Dynamic    Active     Profiled(T)      Te 111/0/24
1       005b.8402.0001   Dynamic    Active     Profiled(T)      Te 111/0/24
1       005c.8402.0001   Dynamic    Active     Profiled(T)      Te 111/0/24
100     005a.8402.0000   Dynamic    Active     Profiled         Te 111/0/24
100     005a.8402.0001   Dynamic    Active     Profiled(NF)     Te 111/0/24
100     005a.8402.0003   Dynamic    Active     Not Profiled     Te 111/0/24
100     005a.8402.0005   Dynamic    Active     Profiled(NF)     Te 111/0/24
100     005a.8402.0007   Dynamic    Active     Profiled         Te 111/0/24
Total MAC addresses : 17
```

2．全ての利用可能なポートプロファイル設定を表示するため、'show running-config'を使います。

```
switch# show running-config port-profile
port-profile default
 vlan-profile
  switchport
  switchport mode trunk
```

```
 switchport trunk allowed vlan all
!
!
port-profile vm_kernel
 vlan-profile
  switchport
  switchport mode access
  switchport access vlan 1
```

3．現在のポートプロファイル設定を表示するため、'show port-profile'コマンドを使います。

```
switch# show port-profile
port-profile default
ppid 0
 vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
  port-profile vm_kernel
  ppid 1
 vlan-profile
  switchport
  switchport mode access
  switchport access vlan 1
```

4．現在の全ての AMPP プロファイルの状態を表示するために、'show port-profile status'コマンドを使います。

```
switch# show port-profile status applied
Port-Profile          PPID       Activated    Associated MAC   Interface
auto-for_iscsi         6         Yes         0050.5675.d6e0   Te 9/0/54
auto-VM_Network        9         Yes          0050.56b3.0001   Te 9/0/53
                                              0050.56b3.0002   Te 9/0/53
                                              0050.56b3.0004   Te 9/0/53
                                              0050.56b3.0014   Te 9/0/53
switch# show port-profile status activated
Port-Profile          PPID       Activated    Associated MAC   Interface
auto-dvPortGroup       1         Yes         None            None
auto-dvPortGroup2      2         Yes         None            None
auto-dvPortGroup3      3         Yes         None            None
auto-dvPortGroup_4_0    4         Yes         0050.567e.98b0   None
auto-dvPortGroup_vlag   5         Yes         0050.5678.eaed   None
auto-for_iscsi         6         Yes         0050.5673.85f9   None
```

```
switch# show port-profile status associated
Port-Profile          PPID       Activated    Associated MAC   Interface
auto-dvPortGroup_4_0    4          Yes         0050.567e.98b0   None
auto-dvPortGroup_vlag   5          Yes         0050.5678.eaed   None
auto-for_iscsi         6          Yes         0050.5673.85f9   None
```

5．プロファイルおよび適用インタフェース情報を表示するために、'show port-profile interface all' コマンドを使用します。

```
switch# show port-profile interface all
Port-profile          Interface
auto-VM_Network        Te 9/0/53
auto-for_iscsi         Te 9/0/54
```

15 VLAN の設定

15.1 VLAN 概要

IEEE 802.1Q Virtual LANs (VLANs)は物理ネットワーク上に複数の仮想ネットワークを重ねる機能を提供します。VLAN は仮想ネットワーク間のネットワークトラフィックを隔離し、管理及びブロードキャストドメインのサイズを小さくすることが可能です。
VLAN は物理的な位置に依存しないことが要求される共通の要件を持ったエンドステーションを含みます。エンドステーションが物理的に同一 LAN セグメントに無かったとしても、一つの VLAN にグループ化することが出来ます。VLAN は一般的に IP サブネットワークと関連付けられ、個々の IP サブネットの全てのエンドステーションは、同一 VLAN に属します。VLAN 間のトラフィックは、ルーティングされなければなりません。VLAN の構成要素は、インタフェース毎に設定できます。

15.2 入力の VLAN フィルタリング

スイッチに到着したフレームは、タグ付/タグ無に基づき、指定されたポートか VLAN のどちらかに関連付けられます。

- タグ付フレームのみ ― フレームが到着したポートは、フレームの VLAN タグにある VLAN ID によって単一 VLAN か複数 VLAN に割り当てられます。これは、trunk モードと呼ばれます。
- タグ無フレームのみ ― これらのフレームは、フレームが到着したポートに割り当てられているポート VLAN ID(PVID)に割り当てられます。
- VLAN タグ付とタグ無フレーム ― 全てのタグ付とタグ無フレームは次の通りに処理されます。
    - すべてのタグ無フレームは native VLAN に分類されます。
    - 送出フレームが priority tag の場合、ポートに CEE map が割り当てられてないならば、native VLAN の全ての送出フレームは、タグ無です。
    - native VLAN に設定された VLAN タグと等しいタグを持ったフレームは、native VLAN で処理されます。
    - 入出力に対して、native VLAN でないタグ付フレームは、ユーザーが指定した VLAN に従って処理されます。これは、trunk モードと呼ばれています。

NOTE
入力の VLAN フィルタは、デフォルトで全てのレイヤ２インタフェースで有効です。これは、VLAN がユーザー設定に依存して受信ポートでフィルタされることを保証しています。

図 15-1 に入力フレームに対するフレーム処理ロジックを示します。

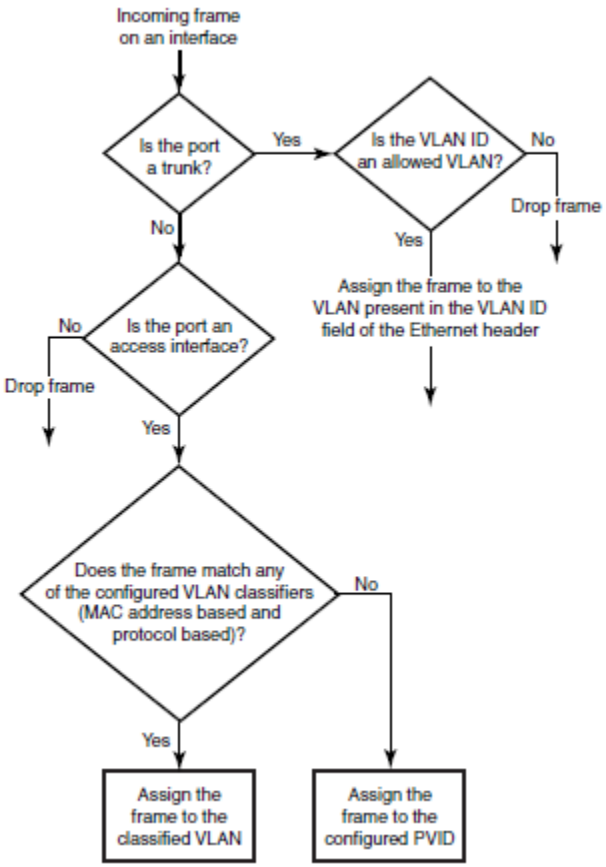

図 15-1 入力の VLAN フィルタ

入力の VLAN フィルタに関して、理解しておくべき重要な要件があります。

- 入力の VLAN フィルタはポートの VLAN メンバに依存します。
- ポートの VLAN メンバは Network OS の CLI から構成されます。
- 動的 VLAN 登録はサポートしていません。
- VLAN フィルタリングを入出力ポートの両方で行います。
- LAG インタフェースのような論理的なレイヤ２インタフェースでの VLAN フィルタはポートインタフェースと同様です。
- VLAN FDB(filtering database)は、入力フレームの転送先を決定します。

補助的に、VLAN FDB について知っておくべき重要な要件があります。

- VLAN FDB は MAC アドレスと VLAN ID に基づき到着フレームの転送先を決定するのを補助する情報を含みます。FDB は、静的定義とスイッチにより学習する動的定義の両方を含みます。
- 学習により FDB エントリを動的に更新する機能をサポートしています。(ポートの状態が許可されていた場合。)
- 動的 FDB エントリは、マルチキャストグループアドレスに対しては生成されません。
- 動的 FDB エントリは、ハードウェアに設定されたエージングタイムに基づき、消えていきます。エージングタイムは、60 から 1000000 秒の間で設定できます。デフォルトは 300 秒です。

- VLAN ID を指定して、静的に MAC アドレスを登録することが出来ます。静的エントリは消えません。
- 静的 FDB エントリは、存在している動的に学習された FDB エントリを上書きし、エントリを消してしまう学習を無効にします。

NOTE
スイッチでのフレーム操作の詳細については、34 ページの『1.5 レイヤ 2 イーサネットの概要レイヤ 2 イーサネットの概要』を参照下さい。

15.3 VLAN 設定のガイドラインと制限

VLAN を設定する場合は、これらの VLAN 設定のガイドラインと制約に従ってください。

- アクティブなトポロジにおいて、独立した VLAN 学習(IVL)機能により、VLAN 単位に MAC アドレスが学習されます。
- MAC アドレス ACL は、いつも静的 MAC アドレスエントリを上書きします。このケースでは、MAC アドレスは転送アドレスであり、FDB エントリは ACL によって上書きされます。
- 本スイッチは、イーサネット DIX フレームと 802.2LLC SNAP encapsulated フレームのみをサポートしています。
- 802.1q トランクリンクの両端で同じネイティブ VLAN を設定する必要があります。そうしないと、ループおよび VLAN リークをブリッジングループの原因となることがあります。
- Brocade VCS ファブリッククラスタ内のすべてのスイッチは、同じ VLAN 番号を使用して設定する必要があります。

15.4 デフォルト VLAN 設定

表 15-1 はデフォルト VLAN の構成を示しています。

表 15-1 デフォルト VLAN 構成

パラメータ	デフォルト設定
デフォルト VLAN	VLAN1
MTU サイズ	2500bytes

15.5 VLAN の構成と管理

NOTE
構成変更を保存するため、'copy running-config startup-config'コマンドを実行してください。

15.5.1 インタフェースポートの有効化・無効化

NOTE
DCB インタフェースは、スタンドアロンモードでは、デフォルトで無効になりますが、Brocade VCS ファブリックモードでは、デフォルトで有効になります。

NOTE
DCB インタフェースは、イーサネットリンクスピードのオートネゴシエーションをサポートしていません。DCB インタフェースは、10 ギガビットイーサネットおよびギガビットイーサネットをサポートしています。

インタフェースポートを有効化・無効化するために、特権実行モードから次の手順を実行してください。

1. グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2. インタフェースタイプとスロット/ポートを指定するために、'interface'コマンドを入力します。VCS モードでは、'gigabitethernet *rbridge-id/slot/port*'オペランドのみを使用します。これらのポートのためのプロンプトは、次のフォーマットになります：
   `switch(config-if-gi-22/0/1)#`

   ```
   switch(config)#  interface tengigabitethernet 0/1
   ```
3. インタフェースの利用を切替えるため、'shutdown'コマンドを入力します。
   インタフェースを有効化するとき：

   ```
   switch(conf-if-te-0/1)# no shutdown
   ```

   インタフェースを無効化するとき：

   ```
   switch(conf-if-te-0/1)# shutdown
   ```

15.5.2 インタフェースポートの MTU 設定

NOTE
ファブリック全体は、単一のスイッチのような働きをします。そのため、MTU はエッジポートにのみ適用できて、ISL 上ではありません。

MTU(maximum transmission unit)を設定するため、インタフェースポート上で、特権実行モードから次の手順を実行してください。

1. グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2. インタフェースタイプとスロット/ポートを指定するために、'interface'コマンドを入力します。

   ```
   switch(config)# interface tengigabitethernet 0/1
   ```
3. インタフェースポートを有効化するため、'no shutdown'コマンドを実行します。
4. インタフェースポートの MTU を指定するため、'mtu'コマンドを実行します。

   ```
   switch(conf-if-te-0/1)# mtu 4200
   ```

15.5.3 VLAN の作成

VLAN はコンフィグレーションの観点から、インタフェースとして取り扱われます。
デフォルトでは、全てのポートは VLAN1(VLAN ID = 1)に割り当てられます。vlan_ID の値は 1 から 3963 が利用できます。VLAN ID 3964 から 4094 はシステムで予約しています。

NOTE
Network OS 3.0.0 では、‘reserved vlan’ コマンドをサポートしていません。

VLAN インタフェースを作成するには、特権実行モードから、次の手順を実行します。

1. グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2. VLAN インタフェースに番号を割り当てるため、'interface vlan'コマンドを実行します。

```
switch(config)# interface vlan 1010
```

15.5.4 VLAN での STP の有効化

インタフェースポートの全ては、一旦 VLAN に構成されます。一つのコマンドで、VLAN の全てのメンバに対して Spanning Tree Protocol (STP)を有効にすることが出来ます。
VLAN の STP を有効にするため、特権実行モードから次の手順を実行してください。

1. グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2. VLAN の STP のタイプを選択するため、'protocol spanning tree'コマンドを実行します。

```
switch(config)# protocol spanning tree mstp
```

3. VLAN インタフェース番号を選択するため、'interface'コマンドを実行します。

```
switch(config)# interface vlan 1002
```

4. VLAN1002 のスパニングツリーを有効にするため、'no spanning-tree shutdown'コマンドを有効にします。

```
switch(conf-if-vl-1002)# no spanning-tree shutdown
```

15.5.5 VLAN の STP の無効化

全てのインタフェースポートは、一旦 VLAN に設定されます。一つのコマンドで、VLAN の全てのメンバの STP を無効化できます。
VLAN の STP を無効化するため、特権実行モードから次の手順を実行してください。

1. グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2. VLAN インタフェース番号を選択するため、'interface'コマンドを実行します。

```
switch(config)# interface vlan 55
```

3. VLAN55 のスパニングツリーを無効化するため、'spanning-tree shutdown'コマンドを実行します。

```
switch(conf-if-vl-55)# spanning-tree shutdown
```

15.5.6 レイヤ２スイッチポートとしてのインタフェースポートの構成

レイヤ２スイッチポートとしてインタフェースを構成するため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。

VCS モードでは、‘gigabitethernet *rbridge-id/slot/port*’オペランドのみを使用します。これらのポートのためのプロンプトは、次のフォーマットになります：`switch(config-if-gi-22/0/1)#`

```
switch(config)# interface tengigabitethernet 0/1
```

3．DCB インタフェースを有効化するため、'no shutdown'コマンドを実行します。

4．レイヤ２スイッチポートとして構成するため、'switchport'コマンドを入力します。

5．DCB インタフェースの状態を確認するため、'do show'コマンドを入力します。

```
switch(conf-if-te-0/1)# do show interface tengigabitethernet 0/1
```

6．DCB インタフェース実行コンフィギュレーションの状態を表示するため、'do show'コマンドを実行します。

```
switch(conf-if-te-0/1)# do show running-config interface tengigabitethernet 0/1
```

15.5.7 アクセスインタフェースとしてのインタフェースポートの構成

各 DCB インタフェースポートは、フレームが untagged か tagged かに基づき受信します。アクセスモードは、untagged と priority-tagged フレームのみ受け付けます。

アクセスインタフェースとしてインタフェースを構成するため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。

```
switch(config)# interface tengigabitethernet 0/1
```

3．DCB インタフェースを有効化するため、'no shutdown'コマンドを実行します。

4．レイヤ２スイッチポートとしてインタフェースを設定するため、'switchport'コマンドを入力します。

```
switch(conf-if-te-0/1)# switchport access vlan 20
```

15.5.8 トランクインタフェースとしてのインタフェースポートの設定

各 DCB インタフェースポートは、フレームが untagged か tagged かに基づき受信します。トランクモードは、VLAN-tagged フレームのみ受け付けます。

トランクインタフェースとしてインタフェースを構成するため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。

```
switch(config)# interface tengigabitethernet 0/19
```

3．DCB インタフェースを有効化するため、'no shutdown'コマンドを実行します。

4．DCB インタフェースをトランクモードとするため、'switchport'コマンドを実行します。

```
switch(conf-if-te-0/19)# switchport mode trunk
```

5．インタフェースを通して、全てまたは一つまたは一切の VLAN インタフェースが送受信するかどうかを指定します。必要に応じて適切な次のコマンドを入力します。

- この例は、VLAN 30 にインタフェースを通して送受信することを許可しています。

```
switch(conf-if-te-0/19)# switchport trunk allowed vlan add 30
```

- この例は、全ての VLAN にインタフェースを通して送受信することを許可しています。

```
switch(conf-if-te-0/19)# switchport trunk allowed vlan all
```

- この例は、VLAN 11 を除く VLAN にインタフェースを通して送受信することを許可しています。

```
switch(conf-if-te-0/19)# switchport trunk allowed vlan except 11
```

- 全ての VLAN に送受信することを抑止しています。

```
switch(conf-if-te-0/19)# switchport trunk allowed vlan none
```

15.5.9　トランクインタフェースの VLAN の無効化

トランクインタフェースの VLAN を無効化するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。

```
switch(config)# interface tengigabitethernet 0/10
```

3．DCB インタフェースを有効化するため、'no shutdown'コマンドを実行します。

4．DCB インタフェースをトランクモードとするため、'switchport'コマンドを実行します。

```
switch(conf-if-te-0/10)# switchport mode trunk none
```

5．トランクポートから VLAN 範囲を削除するには、もう一度、'switchport'コマンドを入力します。

```
switch(conf-if-te-0/10)# switchport trunk allowed vlan remove 30
```

15.6　プロトコルベース VLAN の分類ルールの設定

プロトコルや MAC アドレスに基づく選択された VLAN への分類されたフレームに対して特別なルールを定義するため、VLAN classifier ルールを構成できます。ルールの組は VLAN classifier グループに分類

されます。(175 ページの『15.6.4 VLAN classifier グループと付加ルールの作成』を参照下さい。)
VLAN classifier ルール(1 から 256)は、これらのカテゴリの一つにある構成可能なルールの組です。

- 802.1Q protocol-based classifier ルール
- ソース MAC address-based classifier ルール
- Encapsulated Ethernet classifier ルール

NOTE
複数の VLAN classifier は、別のルールからユニークとなるよう結果として VLAN ID を提供するインタフェース単位に適用されます。

802.1Q protocol-based VLAN は、untagged フレームか優先度タグ付のフレームにのみ適用されます。
Ethernet-II と 802.2 SNAP encapsulated frames の両方は、次のプロトコルタイプをサポートしています。

- Ethernet hexadecimal (0x0000 through 0xffff)
- Address Resolution Protocol (ARP)
- IP version 6 (IPv6)

NOTE
利用可能な全ての VLAN classifier のオプションの完全な情報として、『Network OS Command Reference』を参照下さい。

15.6.1 VLAN classifier ルールの生成

ARP protocol-based VLAN classifier ルールを生成するため、特権実行モードから次の手順で実行してください。

1. グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2. protocol-based VLAN classifier ルール構成するため、'vlan classifier rule'コマンドを入力します。

```
switch(config)# vlan classifier rule 1 proto ARP encap ethv2
```

15.6.2 MAC address-based VLAN classifier ルールの構成

MAC address-based VLAN classifier ルールを構成するため、特権実行モードで次の手順を実行してください。

1. グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2. MAC address-based VLAN classifier ルール構成するため、'vlan classifier rule'コマンドを入力します。

```
switch(config)# vlan classifier rule 5 mac 0008.744c.7fid
```

15.6.3 VLAN classifier ルールの削除

VLAN classifier groups (1 through 16)は、いくつでも VLAN classifier ルールを含めることが出来ます。VLAN classifier group を構成し、VLAN classifier ルールを削除するため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．VLAN classifier group を生成してと削除するルールを指定します。

```
switch(config)# vlan classifier group 1 delete rule 1
```

15.6.4 VLAN classifier グループと付加ルールの作成

VLAN classifier グループ(1 から 16)は、いくつでも VLAN classifier ルールを含むめることが出来る。VLAN classifier グループを構成し VLAN classifier ルールを追加するため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．VLAN classifier group を作成してルールを追加します。

```
switch(config)# vlan classifier group 1 add rule 1
```

15.6.5 インタフェースポートの VLAN classifier グループの有効化

VLAN classifier グループとインタフェースポートを結びつけるために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを入力します。

VCS モードでは、‘gigabitethernet rbridge-id/slot/port’オペランドのみを使用します。これらのポートのためのプロンプトは、次のフォーマットになります。

```
switch(config-if-gi-22/0/1)#
```

```
switch(config)# interface tengigabitethernet 0/10
```

3．DCB インタフェースを無効化する'no shutdown'コマンドを入力します。
4．vlan classifier グループと VLAN インタフェースを有効化し結びつけるために'vlan classifier'コマンドを入力します。(この例では、グループ：１、VLAN：２が使われています。)。

```
switch(conf-if-te-0/10)# vlan classifier activate group 1 vlan 2
```

NOTE

この例では、VLAN2 が既に定義されていることを前提としています。

15.6.6 VLAN 情報の表示

VLAN 情報を表示するため、特権実行モードから次のコマンドを入力します。

1．指定したインタフェースの構成情報と状態を表示するため、'show interface'コマンドを入力します。

```
switch# show interface tengigabitethernet 0/10 port-channel 10 switchport
```

2．指定した VLAN 情報を表示するため'show vlan'コマンドを入力します。例えば、下記は静的・動的を含む全てのインタフェースの VLAN20 の状態を表示します。

```
switch# show vlan 20
```

15.7 MAC アドレステーブルの設定

各 DCB ポートは MAC アドレステーブルを持っています。MAC アドレステーブルは、フラッディングをさけるためユニキャストとマルチキャストを格納しています。内蔵 DCB スイッチはハードウェアでエージングタイマを持っています。もし、MAC アドレスが残留すると、指定した時間後無効化され、MAC アドレステーブルテーブルから削除されます。レイヤ２イーサネット環境において、スイッチがどのように MAC アドレスを操作するかの詳細については、34 ページの『1.5 レイヤ 2 イーサネットの概要』を参照下さい。

15.7.1 MAC アドレスのエージングタイムの指定と無効化

動的エントリが MAC アドレステーブル登録されてから残留する時間を指定することが出来ます。静的アドレスエントリはエージングまたは削除されることはありません。また、エージングを無効にすることも出来ます。デフォルト値は、300 秒です。

NOTE

MAC アドレスのエージングタイムを無効にするためには、エージングタイムを 0 にします。

MAC アドレスのエージングタイムを指定・無効化するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．MAC アドレスのエージングタイムを指定するか、無効にするかによって、適切なコマンドを入力します。

```
switch(config)# mac-address-table aging-time 600
```

15.7.2 MAC アドレステーブルへの静的アドレス登録

MAC アドレステーブルに静的アドレスを登録するため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．下記の例では、VLAN100 で受信するパケットに対して、静的アドレス 0011.2222.3333 を MAC アドレステーブルに登録します。

```
switch(config)# mac-address-table static 0011.2222.3333 forward
tengigabitethernet 0/1 vlan 100
```

16 スパニングツリーの設定

16.1 STP 概要

IEEE 802.1D Spanning Tree Protocol (STP) は 802.1D に準拠したブリッジやスイッチで動作します。STP は冗長接続によりネットワーク上に発生するループを防止します。もし、プライマリ接続が障害となった場合、バックアップ接続が有効化され、ネットワークトラフィックに影響を与えません。スイッチやブリッジで STP が動作していない場合、リンク障害はループに至ります。

NOTE
VCS モードでは、全ての STP 設定は無効化されます。スイッチが'standalone mode'の場合だけ、STP、RSTP、MSTP、PVST+、Rapid PVST+をサポートします。

スパニングツリーが実行中、ネットワークにあるいずれかの LAN からその他の LAN に単一の経路で到達できるよう、ネットワークスイッチは実際のネットワークトポロジをスパニングツリートポロジへ変更します。ネットワークスイッチは、ネットワークトポロジに変更がある度に新しいスパニングツリートポロジを再計算します。

NOTE
スタンドアロンモードで動作しているすべての内蔵 DCB スイッチは、VLAN のループの問題を回避するために構成された xSTP のいくつかのバージョンを持っている必要があります。

各々の LAN に対して、LAN に接続されたスイッチはルートスイッチに最も近いスイッチである指定スイッチを選択します。指定スイッチは、LAN からまた LAN へ全てのトラフィックを転送する役割を持ちます。LAN に接続された指定スイッチのポートは、指定ポートと呼ばれます。スイッチは、そのポートのどれがスパニングツリートポロジの一部かを決定します。ポートがルートポートか指定ポートならばスパニングツリートポロジに含まれます。
STP を使うと、データトラフィックはスパニングツリートポロジの一部であるポートでのみ転送されます。スパニングツリートポロジの一部ではないポートは、自動的に blocking(無効化)状態に自動的に変更されます。それらは、スパニングツリートポロジが壊れ、新しい経路として自動的に有効化されるまで、blocking 状態は維持されます。
STP で動作する全てのレイヤ２インタフェースに対する STP インタフェースの状態は下記の通りです。

- Blocking - インタフェースはフレーム転送しません。
- Listening - インタフェースはフレーム転送するポートの一部としてスパニングツリーにより特定されます。これは、Blocking 状態からの遷移状態です。
- Learning-インタフェースは、フレーム転送に参加する準備をします。

- Forwarding - インタフェースはフレーム転送します。
- Disabled - shutdow 設定か未接続かそのポートではスパニングツリーが動作していないために、インタフェースはスパニングツリーに参加していません。

スパニングツリーに参加しているポートはこれらの状態遷移をします。

- 初期化から blocking へ
- blocking から listening または disabled へ
- listening から learning または disabled へ
- learning から forwarding または blocking または disabled へ
- forwarding から disabled へ

次の STP の機能は、STP の構成に使用するオプションの機能です。

- Root guard - 詳細は 199 ページの『16.9.4 guard root の設定』を参照下さい。
- PortFast BPDU guard と BPDU filter - 詳細は、201 ページの『16.9.8 port fast(STP)の有効化』を参照下さい。

16.1.1 STP の設定

STP の設定手順は次の通りです。

1. グローバルコンフィグレーションモードに移行します。
2. 'protocol spanning-tree'グローバルコマンドを使って、PVST+を有効化します。詳細は、189 ページの『16.8.1 STP, RSTP, MSTP, PVST の有効化』を参照下さい。

```
switch(config)# protocol spanning-tree pvst
```

3. 'bridge-priority'コマンドを使って、ルートスイッチを指定します。詳細は、189 ページの『16.8.4 ブリッジプライオリティの指定』を参照下さい。範囲は 0 から 61440 で、4096 単位に指定することが出来ます。

```
switch(conf-stp)# bridge-priority 28672
```

4. オプション：'spanning-tree portfast'コマンドを使って、スイッチのポートに PortFast 機能を有効化します。詳細は、201 ページの『16.9.8 port fast(STP)の有効化』を参照下さい。

NOTE

PortFast 機能は、ワークステーションや PC が接続されたポートにのみ有効化される必要があります。ワークステーションや PC が接続された全てのポートにこれらのコマンドを繰り返してください。スイッチが接続されたポートには PortFast 機能を設定してはいけません。

NOTE

トランキングおよび非トランキングモードで、ポート上で Port Fast を有効にすると、一時的なブリッジループを引き起こす可能性があります。

```
switch(config)# interface tengigabitethernet 0/10
switch(conf-if-te-0/10)# spanning-tree portfast
```

```
switch(conf-if-te-0/10)# exit
switch(config)# interface tengigabitethernet 0/11
switch(conf-if-te-0/11)# spanning-tree portfast
switch(conf-if-te-0/11)# exit
```

ワークステーションや PC が接続された全てのポートにこれらのコマンドを繰り返してください。

5．オプション：非ブロケード社製スイッチとの相互接続のため、次の'spanning-tree bpdu-mac'コマンドを使ってスイッチと接続したインタフェースを構成する必要があります。

```
switch(config)# interface tengigabitethernet 0/12
switch(conf-if-te-0/12)# spanning-tree bpdu-mac 0100.0ccc.cccd
```

6．次のポートを forwarding モードに設定します。

- ルートスイッチの全てのポート
- ルートポート
- 指定ポート

7．オプション：'spanning-tree guard root'コマンドを使って guard root 機能を設定します。guard root 機能は、ネットワーク中にルートブリッジの位置を強制的に設定する方法です。詳細は、199 ページの『16.9.4　guard root の設定』を参照下さい。隣接スイッチやブリッジに接続している他の全てのポートは、自動的に blocking モードになります。これは、ワークステーションや PC と接続しているポートに適用しません。これらのポートは forwarding モードとなります。

8．特権実行モードに戻ります。

```
switch(conf-if-te-0/12)#end
```

9．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

スパニングツリートポロジが完成すると、ネットワークスイッチはスパニングツリーの一部となっているポートでのみデータを送受信します。スパニングツリーの一部ではないポートで受信されたデータはブロックされます。

NOTE

その他の STP オプションはデフォルト値のまま使用することを推奨します。

更に詳細な情報は、188 ページの『16.8 スパニングツリーの構成と管理』を参照下さい。

16.2　設定時の注意事項および制約事項

スパニングツリーの設定を行う時は、次のコンフィギュレーションの注意事項および制約事項に従ってください。

- 別のものを有効にする前に、現在、有効にしている xSTP を無効にする必要があります。
- パラレルリンクの両側に接続されているすべてのデバイス上で xSTP を有効にしない場合、パケットドロップやパケットフラッディングが発生する可能性があります。
- LAG は、通常のリンクとして扱われており、デフォルトで STP が有効になっています。
- 32 個の MSTP インスタンスと 1 つの MSTP リージョンを持つことができます。
- MSTP インスタンスにマッピングする前に、VLAN を作成します。
- MSTP force-version オプションは、サポートしていません。
- STP が Brocade VCS ファブリッククラスタ間で機能するために、ネイティブ VLAN パケットのタグ付けオプションは、エッジポートで無効にする必要があります。ネイティブ VLAN タグ付けは、デフォルトで有効になっています。
- 誤設定のスパニングツリーが稼働しているローカルエリアネットワークが 1 つ以上のループを持っている場合、スパニングツリーBPDU のトラフィックストームが発生する可能性があります。特定の状況でスパニングツリーBPDU を含むトラフィックストームに長期間さらされた時、VDX は、再起動することがあります。
- さらに、誤設定のスパニングツリーが稼働しているローカルエリアネットワークが 1 つ以上のループを持っている場合、スパニングツリーBPDU のトラフィックストームが発生する可能性があります。エッジループ検出プロトコルは、スパニングツリーBPDU などの制御パケットを伴うトラフィックストーム中でループを排除することはできません。
- ブロケード NetIron MLX やブロケード TurboIron などの、レガシーFoundry 機器の PVST+または R-PVST+を使用して、ルートパスコストを介して強制的に代替ルートパスを作らないで下さい。これは、ネットワーク上のトラフィックの問題を引き起こす可能性があります。
- ネットワーク内の冗長パスでロードバランシングが機能するためには、すべての VLAN－インスタンスマッピング割り当てが一致している必要があります。そうしないと、すべてのトラフィックが 1 つのリンク上を流れます。
- 'global protocol spanning-tree mstp'コマンドを用いて MSTP を有効にする時、RSTP は自動的に有効にされます。
- 同一の MSTP リージョン内に 2 台以上のスイッチが存在するためには、同じ VLAN－インスタンスマッピング、同じコンフィギュレーションリビジョン番号、同じ名前を持つ必要があります。

16.3　RSTP 概要

NOTE
RSTP は、STP と互換性と相互接続性をもつように設計されています。しかし、STP が動作しているスイッチと相互接続する場合、RSTP の高速コンバージェンスの利点はなくなります。

IEEE 802.1w 高速スパニングツリー(RSTP)規格は、802.1D STP 規格の発展したものです。RSTP は、スイッチやポートや LAN の障害時に高速再コンバージェンスが可能になります。そして、エッジポートや新しいルートポートや point-to-point で接続されたポートの再構築が可能となります。
RSTP が動作する全てのレイヤ２インタフェースの状態は次の通りです。

- Learning - インタフェースはフレーム転送に参加するための準備をします。

- Forwarding - インタフェースはフレーム転送します。
- Discarding - インタフェースはフレームを破棄します。802.1D の disabled, blocking, listening 状態が RSTP の discarding 状態に集約されたことに注意してください。discarding 状態のポートは、有効なトポロジに参加せず、MAC アドレス学習も行いません。

表 16-1 は、STP と RSTP 間のインタフェース状態の違いを示しています。

表 16-1　STP と RSTP の状態比較

STP インタフェース状態	RSTP インタフェース状態	有効なトポロジへの 参加	ＭＡＣ学習
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	Yes	No
Learning	Learning	Yes	Yes
Forwarding	Forwarding	Yes	Yes

RSTP では、新しいインタフェースのポート役割もまた違っています。RSTP はトポロジ内で果たすポートの状態と役割間を明確に区別しています。RSTP は STP で定義されるルートポート、指定ポートを使用しますが、ブロックポートはバックアップポートと代替ポートに分離されます。

- Backup port - 指定ポートのバックアップを提供し、同一 LAN や指定スイッチとして働くブリッジに２つ以上のポートで接続する場合だけ存在します。
- Alternate port - ルートブリッジへの冗長パスを提供するルートポートに代替ポートとして働きます。

ルートポートと指定ポートだけが、有効なトポロジの一部となります。代替・バックアップポートはトポロジに組み込まれません。
ネットワークが安定していると、ルートポートと指定ポートはフォワーディング状態であり、代替ポートとバックアップポートは、ディスカーディング状態です。トポロジチェンジが発生すると、新たな RSTP ポートの役割は、代替ポートがフォワーディング状態となる高速遷移を可能とすることです。
更に詳細な情報は、188 ページの『16.8 スパニングツリーの構成と管理』を参照下さい。

16.3.1　RSTP の設定

基本的な RSTP の設定手順は次の通りです。

１．グローバルコンフィグレーションモードに移行します。

２．'protocol spanning-tree'グローバルコマンドを津あって、RSTP を有効化します。詳細は、189 ページの『16.8.1 STP, RSTP, MSTP, PVST の有効化』を参照下さい。

```
switch(config)# protocol spanning-tree rstp
```

３．'bridge-priority'コマンドを使って、ルートスイッチを指定します。詳細は、189 ページの『16.8.4 ブリッジプライオリティの指定』を参照下さい。範囲は 0 から 61440 で、4096 単位に指定することが出来ます。

```
switch(conf-stp)# bridge-priority 28582
```

４．'bridge forward delay'を設定します。詳細は、190 ページの『16.8.5 ブリッジ転送遅延時間の指定』を参照してください。

```
switch(conf-stp)# forward-delay 20
```

５．'bridge maximum aging time'を指定します。詳細は、191 ページの『16.8.6 bridge maximum aging time の指定』を参照下さい。

```
switch(conf-stp)# max-age 25
```

６．'error disable timeout timer'を有効にします。詳細は、191 ページの『16.8.7 error disable timeout timer の有効化』を参照下さい。

```
switch(conf-stp)# error-disable-timeout enable
```

７．'error-disable-timeout interval'を設定します。詳細は、192 ページの『16.8.8 error disable timeout interval の指定』を参照下さい。

```
switch(conf-stp)# error-disable-timeout interval 60
```

８．'port-channel path cost'を設定します。詳細は、192 ページの『16.8.9 port-channel path cost の指定』を参照下さい。

```
switch(conf-stp)# port-channel path-cost custom
```

９．'bridge hello time'を設定します。詳細は、193 ページの『16.8.10 bridge hello time の設定』を参照下さい。

```
switch(conf-stp)# hello-time 5
```

１０．オプション：'spanning-tree portfast'コマンドを使って、スイッチのポートに PortFast 機能を有効化します。詳細は、201 ページの『16.9.8 port fast(STP)の有効化』を参照下さい。

NOTE

PortFast 機能は、ワークステーションや PC が接続されたポートにのみ有効化される必要があります。ワークステーションや PC が接続された全てのポートにこれらのコマンドを繰り返してください。スイッチが接続されたポートには PortFast 機能を設定してはいけません。

NOTE

トランキングおよび非トランキングモードでポート上の Port Fast を有効にすると、一時的なブリッジループを引き起こす可能性があります。

```
switch(config)# interface tengigabitethernet 0/10
switch(conf-if-te-0/10)# spanning-tree portfast
switch(conf-if-te-0/10)# exit
switch(config)# interface tengigabitethernet 0/11
switch(conf-if-te-0/11)# spanning-tree portfast
switch(conf-if-te-0/11)# exit
switch(config)#
```

ワークステーションや PC が接続された全てのポートにこれらのコマンドを繰り返してください。

１１．次のポートを forwarding モードに設定します。

- ルートスイッチの全てのポート
- ルートポート
- 指定ポート

詳細は、202 ページの『16.9.9 ポートプライオリティの指定』を参照下さい。

１２．オプション：'spanning-tree guard root'コマンドを使って guard root 機能を設定します。guard root 機能は、ネットワーク中にルートブリッジの位置を強制的に設定する方法です。詳細は、199 ページの『16.9.4 guard root の設定』を参照下さい。

隣接スイッチやブリッジに接続している他の全てのポートは、自動的に blocking モードになります。これは、ワークステーションや PC と接続しているポートに適用しません。これらのポートは forwarding モードとなります。

１３．特権実行モードに戻ります。

```
switch(config)# end
```

１４．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

16.4 MSTP 概要

IEEE802.1s Multiple STP(MSTP)は、単一の物理トポロジ上で多数のループフリーなトポロジの作成をサポートします。MSTP は同一のスパニングツリーインスタンスにマッピングされる多数の VLAN を有効にし、多数の VLAN をサポートするために必要なスパニングツリーインスタンス数を減らすことが可能です。各 MSTP インスタンスは、他のスパニングツリーインスタンスと独立してスパニングツリーのトポロジを構成することが出来ます。MSTP を使うと、データトラフィックに対して、多数の転送可能なパスを設けることが出来ます。あるインスタンスでの障害は、他のインスタンスに影響を与えることはありません。更に MSTP では、ネットワーク上に存在する物理リソースをより効果的に使用することが可能になり、VLAN 通信のよりよいロードバランスを実現できます。

NOTE

MSTP モードでは、高速コンバージェンスが可能となるよう自動的に RSTP が有効になります。

多数のスイッチは、多数のスパニングツリーインスタンスに参加するよう同一の MSTP 構成で一貫して構成されなければなりません。同一 MSTP 構成を持って接続されたスイッチのグループは、MSTP リージョンと呼ばれます。

NOTE

32 の MSTP インスタンスと一つの MSTP リージョンをサポートしています。

MSTP はリージョンを使ってスイッチドメインを管理する階層構造を導入しています。共通の MSTP 構成属性を共有するスイッチは、一つのリージョンに属します。MSTP 構成は、各スイッチが存在する MSTP リージョンを決定します。共通の MSTP 構成属性は次の通りです。

- 英数字のコンフィグ名称(32 バイト)
- コンフィグレーションレビジョン番号(2 バイト)
- MSTP インスタンスに各 VLAN をマップする 4096 のエレメントテーブル

リージョン境界は、上記の属性に基づいて決定されます。多数のスパニングツリーインスタンスは、MSTP リージョン内で動作し、そのインスタンスにマッピングされている VLAN に対して有効なトポロジを決定する RSTP インスタンスです。全てのリージョンは、リージョン内の全てのスイッチを含むシングルスパニングツリーを形成した common internal spanning tree(CIST)を持っています。CIST インスタンスと MSTP インスタンスの違いは、CIST インスタンスは MSTP リージョンを跨って動作し、リージョンを跨ってループフリーなトポロジを形成しますが、MSTP インスタンスは、一つのリージョン内のみで動作します。CIST インスタンスは、リージョンを跨るスイッチが RSTP をサポートしているなら、RSTP を使って動作します。しかし、幾つかのスイッチが 802.1D STP を使っているなら、CIST インスタンスは、802.1D に戻ります。各リージョンは、他のリージョンに対して単一の STP か RSTP ブリッジとして論理的に見えます。

16.4.1 MSTP の構成

基本的な MSTP の設定手順は次の通りです。

1. グローバルコンフィグレーションモードに移行します。
2. 'protocol spanning-tree'グローバルコマンドを使って MSTP を有効にする。詳細は、189 ページの『16.8.1 STP, RSTP, MSTP, PVST の有効化』を参照下さい。

```
switch(config)# protocol spanning-tree mstp
```

3. 'region'コマンドを使ってリージョン名称を指定します。更に詳細は、195 ページの『16.8.16 MSTP リージョン名称の指定』を参照下さい。

```
switch(conf-mstp)# region brocade1
```

4. 'revison'コマンドを使って、レビジョン番号を指定します。更に詳細は、196 ページの『16.8.17 MSTP 構成のレビジョン番号の指定』を参照下さい。

```
switch(conf-mstp)# revision 1
```

5. 'instance'コマンドを使って、VLAN を MSTP インスタンスに割り当てます。更に詳細は、194 ページの『16.8.14 VLAN の MSTP インスタンスへのマッピング』を参照下さい。

```
switch(conf-mstp)# instance 1 vlan 2, 3
switch(conf-mstp)# instance 2 vlan 4-6
switch(conf-mstp)# instance 1 priority 4096
```

6. 'max-hops'コマンドを使って、インタフェース上にループを防止するために BPDU の最大ホップ数を指定します。更に詳細は、195 ページの『16.8.15 BPDU(MSTP)最大 hop 数の指定』を参照下さい。

```
switch(conf-mstp)# max-hops 25
```

7. 特権実行モードに戻ります。

```
switch(config)# end
```

8. running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

MSTP に関する更に詳細な情報は、188 ページの『16.8 スパニングツリーの構成と管理』を参照下さい。

16.5 PVST+と Rapid PVST+の概要

典型的なブリッジのネットワークトポロジは、リンク障害のために、交代パスを提供するため冗長接続を持ちます。しかし、イーサネットフレームに TTL の概念が無いので、これはネットワークにループが存在すると、永続的なフレームの循環という結果になります。ループを防止するために、全てのブリッジに接続するスパニングツリーはリアルタイムに形成されます。冗長ポートはブロッキング状態（non-forwarding）になります。それらは、必要な時に有効化されます。
ブリッジトポロジに対するスパニングツリーを構築するために、ブリッジは制御フレーム(BPDU - Bridge Protocol Deta Unit)を交換しなければなりません。プロトコルは、BPDU の意味と必要となるステートマシンを定義しています。最初のスパニングツリープロトコル(STP)は IEEE 802.1d 規格の一部になりました。
しかし、STP のコンバージェンス時間はリンク障害時 50 秒です。これは、すぐに受け入れられなくなってきました。STP の主な骨組みを維持したまま、ラピッドスパニングツリー(RSTP)の一部として、コンバージェンス時間スピードアップするためにステートマシンが変更されました。RSTP は IEEE 802.1w 規格の一部になっています。
しかし、STP と RSTP 共に単一な論理トポロジを構築するものです。一般的なネットワークは、多数の VLAN を持ちます。単一の論理トポロジは、多数の VLAN に対する冗長パスの有効性を効果的に使用できていません。もし、ポートが STP/RSTP 配下の一つの VLAN に対して block/discard に設定されれば、他の全ての VLAN にも同様に設定されます。
Pre-VLAN Spanning Tree(PVST+)プロトコルは、ネットワーク上の各 VLAN に対するスパニングツリーインスタンスで動作します。RSTP ステートマシンが動作する PVST のバージョンは、Rapid-PVST(R-PVST+)と呼ばれます。Rapid Pre-VLAN Spanning Tree+(R-PVST+)は、スイッチ上の各 VLAN に対するスパニングツリーインスタンスの一つを持ちます。
しかし PVST は、ネットワーク上に多くの VLAN があると、多くの CPU パワーを消費するので、スケーラブルではありません。RSTP+と R-PVST+の両極端の間での妥協点は、Multiple Spanning Tree(MSTP)になります。それは、IEEE 802.1s で標準化され、後に IEEE 802.1Q-2003 規格に統合されました。MSTP は独立した VLAN であるスパニングツリーの多数のインスタンス上で動作します。そして、各インスタンスに VLAN の集合を割り当てます。

NOTE
Brocade Network OS v3.0.0 は、PVST+と R-PVS+のみをサポートします。 PVST と R-PVST プロトコルは、Cisco 独自のものであり、サポートしていません。

PVST+や R-PVST+を構成するために、'protocol spanning-tree pvst'と'protocol spanning-tree rpvst'コマンドを使用します。詳細は、『Network OS Command Reference』を参照下さい。

例えば、下記の手順は VLAN10 に対する PVST+を設定します。

```
switch(config)# protocol spanning-tree pvst
switch(conf-pvst)# bridge-priority 4096
switch(conf-pvst)# forward-delay 4
switch(conf-pvst)# hello-time 2
switch(conf-pvst)# max-age 7
```

16.6　PVST+と R-PVST+のガイドラインと制限

PVST+と R-PVST+を構成するとき、次の事項を考慮してください。

- ネイティブ VLAN のタギングを無効化することは、スタンドアロンモードで STP/RSTP/MSTP スイッチで必要とされ、それ以外は、PVST+/R-PVST+が収束しないで、ネイティブ VLAN 上のループをつくります。タグ付けされたネイティブ VLAN データトラフィックは、無視されます。ネイティブ VLAN のタグなしデータは、転送されます。
- ネイティブ VLAN のタギングを無効化することは、ファブリッククラスタモードのエッジポートで必要です。それ以外は、PVST+/R-PVST+が収束しないで、ネイティブ VLAN 上のループをつくります。タグ付けされたネイティブ VLAN データトラフィックは無視されます。ネイティブ VLAN のタグなしデータは転送されます。
- PVST+モードをインタフェースで有効にせずに、VLAN の下で RSTP が有効になっている VDX が接続しているタグ付きポートで VLAN が構成されている場合、タグ付きのポートから BPDU は廃棄されます。

16.7　デフォルトのスパニングツリー設定

各スパニングツリーのデフォルト設定値を示します。

NOTE

ここで示すデフォルト設定値は、ファームウェアのデフォルト設定にコンフィグレーションを初期化した場合の値であり、工場出荷時の設定とは異なります。工場出荷時の設定は、添付 CD などモジュール付属の参照下さい。

表 16-2 に、STP 構成のデフォルト値を示します。

表 16-2　STP デフォルト構成パラメータ

パラメータ	デフォルト設定
Spanning-tree mode	STP、 RSTP、MSTP が無効（デフォルト）
Bridge priority	32768
Bridge forward delay	15 秒
Bridge maximum aging time	20 秒
Error disable timeout timer	無効
Error disable timeout interval	300 秒
Port-channel path cost	スタンダード
Bridge hello time	2 秒

表 16-3 に、MSPT のみを設定下場合のデフォルト値を示します。

表 16-3　MSTP デフォルト構成パラメータ

パラメータ	デフォルト設定
Cisco interoperability	無効
Switch priority (when mapping a VLAN to an MSTP instance)	32768
Maximum hops	20 hops
Revision number	0

表 16-4 に、10GbE DCB インタフェースのデフォルト値を示します。

表 16-4　10GbE DCB インタフェースデフォルト構成パラメータ

パラメータ	デフォルト設定
Spanning tree	インタフェース上で無効
Automatic edge detection	無効
Path cost	2000
Edge port	無効
Guard root	無効
Hello time	2 秒
Link type	Point-to-point
Port fast	無効
Port priority	128
DCB interface root port	DCB インタフェースがルートポートになることを許可
DCB interface BPDU restriction	制限は無効

16.8　スパニングツリーの構成と管理

NOTE

コンフィグレーションを格納するため、'copy running-config startup-config'コマンドを入力してくださ

い。

16.8.1 STP, RSTP, MSTP, PVST の有効化

ループ検出または防止するために STP を有効化します。STP はループフリーなトポロジでは必要ありません。STP の種類を切替える場合は、一旦 STP を無効化しなければなりません。デフォルトでは、STP,RSTP,MSTP は有効ではありません。

特権実行モードで次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．STP, RSTP, MSTP, PVST+, R-PVST+を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree rstp
```

16.8.2 STP, RSTP, MSTP の無効化

NOTE

'no protocol spanning-tree'コマンドを使って、インタフェースのプロトコルに定義されている全ての構成を削除することが出来ます。

STP, RSTP, MSTP を無効化するために、特権実行モードで次の手順を実行してください。デフォルトでは、STP, RSTP, MSTP は有効ではありません。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．STP, RSTP, MSTP, PVST+, R-PVST+を無効にするため、'protocol'コマンドを入力してください。

```
switch(config)#no protocol spanning-tree
```

16.8.3 STP, RSTP, MSTP を全面的に停止する

STP, RSTP, MSTP を全面的に停止するために、特権実行モードで次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．STP, RSTP, MSTP, PVST+, R-PVST+を全面的に停止するため、'shutdown'コマンドを入力してください。下記の'shutdown'コマンドは全ての３つのモードで機能します。

```
switch(conf-mstp)# shutdown
```

16.8.4 ブリッジプライオリティの指定

STP,RSTP,MSTP のどのモードでも、スイッチのプライオリティを指定するために、'bridge-priority'コマンドを使います。ルートスイッチを決定した後、ルートスイッチとして指定するスイッチに適切な値を設定します。もし、スイッチが他の全てのスイッチより低いブリッジプライオリティを持っているなら、他のスイッチは自動的にそのスイッチをルートスイッチとして自動的に選択します。

ルートスイッチは、中心に位置づけ、継続不可能な場所に設置するべきではありません。バックボーンスイッチは、端末に接続しないため一般的にルートスイッチとして働きます。例えば、ポートをブロック状態にしたり、フォワーディング状態にしたりといった、ネットワーク上のその他全ての判断は、ルートスイッチの観点から決定されます。
Bridge Protocol Data Units(BPDU)は、スイッチ間で交換される情報を伝達します。ネットワーク上の全てのスイッチの電源が投入されると、ルートスイッチを選択するプロセスが開始されます。各スイッチは、VLAN 毎に直接接続されたスイッチに BPDU を送信します。各スイッチはスイッチが送信した BPDU と受信した BPDU を比較します。ルートスイッチの選択プロセスでは、もしスイッチ２が広告する root ID より低い番号となる root ID をスイッチ１が広告するならば、スイッチ２は root ID を広告するのを停止し、スイッチ１の root ID を受け入れます。最も低いプライオリティをもったスイッチがルートスイッチとなります。
さらに、特定の VLAN のためのブリッジプライオリティを指定することもできます。VLAN パラメータが提供されていない場合、プライオリティの値は、すべての VLAN ごとのインスタンスに対してグローバルに適用されます。しかし、明示的に設定している VLAN には、VLAN 単位の設定は、グローバル設定よりも優先されます。

NOTE
VLAN の値は、1 から 3962 以内で、3963 から 4094 までは、リザーブされています。

ブリッジプライオリティを指定するために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．STP, RSTP, MSTP, PVST+, RPVST+を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree rstp
```

3．ブリッジプライオリティを指定します。範囲は 0 から 61400 までで、値は 4096 単位でのみ設定できます。デフォルトは、32678 です。

```
switch(conf-stp)# bridge-priority 20480
```

4．オプション：特定の VLAN のブリッジプライオリティを指定します。

```
switch(conf-stp)# bridge-priority 20480 vlan 10
```

16.8.5 ブリッジ転送遅延時間の指定

STP,RSTP,MSTP のどのモードでも、全てのスパニングツリーインスタンスでフォワーディングを開始するまでの listening 及び learning 状態をどのくらい維持するかを指定するためにこのコマンドを使います。範囲は、4 から 30 秒です。デフォルト 15 秒です。次の関係が維持される必要があります。

```
2*(forward_delay - 1)>=max_age>=2*(hello_time + 1)
```

さらに、特定の VLAN のための転送遅延を指定することもできます。VLAN パラメータが提供されていない場合、プライオリティの値は、すべての VLAN 毎のインスタンスに対してグローバルに適用されます。しかし、明示的に設定している VLAN では、VLAN 単位の設定がグローバル設定よりも優先されます。

VLAN の値は、1 から 3962 以内で、3963 から 4094 までは、リザーブされています。
ブリッジ転送遅延を指定するために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．STP, RSTP, MSTP, PVST+, R-PVST+を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree stp
```

3．ブリッジ転送遅延を指定します。

```
switch(conf-stp)# forward-delay 20
```

4．オプション：特定の VLAN のためのブリッジ転送遅延を指定します。

```
switch(conf-stp)# forward-delay 20 vlan 10
```

16.8.6 bridge maximum aging time の指定

STP,RSTP,MSTP のどのモードでも、インターフェースに Bridge Protocol Data Unit (BPDU)構成情報を格納する前に経過する最大時間を制御するために、このコマンドを使用します。'maximum aging time'を設定する場合、max-age は hello-time より大きくなければなりません。この範囲は、6 から 40 秒で、デフォルトは、20 秒です。次の関係を維持しなければなりません。

```
2*(forward_delay - 1)>=max_age>=2*(hello_time + 1)
```

さらに、特定の VLAN のための maximum age を指定することもできます。VLAN パラメータが提供されていない場合、プライオリティの値は、すべての VLAN ごとのインスタンスに対してグローバルに適用されます。しかし、明示的に設定している VLAN では、VLAN 単位の設定がグローバル設定よりも優先されます。
VLAN の値は、1 から 3962 以内で、3963 から 4094 までは、リザーブされています。
'bridge maximum aging time'を指定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．STP, RSTP, MSTP, PVST+, R-PVST+を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree stp
```

3．bridge maximum aging time を指定します。

```
switch(conf-stp)# max-age 25
```

4．オプション：特定の VLAN のための bridge maximum aging time を指定します。

```
switch(conf-stp)# max-age 25 vlan 10
```

16.8.7 error disable timeout timer の有効化

STP,RSTP,MSTP のどのモードでも、ポートを無効状態にするまでのタイマーを有効にするため、このコマンドを使用します。'STP BPDU guard'によりポートが無効にされている時、ポートが手動で有効にされなければ、ポートは無効のままです。このコマンドにより、ポートを無効状態から有効化することができます。'error disable timeout interval'設定の詳細については、192 ページの『16.8.8 error disable

timeout interval の指定』を参照下さい。

'error disable timeout timer'を設定するため、特権実行モードで次の手順を実行します。デフォルトでは、タイムアウト機能は無効です。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．STP, RSTP, MSTP, PVST+, R-PVST+を有効にするため、'protocol'コマンドを入力してください。

```
witch(config)# protocol spanning-tree stp
```

3．'error disable timeout timer'を有効化します。

```
switch(conf-stp)# error-disable-timeout enable
```

16.8.8 error disable timeout interval の指定

STP,RSTP,MSTP のどのモードでも、インタフェースがタイムアウトする時間を秒で指定するためこのコマンドを使用します。範囲は、10 から 1000000 秒です。デフォルトは 300 秒です。デフォルトでは、タイムアウト機能は無効です。
インタフェースがタイムアウトする時間を秒で指定するために、特権実行モード次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．STP, RSTP, MSTP, PVST+, R-PVST+を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree stp
```

3．インタフェースのタイムアウト時間を秒指定します。

```
switch(conf-stp)# error-disable-timeout interval 60
```

16.8.9 port-channel path cost の指定

STP,RSTP,MSTP のどのモードでも、port-channel path cost を指定するためにこのコマンドを使用します。デフォルトのコストは、'standard'です。パスコストのオプションは次の通りです。

- custom - port-channel の帯域に沿ってパスコストを変更する場合指定します。
- standard - port-channel の帯域に沿ってパスコストを変更しない場合指定します。

'port-channel path cost'を指定するために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．STP, RSTP, MSTP, PVST+, R-PVST+を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree stp
```

3．'port-channel path cost'を指定します。

```
switch(conf-stp)# port-channel path-cost custom
```

4．特権実行モードに戻ります。

```
switch(config)# end
```

5．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

16.8.10 bridge hello time の設定

STP と RSTP モードで、'bridge hello time'を設定するためこのコマンドを使用します。'hello time'は、インタフェースが他のデバイスに hello Bridge Protocol Data Units (BPDUs)をどの位頻繁にブロードキャストするかを決定します。範囲は 1 から 10 行です。デフォルトは 2 秒です。
'hello-time'を設定する場合、'max-age'設定が'hello-time'設定より大きくなければなりません。次の関係が維持される必要があります。

```
2*(forward_delay - 1)>=max_age>=2*(hello_time + 1)
```

さらに、特定の VLAN のための'hello-time'を指定することもできます。VLAN パラメータが提供されていない場合、プライオリティの値は、すべての VLAN ごとのインスタンスに対してグローバルに適用されます。しかし、明示的に設定している VLAN では、VLAN 単位の設定がグローバル設定よりも優先されます。
VLAN の値は、1 から 3962 以内で、3963 から 4094 までは、リザーブされています。
'bridge hello time'を設定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．STP, RSTP, MSTP, PVST+, R-PVST+を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree stp
```

3．インタフェースで'hello BPDU'の送信間隔を秒単位で指定します。

```
switch(conf-stp)# hello-time 5
```

4．オプション：特定の VLAN のための'hello BPDU'の送信間隔を秒単位で指定します。

```
switch(conf-stp)# hello-time 5 vlan 10
```

5．特権実行モードに戻ります。

```
switch(config)# end
```

6．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

16.8.11 transmit hold count (RSTP、MSTP、R-PVST+)の設定

RSTP と MSTP モードで、'transmit hold count'を指定することで BPDU のバーストサイズを設定するためこのコマンドを使用します。コマンドは、1 秒間のポーズの前に 1 秒間当たりに送信する最大 BPDU 数を設定します。範囲は 1 から 10 です。デフォルトは 6 秒です。
'transmit hold count'を指定するために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力し

ます。

2．'transmit hold count'を指定します。

```
switch(config)# transmit-holdcount 5
```

3．特権実行モードに戻ります。

```
switch(config)# end
```

4．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

16.8.12　　Cisco 相互接続性(MSTP)の設定

MSTP モードで、いくつかの Cisco スイッチとの相互接続の機能を有効にしたり無効にしたりするために、’ cisco-interoperability’コマンドを使います。もし、Cisco 相互接続性がネットワークでいずれかのスイッチに必要となった場合、そしてネットワーク上の全てのスイッチに互換性が必要となった場合、このコマンドを使って有効化します。デフォルトでは Cisco 相互接続性は無効となっています。

NOTE

このコマンドは、幾つかの旧式の Cisco スイッチの MSTP BPDU にある"version 3 length"が、現在の規格に適合しないために必要となります。

ある旧式の Cisco スイッチとの相互接続性を有効化するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．MSTP を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree mstp
```

3．Cisco 相互接続性を有効にします。

```
switch(conf-mstp)# cisco-interoperability enable
```

16.8.13　　Cisco 相互接続性(MSTP)の無効化

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．MSTP を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree mstp
```

3．Cisco 相互接続性を無効にします。

```
switch(conf-mstp)# cisco-interoperability disable
```

16.8.14　　VLAN の MSTP インスタンスへのマッピング

MSTP モードで、VLAN を MSTP インスタンスへマッピングするために、’ instance’コマンドを使用します。インスタンスに VLAN の設定をグループ化することができます。このコマンドは VLAN が生成された後にのみ使用することができます。VLAN インスタンスマッピングは、基礎となる VLAN が削除され

るとコンフィグレーションから削除されます。

VLAN を MSTP インスタンスにマッピングするために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．MSTP を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree mstp
```

3．VLAN を MSTP インスタンスにマッピングします。

```
switch(conf-mstp)# instance 5 vlan 300
```

4．特権実行モードに戻ります。

```
switch(config)# end
```

5．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

16.8.15　　BPDU(MSTP)最大 hop 数の指定

MSTP モードで、MSTP リージョンでの BPDU の最大 hop 数を設定するためにこのコマンドを使用します。BPDU の最大 hop 数を指定することは、インタフェースでのループ発生を回避することになります。hop 数を変更すると、全てのスパニングツリーインスタンスに影響です。範囲は、1 から 40 です。デフォルトは 20 です。

MSBP リージョンでの BPDU 最大 hop 数を設定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．MSTP を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree mstp
```

3．MSPT リージョンでの BPDU の最大 hop 数を指定するため、'max-hops'コマンドを入力します。

```
switch(conf-mstp)# max-hops hop_count
```

4．特権実行モードに戻ります。

```
switch(config)# end
```

5．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

16.8.16　　MSTP リージョン名称の指定

MSTP モードで、MSTP リージョン名称を割り当てるためこのコマンドを使用します。リージョン名称は、最大 32 文字で大文字小文字を識別します。

MSTP リージョン名を設定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力し

ます。

2．MSTP を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree mstp
```

3．MSTP リージョン名称を設定するため、'region'コマンドを入力します。

```
switch(conf-mstp)# region Sydney
```

4．特権実行モードに戻ります。

```
switch(config)# end
```

5．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

16.8.17　　MSTP 構成のレビジョン番号の指定

MSTP モードで、MSTP 構成のレビジョン番号を指定するためこのコマンドを使用します。範囲は、0 から 255 です。デフォルトは 0 です。

MSTP 構成のレビジョン番号を指定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．MSTP を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree mstp
```

3．MSTP 構成のレビジョン番号を指定するため、'revision'コマンドを入力します。

```
switch(conf-mstp)# revision 17
```

4．特権実行モードに戻ります。

```
switch(config)# end
```

5．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

16.8.18　　スパニングツリーカウンタのクリア

特権実行モードで、全てのまたは指定したインタフェースのスパニングツリーカウンターをクリアするためこのコマンドを使用します。

スパニングツリーカウンタをクリアするため、特権実行モードで次の手順を実行します。

1．全てのインタフェースの全てのスパニングツリーカウンターをクリアするために、'clear'コマンドを使います。

```
switch# clear spanning-tree counter
```

2．指定した port-channel や DCB ポートインタフェースに関連したスパニングツリーカウンターをクリアするために、'clear'コマンドを使います。

```
switch# clear spanning-tree counter interface tengigabitethernet 0/1
```

16.8.19　　スパニングツリー検出プロトコルのクリア

特権実行モードで、全てのインタフェースや特定のインタフェースでの隣接スイッチと強制的に再ネゴシエーションを行うようプロトコルマイグレーションプロセスをリスタートします。

プロトコルマイグレーションプロセスをリスタートするために、特権実行モードで次の手順を実行します。

1．全てのインタフェースの全てのスパニングツリー検出プロトコルをクリアするために、'clear'コマンドを使います。

```
switch# clear spanning-tree detected-protocols
```

2．指定した port-channel や DCB ポートインタフェースに関連したスパニングツリー検出プロトコルをクリアするために、'clear'コマンドを使います。

```
switch# clear spanning-tree detected-protocols interface tengigabitethernet 0/1
```

16.8.20　　STP 関連情報の表示

STP, RSTP, MSTP, PVST, Rapid-PVST 関連の全ての情報を表示するために、特権実行モードで'show spanning tree brief'コマンドを入力します。

NOTE

事実上のガードをルートする時、’ show spanning-tree brief’コマンド出力は、ポート状態を ERR（root_inc でない）と示します。

16.9　DCB インタフェースポート毎の STP, RSTP, MSTP の設定

この章では、10 ギガビットイーサネットの DCB インタフェースポート毎に STP, RSTP, MSTP を有効、設定するためのコマンドを詳細に説明します。

NOTE

VCS モードでは、全ての STP オプションは無効になります。スイッチがスタンドアロンモードの時のみ、ポートでの STP, RSTP, MSTP, PVST+, R-PVST+をサポートしています。

16.9.1　自動エッジ検出機能の有効化

DCB インタフェースで、エッジポートを自動的に特定するために、このコマンドを使用します。ポートは、もし BPDU を受信しなければ、エッジポートになります。デフォルトでは、自動エッジ検出機能は無効です。

NOTE

自動エッジ検出機能(“spanning-tree autoedge”オプション)は、未サポートでス。ポートの接続先ネットワークに、ループがないことが確実な場合は、“spanning-tree edgeport” オプションを設定してくだ

さい。

16.9.2 パスコストの設定

DCB インタフェースで、スパニングツリー計算のためのパスコストを設定するためこのコマンドを使用します。より小さいパスコストにより、インタフェースが root となる可能性が高くなります。範囲は、1 から 200000000 です。デフォルトのパスコストは、10G インタフェースのための 2000 です。さらに、特定の VLAN のためのスパニングツリーコストを指定することもできます。VLAN パラメータが提供されていない場合、プライオリティの値は、すべての VLAN ごとのインスタンスに対してグローバルに適用されます。しかし、明示的に設定している VLAN では、VLAN 単位の設定がグローバル設定よりも優先されます。
VLAN の値は、1 から 3962 以内で、3963 から 4094 までは、リザーブされています。

インタフェースにスパニングツリー計算のためのパスコストを設定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。

```
switch(config)# interface tengigabitethernet 0/1
```

2．DCB インタフェースを有効化するため、'no shutdown'コマンドを入力します。

```
switch(conf-if-te-0/1)# no shutdown
```

3．DCB インタフェースでのスパニングツリー計算のためのパスコストを設定するため'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)# spanning-tree cost 10000
```

4．オプション：特定の VLAN のためのパスコストを設定するには、'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)#spanning-tree cost 10000 vlan 10
```

5．特権実行モードに戻ります。

```
switch(conf-if-te-0/1)# end
```

6．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

16.9.3 エッジポートとしてポート（インターフェース）の有効化

DCB インタフェースで、ポートを forwarding ステータスに高速遷移させるエッジポートに指定するため、このコマンドを使用します。エッジポートに指定するため、次のガイドラインに従ってください。

- BPDU を受信しなければエッジポートとなります。
- エッジポートで BPDU を受信すれば、通常のスパニングツリーポートとなり、エッジポートとはなりません。

- ネットワークでループを生成することが無いエンドステーションと直接接続しているポートなので、エッジポートは直接 forwarding 状態となり、listening/learning 状態をスキップします。
- このコマンドは、RSTP と MSTP でサポートされます。STP に対しては、' spanning-tree portfast'コマンドを使用してください。(201 ページの『16.9.8 port fast(STP)の有効化』を参照下さい。)

DCB インタフェースをエッジポートに指定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。

```
switch(config)# interface tengigabitethernet 0/1
```

3．DCB インタフェースを有効化するため、'no shutdown'コマンドを入力します。

```
switch(conf-if-te-0/1)# no shutdown
```

4．DCB インタフェースをエッジポートに指定するため'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)# spanning-tree edgeport bpdu-filter
```

16.9.4 guard root の設定

DCB インタフェースで、スイッチに guard root を有効化するため、このコマンドを使用します。guard root は、ネットワーク上にルートブリッジを強制的に配置する方法を提供します。インタフェースに設定された guard root で、スイッチはどのインタフェースがスパニングツリールートポートやルートパスになることが共用されるかを制限することが可能となります。ルートポートは、ルートスイッチへの最短パスを提供します。デフォルトでは、guard root は無効です。
guard root は、悪意のある攻撃や、ルートブリッジにするつもりの無いブリッジデバイスがルートブリッジになるような意図しない誤設定からルートブリッジを保護します。これは、データパスでは致命的なボトルネックとなります。guard root は、有効化されたポートが指定ポートであることを保証します。もし、guard root が設定されたポートが、高優先度の BPDU を受信すると、discarding 状態となります。
さらに、特定の VLAN のための guard root を指定することもできます。VLAN パラメータが提供されていない場合、プライオリティの値は、すべての VLAN ごとのインスタンスに対してグローバルに適用されます。しかし、明示的に設定している VLAN では、VLAN 単位の設定がグローバル設定よりも優先されます。
VLAN の値は、1 から 3962 以内で、3963 から 4094 までは、リザーブされています。

DCB インタフェースに guard root を設定するために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。

```
switch(config)# interface tengigabitethernet 0/1
```

3．DCB インタフェースを有効化するため、'no shutdown'コマンドを入力します。

```
switch(conf-if-te-0/1)# no shutdown
```

4．DCB インタフェースに guard root を有効にするため、'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)#  spanning-tree guard root
```

5．VLAN のための guard root を有効にするため、'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)# spanning-tree guard root vlan 10
```

16.9.5 MSTP hello time の設定

DCB インタフェースで、ルートスイッチからの BPDU の送信間隔を設定するため、このコマンドを使用します。hello-time の変更は、全てのスパニングツリーインスタンスに影響します。'max-age'は、'hello-time'より大きくなければなりません。(191 ページの『16.8.6 bridge maximum aging time の指定』を参照ください。)範囲は、1 から 10 秒です。デフォルトは、2 秒です。

DCB インタフェースに MSTP hello time を設定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。

```
switch(config)# interface tengigabitethernet 0/1
```

3．DCB インタフェースを有効化するため、'no shutdown'コマンドを入力します。

```
switch(conf-if-te-0/1)# no shutdown
```

4．DCB インタフェースに hello time を設定するため'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)# spanning-tree hello-time 5
```

5．特権実行モードに戻ります。

```
switch(conf-if-te-0/1)# end
```

6．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

16.9.6 MSTP インスタンスの制限の指定

DCB インタフェースで、MSTP インスタンスの制限を指定するため、このコマンドを使用します。

DCB インタフェースに MSTP インスタンスの制限を指定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。

```
switch(config)# interface tengigabitethernet 0/1
```

3．DCB インタフェースを有効化するため、'no shutdown'コマンドを入力します。

```
switch(conf-if-te-0/1)# no shutdown
```

4．DCB インタフェースに制限を設定するため、’spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)# spanning-tree instance 5 restricted-tcn
```

5．特権実行モードに戻ります。

```
switch(conf-if-te-0/1)# end
```

6．running-config file を startup-config file に格納するため、`copy’ コマンドを実行します。

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

16.9.7 リンクタイプの指定

DCB インタフェースで、リンクタイプを指定するためこのコマンドを使用します。'point-to-point'を指定すると、高速スパニングツリーが forwarding 状態に遷移することを有効化します。'shared'を指定すると、高速スパニングツリーの遷移を無効にします。

DCB インタフェースにリンクタイプを指定するために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。

```
switch(config)# interface tengigabitethernet 0/1
```

3．DCB インタフェースのリンクタイプを有効にするため、'no shutdown'コマンドを入力します。

```
switch(conf-if-te-0/1)# no shutdown
```

4．DCB インタフェースに制限を設定するため'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)# spanning-tree link-type shared
```

16.9.8 port fast(STP)の有効化

DCB インタフェースで、高速に forwarding 状態に遷移することを可能とする'port fast'を有効化するため、このコマンドを使用します。'port fast'は、標準の forward time を待つことなく、インタフェースを即座に forwarding 状態にします。

NOTE

もし、'portfast bpdu-guard'オプションがインタフェースで有効になっており BPDU を受信した場合、インタフェースは無効化され'ERR_DISABLE'状態にします。

NOTE

トランキングおよび非トランキングモードでは、ポート上で Port Fast を有効にすると、一時的なブリッジループを引き起こす可能性があります。

MSTP と RSTP には'spanning-tree edgeport'コマンドを使用下さい。(198 ページの『16.9.3 エッジポートとしてポート（インターフェース）の有効化』を参照下さい。)

インタフェースに、STP の'port fast'を有効にするため、特権モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。

```
switch(config)# interface tengigabitethernet 0/1
```

3．DCB インタフェースを有効に設定するため、'no shutdown'コマンドを入力します。

```
switch(conf-if-te-0/1)# no shutdown
```

4．DCB インタフェースの'port fast'を有効にするため'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)# spanning-tree portfast
```

16.9.9 ポートプライオリティの指定

DCB インタフェースで、ポートプライオリティを指定するために、このコマンドを使用します。範囲は、0 から 240 で、16 単位で指定します。デフォルトは 128 です。
さらに、特定の VLAN のためのスパニングツリープライオリティを指定することもできます。VLAN パラメータが提供されていない場合、プライオリティの値は、すべての VLAN ごとのインスタンスに対してグローバルに適用されます。しかし、明示的に設定している VLAN では、VLAN 単位の設定がグローバル設定よりも優先されます。
VLAN の値は、1 から 3962 以内で、3963 から 4094 までは、リザーブされています。

DCB インタフェースにポートプライオリティを設定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定して、'interface'コマンドを入力します。

```
switch(config)# interface tengigabitethernet 0/1
```

3．DCB インタフェースを有効にするため、'no shutdown'コマンドを入力します。

```
switch(conf-if-te-0/1)# no shutdown
```

4．DCB インタフェースにポートプライオリティ設定するため、'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)# spanning-tree priority 32
```

16.9.10 ルートポート遷移の抑止

DCB インタフェースで、ポートのルートポートへの遷移を抑止するためこのコマンドを使用します。デフォルトは、DCB インタフェースがルートポートに遷移できます。

ポートがルートポートに遷移することを抑止するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。

```
switch(config)# interface tengigabitethernet 0/1
```

3．DCB インタフェースを有効にするため、'no shutdown'コマンドを入力します。

```
switch(conf-if-te-0/1)# no shutdown
```

4．ポートがルートポートに遷移することを抑止するため'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)# spanning-tree restricted-role
```

16.9.11　　トポロジチェンジ通知の抑止

DCB インタフェースで、トポロジチェンジ通知 BPDU の送信を抑止するためにこのコマンドを使用します。デフォルトでは、抑止しません。

トポロジチェンジ通知 BPDU の送信を抑止するために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。

```
switch(config)# interface tengigabitethernet 0/1
```

3．DCB インタフェースを有効にするため、'no shutdown'コマンドを入力します。

```
switch(conf-if-te-0/1)# no shutdown
```

4．トポロジチェンジ通知 BPDU の送信を抑止するため'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)#spanning-tree restricted-tcn
```

16.9.12　　スパニングツリーの有効化

DCB インタフェースで、スパニングツリーを有効化するために、このコマンドを使います。デフォルトでは、スパニングツリーは無効です。

スパニングツリーを有効化するため特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。

```
switch(config)# interface tengigabitethernet 0/1
```

3．DCB イインタフェースを有効にするため、'no shutdown'コマンドを入力します。

```
switch(conf-if-te-0/1)# no shutdown
```

4．スパニングツリーを有効化するため'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)# no spanning-tree shutdown
```

16.9.13　　スパニングツリーの無効化

DCB インタフェースで、スパニングツリーを無効化するために、このコマンドを使います。デフォルトでは、スパニングツリーは無効です。

スパニングツリーを無効化するため特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。

```
switch(config)# interface tengigabitethernet 0/1
```

3．DCB イインタフェースを有効にするため、'no shutdown'コマンドを入力します。

```
switch(conf-if-te-0/1)# no shutdown
```

4．スパニングツリーを無効化するため'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)# spanning-tree shutdown
```

NOTE

インタフェースでスパニングツリーが無効化された状態で、インタフェース自身も shutdown 定義されている場合、’`show spanning-tree interface`’での protocol 表示が正しくない場合があります。

---

17 リンクアグリゲーションの設定

17.1 リンクアグリゲーション概要

リンクアグリゲーションは、複数の物理イーサネットリンクをパフォーマンスと冗長性を向上する単一の論理トランクにまとめるものです。結合されたトランクはリンクアグリゲーショングループ(LAG:Link Aggregation Group)と呼びます。LAG はスパニングツリープロトコル、IEEE802.1Q VLAN などで接続されたデバイスからは一つのリンクに見えます。LAG の一つの物理リンクがダウンした場合、他のリンクはアップしたまま通信が途絶えません。
リンクを LAG に設定するため、物理リンクは同じスピードでなければならず、全てのリンクは同じ隣接デバイスと接続される必要があります。リンクアグリゲーションは、手動で LAG を構成したり、IEEE802.3ad の Link Aggregation Control Protocol (LACP)を使って動的に構成する方法があります。
複数の入力ソースからのトラフィックが同じ出力ポートにキューイングすると、入力ソースが単一の物理リンクかまたは複数のメンバーリンクを持つトランクであるかにかかわらず、すべての入力ソースは、同じ重みを与えられます。

NOTE
LAG と LAG インタフェースはまたポートチャネル(port-channel)とも呼びます。

リンクアグリゲーションの利点を下記にまとめます。

- 帯域の増加(論理帯域は要求に応じて動的に変化します。)
- アベイラビリティの向上
- 負荷分割
- 高速な構成設定と再構成

本スイッチは、次のトランクタイプをサポートしています。

- 静的な標準 LAG
- LACP を使用した動的な標準ベースの LAG
- 静的な Brocade 独自 LAG
- LACP 拡張機能を使用した Brocade 独自の動的な LAG

17.1.1 リンクアグリゲーショングループの設定

内蔵 DCB スイッチでは標準 LAG として 16 リンクまでのリンクアグリゲーショングループ(LAG: Link Aggregation Group)を最大 24 まで設定できます。各 LAG はアグリゲータと関連付けられています。アグリゲータはイーサネットフレームの収集と分配機能を管理します。
各ポートでのリンクアグリゲーションは次の制御を行います。

- ポートアグリゲーションを制御するための構成情報の維持
- LAG で接続した他のデバイスとの構成情報の交換

- ポートが LAG に参加・離脱した場合のアグリゲータへの追加と切り離し
- アグリゲータのフレーム収集と分配機能の有効化・無効化

内蔵 DCB スイッチでの各リンクは一つの LAG と関連付けることができるが、二つ以上の LAG とは関連付けられません。LAG へのリンクの追加・削除は静的、動的、LACP を介して制御できます。
各 LAG は次のコンポーネントから構成されます。

- LAG に含まれる個々のリンクの MAC アドレスとは異なる MAC アドレス
- 隣接デバイスとの接続を識別するための各リンクに対するインタフェース番号
- 各リンクに対する管理キー。同じ管理キーを持つリンクだけが同一 LAG に結合されます。LACP を使って構成された各リンク上では、LACP が自動的に port-channnel 識別番号と同じ管理キーを構成します。

17.1.2 リンクアグリゲーションコントロールプロトコル(LACP)

リングアグリゲーションコントロールプロトコル(LACP: Link Aggregation Control Protocol)は、２つのパートナーシステムで論理トランクの間の物理リンクの属性を自動的に調整するための IEEE802.3ad で規定される標準のプロトコルです。LACP はリンクが LAG に結合できるかどうかを自動的に決定します。もし、リンクが LAG に結合できる場合は、LACP はリンクを LAG にまとめます。LAG の全てのリンクは同一の管理特性を持ちます。LACP は２つのモードで動作します。

- パッシブモード ― LACP は、パートナーシステムからの Link Aggregation Control Protocol Data Unit (LACPDU)に応答しますが、LACPDU の交換はしません。
- アクティブモード ― LACP は、パートナーシステムからの LACPDU 送信に係らず LACPDU を交換します。

17.1.3 動的リンクアグリゲーション

動的リンクアグリゲーションは LAG からどのリンクを追加・削除するかを調整するために LACP を使用します。通常、複数の物理イーサネットリンクを共有している２つのパートナーシステムは、LACP を使ってそれら多くの物理リンクを結合します。LACP は両パートナーシステム上で LAG を生成し、LAG ID によって LAG を識別します。同一の管理キーをもった全てのリンクと同一パートナースイッチに接続された全てのリンクは、LAG のメンバーとなります。LACP は各リンクの状態をモニタするため継続的に LACPDU を交換します。

17.1.4 静的リンクアグリゲーション

静的リンクアグリゲーションでは、リンクはパートナーシステム間で LACPDU を交換することなく LAG にリンクが追加されます。静的リンクでのフレームの収集・分配はリンクの動作状態や管理状態により決定されます。

NOTE

ポートチャネルを shutdown して reload など装置の再起動をしないで下さい。物理リンクとの状態不

整合となり、通信エラーとなります。閉塞する場合は、ポートチャネルのメンバの物理リンクを shutdown してください。

17.1.5 Brocade 独自のアグリゲーション

Brocade 独自のアグリゲーションは、標準のリンクアグリゲーションと類似しているが、トラフィックを分散する方法が異なります。それには、アグリゲートされる前にリンクメンバーで追加されるルールを合わせておかなければなません。

- 最も重要なルールは、リンクメンバ間のファイバ長に大きな差が無いことであり、すべてのメンバーは同じ port-group の一部であることである。(内蔵 DCB スイッチではアップリンクポートとサーバ接続ポートは同一 port-group ではありません。)
- 最大で port-group 当たり 4 つの Brocade LAG を生成することが出来ます。

17.1.6 LAG の分配プロセス

LAG アグリゲータはイーサネットフレームの収集と分配と関連があります。収集と分配プロセスは次が保証されることを必要とします。

- 制御用 PDU の挿入と監視
- 制御用の通信を特定のリンクへの制限
- 個別リンク間の負荷分散
- LAG メンバー内での動的変更の制御

17.2 Virtual LAG 概要

virtual LAG(vLAG)の設定は LAG の設定と類似しています。一旦、VCS ファブリックが多数のスイッチに跨る LAG の設定を検出すると、LAG は自動的に vLAG になります。
VCS ファブリック上の LACP は、同一の LACP システム ID を送信することで単一の論理スイッチを模擬します。
vLAG の特徴：

- 同一のスピードのポートのみアグリゲートされます。
- Brocade 独自の LAG は vLAG では利用できません。
- LACP は自動的に協調し vLAG を形成します。
- ポートチャネルインタフェースは、全ての vLAG メンバー上で生成されます。
- VCS ファブリックは、vLAG の全てのノードを一貫した設定を必要とします。
- 静的 LAG と同様に、vLAG は設定エラーを検出できません。
- ポートを持たない vLAG は許容されます。
- IGMP snooping は vLAG のプライマリリンクで行われます。
- インタフェース統計情報は、vLAG メンバスイッチ単位に集計・表示されます。統計情報は、vLAG に参加するスイッチ間で統合されません。
- リンク及びノードレベルの冗長を実現するため、VCS ファブリックは静的 vLAG をサポートします。

VCS の vLAG は、静的 vLAG がサポートされるので、LACP が実装されていないサーバとの間でも機能します。

17.2.1 vLAG の構成

Network OS v3.0.0 は、ポートチャネルでの"許されたスピード"を 1 Gbps または 10 Gbps に設定するため、speed オプションをサポートしています。デフォルトは 10 Gbps です。ポートチャネルが 1 Gbps である場合、そのスピードは、ポートチャネルを有効にする前に設定する必要があります。そうでない場合、スピード不一致のため LAG/vLAG は構成されません。
'speed'コマンドについては、『Network OS Command Reference』を参照してください。

NOTE
DCB 機能は、vLAG ではサポートされていません。

---

vLAG の全てのメンバノードでこの手順を実行してください。
vLAG を設定するため、グローバルコンフィグレーションモードで次の手順を実行してください。

1．VCS ファブリック内の２つのスイッチ間で LAG を設定します。
更に詳細な情報は、205 ページの『17.1.1 リンクアグリゲーショングループの設定』を参照下さい。VCS ファブリックが多数のスイッチ間で LAG 構成が定義されていることを検出すると、LAG は自動的に vLAG になります。

```
switch(config)# interface port-channel 10
```

2．特権実行モードに戻るため、'end'コマンドを使います。

```
switch(conf-int-po10)# end
```

3．ポートチャネルの詳細を確認するために'show'コマンドを使います。

```
switch# show port-channel detail
LACP Aggregator: Po 27
Aggregator type: Standard
 Ignore-split is disabled
 Actor System ID - 0x8000,00-05-33-6f-18-18
 Admin Key: 0027 - Oper Key 0027
 Receive link count: 4 - Transmit link count: 4
 Individual: 0 - Ready: 1
 Partner System ID - 0x8000,00-05-1e-cd-6e-9f
 Partner Oper Key 0027
 Member ports on rbridge-id 231:
  Link: Te 231/0/22 (0xE718160201) sync: 1 *
  Link: Te 231/0/23 (0xE718170202) sync: 1
  Link: Te 231/0/36 (0xE718240305) sync: 1
  Link: Te 231/0/37 (0xE718250306) sync: 1
```

4．ポートチャネルインタフェースの詳細を確認するため'show'コマンドを使います。

```
switch# show port port-channel tengigabitethernet 1/0/21
```

```
LACP link info: te0/21 -0x18150014
Actor System ID: 0x8000,01-e0-52-00-01-00
Actor System ID Mapped Id: 0
Partner System ID: 0x0001,01-80-c2-00-00-01
Actor priority: 0x8000 (32768)
Admin key: 0x000a (10) Operkey: 0x0000 (0)
Receive machine state : Current
Periodic Transmission machine state : Slow periodic
Muxmachine state : Collecting/Distr
Admin state: ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
Operstate: ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Partner operstate: ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Partner oper port: 100
```

17.2.2 vLAG 分割を無視する設定

'vlag ignore-split'コマンドは、LACP ベース vLAG 用です。この構成のスコープは、ポートチャネルごとに設定できます。vLAG が二つ以上のノードにまたがるシナリオでは、vLAG のノードのいずれかがダウン状態になる場合にパケット損失の程度を最小限に抑えることができます。
ノード間の接続がファブリック分割のために失われた場合（ダウン状態になる 1 つのメンバとは対照的）に、マルチキャスト/ブロードキャストパケットの重複があります。
個々のリンクが障害の 1 点で起きないように、ファブリック内の冗長性を構築することをお勧めします。
図 17-1 は、RB2、RB3、RB4 の 3 つのリンクを持った二重の vLAG 構成を示します。Host-1 が Host-2 または Host3 と通信している最中に RB2、RB3、RB4 のいずれかが再起動すると、瞬間的なトラフィックの中断が発生することがあります。

NOTE
'ignore-split'を有効にして、Linux サーバー/ nic-team /CNA と相互運用している間、サーバーからのトラフィックの早期出力のために、VLAG ノードの再起動が 1 秒以上失われる可能性があります。

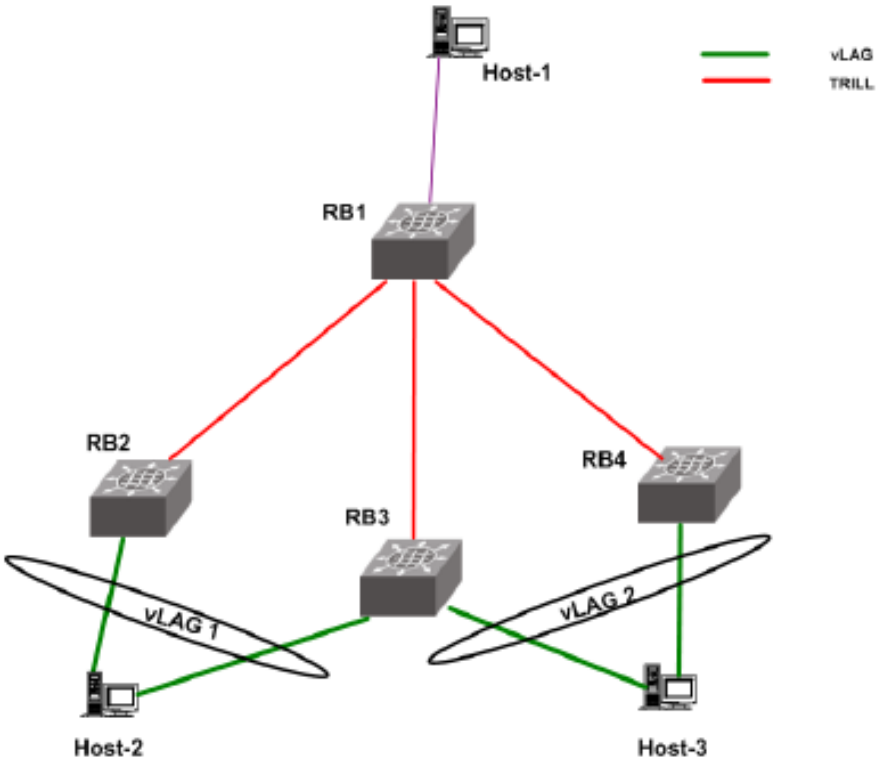

図 17-1 ignore split の VLAG 設定

vLAG フェイルオーバーダウンタイムを減らすために、vLAG でリンク（この場合は RB2、RB3、及び RB4）の全てに ignore split を設定する必要があります。

'vLAG ignore split'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手順を実行します。

1. RB2 にログインします。vLAG1 の第 1 の脚。
2. 第 1 の脚のためのポートチャネルにアクセスします。

```
switch(config)# interface port-channel 1
```

3. 'vLAG ignore split'を有効にします。

```
switch(config-Port-channel-1)# vlag ignore-split
```

4. RB3 にログインします。vLAG1 の第 2 の脚。
5. 第 2 の脚のためのポートチャネルにアクセスします。

```
switch(config)# interface port-channel 2
```

6. 'vLAG ignore split'を有効にします。

```
switch(config-Port-channel-2)# vlag ignore-split
```

7. 第 3 の脚のためのポートチャネルにアクセスします。

```
switch(config)# interface port-channel 3
```

8. 'vLAG ignore split'を有効にします。

```
switch(config-Port-channel-3)# vlag ignore-split
```

17.2.3 リモート Rbridge 上のロードバランスの設定

この機能を使用すると、vLAG にトラフィックを転送するために、vLAG のメンバーではないリモート

Rbridge（また、非ローカル RBridge として認識される）で、ロードバランシング機能を設定することができます。vLAG 方向の可能なパスにトラフィックを分散するには、RB2 に'lag-load-balancing’を設定することができます。利用できる特性を、表 17-1 に示します。

表 17-1　ロードバランス条件

パラメータ	詳細条件
dst-mac-vid	宛先 MAC アドレスと VID ベースのロードバランシング
dst-mac-vid	送信元 MAC アドレスと VID ベースのロードバランシング
src-dst-mac-vid	送信元および宛先 MAC アドレスと VID ベースのロードバランシング
src-dst-ip	発信元と宛先の IP アドレスベースのロードバランシング
src-dst-ip-mac-vid	送信元と宛先の IP アドレス、MAC アドレスおよび VID ベースのロードバランシング。
src-dst-ip-port	発信元と宛先の IP アドレスと TCP / UDP ポートベースのロードバランシング
src-dst-ip-mac-vid-port	送信元と宛先の IP アドレス、MAC アドレス、VID および TCP / UDP ポートベースのロードバランシング。

さらに、Rbridge は、クラスタ内に存在する異なる vLAG に、異なる特性に設定することができます。この特徴は、各 Rbridge と各 vLAG に有効にできるので、異なる load-balance 特性は異なる vLAG に向かうトラフィックを設定することができます。'show running-config rbridge-id'コマンドは、コンフィギュレーション情報を表示します。'show fabric vlag-load-balance'コマンドは VLAG ためのロードバランスを表示します。

次の例では、"宛先 MAC アドレスと VID ベースのロードバランシング"の特性を設定します。

```
switch(config)# rbridge-id 2
switch(config-rbridge-id-2)# fabric vlag 20 load-balance dst-mac-vid
switch(config-rbridge-id-2)# end
switch# show running-config rbridge-id 2
rbridge-id 2
 interface-nodespecific ns-vlan 10
 interface-nodespecific ns-ethernet 100
 fabric vlag 10 load-balance src-dst-mac-vid
 fabric vlag 20 load-balance dst-mac-vid
 no protocol vrrp
switch# show fabric vlag-load-balance 10
Fabric Vlag Load-Balance Information
------------------------------
Rbridge-Id       : 2
Vlag           : 10
Load-Balance Flavor : Source and Destination MAC address and VID based load balancing
switch# show fabric vlag-load-balance all
```

```
Fabric Vlag Load-Balance Information
-------------------------------
Rbridge-Id       : 2
Vlag             : 10
```

17.3　LACP 設定のガイドラインと制限

この章では、別途明確に示されているものを除いて、標準ベースの LAG 構成に適用されます。
LACP を構成する場合は、これら LACP 構成のガイドラインと制限に従ってください。

- 内蔵 DCB スイッチの全てのポートは全二重でのみ動作します。
- switchport インタフェース ー "switchport"インタフェースとして定義されたインタフェースは LAG に結合できません。しかし、LAG は”switchport”として定義してください。
- vLAG では、LACP をご使用下さい。

17.4　デフォルト LACP 構成情報

表 17-2 はデフォルトの LACP 構成情報を一覧しています。

表 17-2　デフォルト LACP 構成パラメータ

パラメータ	デフォルト設定
システムプライオリティ	32768
ポートプライオリティ	32768
タイムアウト	Long（標準 LAG）または short（Brocade　LAG）

17.5　LACP の構成と管理

NOTE
コンフィグレーションを格納するため、'copy running-config startup-config'コマンドを入力してください。

17.5.1　ポートの LACP 有効化

既存の LAG にインタフェースを追加するために、新しいインタフェースに対して同じ LAG グループ番号を使ってこの手続きを繰り返してください。
インタフェースの LACP を有効化するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行

します。

```
switch(config)# interface tengigabitethernet 0/1
```

3．DCB インタフェースを有効化するため、'no shutdown'コマンドを入力します。

```
switch(conf-if-te-0/1)# no shutdown
```

4．DCB インタフェースに対する LACP を設定するため、'channel-group'コマンドを入力します。

```
switch(conf-if)# channel-group 4 mode active type brocade
```

17.5.2 LACP システムプライオリティの設定

LACP が動作中の各スイッチに LACP システムプライオリティを設定します。LACP はシステム ID を形成するためのスイッチ MAC アドレスとして、また他のスイッチとのネゴシエーションの間、システムプライオリティを使用します。
システムプライオリティは、1 から 65535 の範囲の数字で設定できます。数字が大きいほどプライオリティが低くなります。デフォルトプライオリティは 32768 です。

LACP システムプライオリティを設定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．LACP システムプライオリティを指定します。

```
switch(config)# lacp system-priority 25000
```

17.5.3 DCB インタフェースの LACP タイムアウト時間の設定

LACP タイムアウトは、隣接デバイスがタイムアウトするまでの待ち時間を設定します。short 指定の場合は 3 秒、long の場合は 90 秒です。デフォルトは long です。
インタフェースの LACP タイムアウト時間を指定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。

```
switch(config)# interface tengigabitethernet 0/1
```

3．DCB インタフェースを有効化するため、'no shutdown'コマンドを入力します。

```
switch(conf-if-te-0/1)# no shutdown
```

4．DCB インタフェースのタイムアウト時間を指定します。

```
switch(conf-if-te-0/1)# lacp timeout short
```

17.5.4 LAG の LACP 統計情報のクリア

LACP 統計情報カウンタをクリアするため、LAG グループ番号を指定して'clear'コマンドを入力します。
特定の LAG の LACP カウンタをクリアする例

```
switch# clear lacp 42 counters
```

17.5.5 全 LAG グループの LACP 統計情報のクリア

全 LAG グループの LACP 統計情報カウンタをクリアするため、'clear'コマンドを入力します。
LACP カウンタのクリアする例

```
switch# clear lacp counters
```

17.5.6 LACP 情報の表示

LACP 統計情報と構成情報を表示するため'show'コマンドを使います。『Network OS Command Reference』を参照してください。

17.6 LACP トラブルシューティング

LACP 構成でのトラブルシュートのため、次のトラブルシュートのヒントをお使い下さい。
IEEE802.3ad 準拠の動的トラングを設定したがリンクが LAG に組み込まれない場合：

- 両装置での接続ポートのトランクタイプが標準となっているか設定を確認する。
- 両装置での接続ポートが両方ともパッシブモードとなっていないか設定を確認する。いずれー方がアクティブでなければなりません。
- 'no shutdown'コマンドがリンクの両端のインターフェース上で入力されたことを確実にすることによって、port-channel インタフェースが administrative up 状態にあることを確認します。
- port-channel がギガビットインターフェースを使用している場合、speed パラメータを 1000 に設定されていることを確認してください。
- LAG のポートが同一の隣接スイッチに接続されているか確認してください。
- スイッチのシステム ID がユニークかを確認してください。'show lacp sys-id'を入力することで確認できます。
- 両装置で PDU に関するエラーなく LACPDU が送受信されているか確認する。'show lacp counters number'を実行し、受信と送信の統計情報を確認します。統計情報は増加し続けているはずで、ゼロかー定値ではないはずです。もし PUD の受信が増えない場合は、隣接スイッチで'show interface <link-name>'コマンドを入力して、CRC エラーを確認します。もし、PDU の送信が増加しない場合は、'show interface <link-name>'コマンドを入力して、リンクの動作状態を確認し、状態が"up"となっているか確認します。

Brocade ベースのダイナミックトランクがリンク上に設定されている場合、リンクが LAG に参加することはできません：

- リンクの両端のトランクタイプが Brocade として構成されることを確認してください。
- リンクの両端をパッシブモードで構成されていないことを確認してください。いずれー方がアクティブでなければなりません。
- 'no shutdown'コマンドがリンクの両端のインターフェース上で入力されたことを確実にすることによって、port-channel インタフェースが administrative up 状態にあることを確認します。

- LAG のポートが同一の隣接スイッチに接続されているか確認してください。
- スイッチのシステム ID がユニークかを確認してください。'show lacp sys-id'を入力することで確認できます。
- 両装置で PDU に関するエラーなく LACPDU が送受信されているか確認する。'show lacp counters number'を実行し、受信と送信の統計情報を確認します。統計情報は増加し続けているはずで、ゼロか一定値ではないはずです。もし PUD の受信が増えない場合は、隣接スイッチで'show interface <link-name>'コマンドを入力して、CRC エラーを確認します。もし、PDU の送信が増加しない場合は、'show interface <link-name>'コマンドを入力して、リンクの動作状態を確認し、状態が"up"となっているか確認します。
- リンクのファイバーの長さは 7 マイクロ秒のデスキュー値を持っていることを確認してください。そうでない場合は、リンクが LAG に参加することができず、次の RASLOG メッセージが発生します。

  ```
  Deskew calculation failed for link <link-name>.
  ```

  リンクがこの問題が発生した場合は、'show port-channel'コマンドを実行すると、次のメッセージが表示されます。

  ```
  Mux machine state : Deskew not OK.
  ```

  Brocade ベースのスタティックトランクがリンクの上に構成されている場合、リンクが LAG に参加することはできません：
- リンクの両端が、トランクタイプの Brocade として設定され、モードが‘ON’であることを確認してください。
- 'no shutdown'コマンドがリンクの両端のインターフェース上で入力されたことを確実にすることによって、port-channel インタフェースが administrative up 状態にあることを確認します。

標準ベースのスタティックトランクがリンクで構成されている場合、リンクが LAG に参加することはできません：

- リンクの両端が、トランクタイプの標準として設定され、モードが‘ON’であることを確認してください。
- 'no shutdown'コマンドがリンクの両端のインターフェース上で入力されたことを確実にすることによって、port-channel インタフェースが administrative up 状態にあることを確認します。

18 NIC 冗長(track)の設定

18.1 NIC 冗長(track)の概要

NIC 冗長(track)は、チーミング等のサーバでの LAN 冗長化機能と連携して、装置全体の LAN 冗長を実現する機能です。
NIC 冗長(track)は単一のスイッチ上で機能するもので、複数のスイッチ間での冗長機能を提供するものではありません。本機能は、監視対象に設定したインタフェースで障害を検出(リンクダウン)すると、そのインタフェースに関連付けられているインタフェースを自動的にシャットダウンさせるものです。また、逆に監視対象のインタフェースが回復(リンクアップ)すると、自動的に関連付けられているインタフェースもオンラインにします。
本機能の対象となるインタフェースは、物理ポートと LAG です。LAG には、動作状態の LAG メンバー(物理ポート)の最小数を指定することができます。動作状態の LAG メンバーがその閾値以下の場合、LAG は障害状態となり動作状態のメンバーが閾値を越えるまで回復しません。NIC 冗長(track)で LAG を監視対象とした場合も、障害検出はこの閾値設定に従います。

18.2 NIC 冗長(track)の構成

18.2.1 ポート監視の有効化と設定(物理ポート)

インタフェースの監視機能を有効化するために、特権実行モードから次の手順を実行してください。

1. グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2. 障害発生時閉塞するインタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。

```
switch(config)#interface tengigabitethernet 0/9
```

3. インタフェースを有効化するため、'no shutdown'コマンドを入力します。
4. インタフェースに対する track 機能を有効化するため、'track'コマンドを入力します。

```
switch(conf-if)#track enable
```

5. 監視対象インタフェースを指定するため'track'コマンドを入力します。複数のインタフェースを監視する場合は、'track'コマンドを繰り返してインタフェースを追加します。

```
switch(conf-if)#track interface ethernet 0/1
```

NOTE
一つの閉塞対象インタフェースに対して複数インタフェースを監視している場合、いずれかのインタフェースで障害が発生している最中に reload を実行しないで下さい。もし、reload が必要な場合は、閉塞対象インタフェースに関連付けられている監視対象の全てのインタフェースに接続されたケーブルを、一旦抜いてから reload を実行してください。

18.2.2 ポート監視の有効化と設定(LAG)

インタフェースの監視機能を有効化するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．障害発生時閉塞するインタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。

```
switch(config)#interface tengigabitethernet 0/9
```

3．インタフェースを有効化するため、'no shutdown'コマンドを入力します。

4．インタフェースに対する track 機能を有効化するため、'track'コマンドを入力します。

```
switch(conf-if)#track enable
```

5．監視対象インタフェースを指定するため'track'コマンドを入力します。複数のインタフェースを監視する場合は、'track'コマンドを繰り返してインタフェースを追加します。

```
switch(conf-if)#track interface port-channel 10
```

18.2.3 ポート監視の無効化

インタフェースの監視機能を削除するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。

```
switch(config)#interface tengigabitethernet 0/9
```

3．インタフェースを有効化するため、'no shutdown'コマンドを入力します。

4．インタフェースに対する track 機能を削除するため、'no track'コマンドを入力します。

```
switch(conf-if)#no track enable
```

19 LLDP の設定

19.1 LLDP 概要

IEEE 802.1AB Link Layer Discovery Protocol (LLDP)は、正確なネットワークトポロジを検出・維持し、マルチベンダ環境での LAN トラブルシューティングを簡単化するためのネットワーク管理ツールの機能を拡張します。効率的・効果的に LAN 上の様々なデバイスを操作するために、これらのデバイスで有効になっているプロトコルやアプリケーションの構成が正しいことを保証しなければなりません。劇的に拡大するレイヤ２ネットワークでは、ネットワーク管理者にとって静的に監視やネットワーク上の各デバイスを設定することは困難です。
LLDP を用いることで、ルーターやスイッチのようなネットワークデバイスは他のネットワークデバイスに自身の情報を広告し、それらが検出した情報を格納します。デバイスの構成や機能や識別といった詳細情報が広告されます。LLDP は次を定義します。

- 共通の広告メッセージ群
- 広告を転送するためのプロトコル
- 受信される広告に含まれる情報を格納する方法

NOTE
LLDP は、互いに学習するために２つのデバイスに異なるネットワークレイヤプロトコル実行を可能とするデータリンクレイヤ上で実行されます。

LLDP 情報は定期的に送信され、一定時間格納されます。デバイスが LLDP 広告フレームを受信するたびに、デバイスは情報を格納し、タイマーを初期化します。もし、タイマーが有効期間(TTL)に到達すると、LLDP デバイスは、有効で最新の LLDP 情報だけがネットワークデバイスに格納されネットワーク管理システムで利用可能であることが保証されるよう格納情報を削除します。

19.2 レイヤ２トポロジマッピング

LLDP プロトコルにより、ネットワーク管理システムで、レイヤ２ネットワークトポロジを正確に検出及びモデル化することができます。LLDP デバイスは広告を送受信するので、デバイスは隣接デバイスに関して検出した情報を格納します。隣接機器の管理アドレスやデバイスタイプ、ポート ID といった広告データは、ネットワーク上の隣接デバイスが何かを決定するのに役立ちます。

NOTE
Brocade の LLDP 実装は、１対１接続をサポートしています。各インタフェースは一つだけの隣接装置の情報を持ちます。

高機能の管理ツールは、レイヤ２物理トポロジから引き出した LLDP 情報を検索することが出来ます。管理ツールは LLDP の交換情報で提供されたデバイスの管理アドレス経由で、隣接デバイスの検索を続けることが出来ます。このプロセスが繰り返されるので、完全なレイヤ２トポロジがマップされます。

LLDP では、２つのリンクパートナー間のリンクレベル情報の交換を通じて、リンク検出が完成されます。リンクレベル情報は、リンクレベルパートナーで動的な変更を反映して、定期的に更新されます。LLDP の交換情報の基本フォーマットは、タイプ・長さ・値(TLV)のフィールドからなります。
LLDP は、ローカルとリモートの両方のコンフィグレーションのデータベースを保持します。LLDP の規格は、現在３つのカテゴリの TLV をサポートしています。Brocade の LLDP 実装では、Brocade 独自の TVL 拡張を付加しています。４つの TLV セットは次の通りです。

- 基本管理 TLV セット：このセットはレイヤ２トポロジをマップするための情報を提供し、次の TLV を含みます。
  - Chassis ID TLV — ポートを装備するスイッチやルータの ID を提供する。必須 TLV。
  - Port description TLV — 英数字フォーマットでポートの説明を提供する。もし、LAN デバイスが RFC-2863 をサポートしているなら、port description TLV の値は、“ifDescr”オブジェクトと等しい。必須 TLV。
  - System name TLV — 英数字フォーマットでシステム名称を提供する。もし、LAN デバイスが RFC-3418 をサポートしているなら、system name TLV は、“sysName”オブジェクトと等しい。オプション TLV。
  - System description TLV — 英数字フォーマットでネットワークエンティティの説明を提供する。これは、システム名称、ハードウェアバージョン、オペレーティングシステム、サポートしているネットワークソフトウェアを含む。もし、LAN デバイスが RFC-3418 をサポートしているなら、この値は、"sysDescr”オブジェクトと等しい。オプション TVL。
  - System capabilities TLV — デバイスのプライマリ機能とデバイスで有効になっているかどうかをします。ケイパビリティは、２オクテットで示される。第一オクテットは、Repeater, Bridge, WLAN AP, Router, Telephone, DOCSIS cable device, Station, これ以外をそれぞれ示す。第二オクテットはリザーブです。オプション TLV。
  - Management address TLV — ローカルスイッチのアドレスを示す。リモートスイッチは、ローカルスイッチに関連する情報を得るためにこのアドレスを使う。オプション TLV。
- IEEE 802.1 TLV set：このセットは、ローカルとリモートデバイス間の不整合な設定を摘出するための情報を提供する。不整合が検出されるとトラップやイベントが 一度報告される。オプション TLV。このセットは次の TLV を含みます。
  - Port VLANID TLV — VLAN ポートで受信される untagged もしくは優先 tag データに関連したポート VLAN ID(PVID)を示す。
  - PPVLAN ID TLV — VLAN ポートで受信される untagged もしくは優先 tag データに関連したポート及びプロトコルベース VLAN ID(PPVID)を示す。TLV は、ポートがポート及びプロトコルベース VLAN(PPVLANs)をサポートしているかどうか、また、一つもしくはそれ以上の PPVLANs が有効かどうかを示す"flags"フィールドをサポートします。Link Layer Discovery Protocol Data Unit (LLDPDU)の PPVLAN ID TLV の数は、ポートで有効となっている PPVLANs の数に依存する。
  - VLAN name TLV — デバイス上の VLAN の名称を示す。もし、LAN デバイスが RFC-2674 をサポートしているなら、値は“dot1QVLANStaticName”オブジェクトと同じです。LLDPDU の VLAN name TLV の数は、ポートで有効な VLAN の数に依存する。
  - Protocol identity TLV — デバイスのポートでアクセス可能なプロトコルのセットを示す。TLV の

protocol identity フィールドは、プロトコルを認識する受信デバイスを有効にするレイヤ２アドレスの後にオクテット数を含む。例えば、802.3 length (2 オクテット), LLC addresses (2 オクテット), 802.3 control (1 オクテット), protocol ID (2 オクテット), protocol version (1 オクテット)という少なくとも 8 オクテットを含むスパニングツリープロトコルを、デバイスは広告しようとする。

- IEEE 802.3 TLV set：オプション TLV。このセットは次の TLV を含む。
  - MAC/PHY configuration/status TLV — ローカルインタフェースの利用可能な転送方式とビットレート及び現在の転送方式とビットレートを示す。また、現在の設定が auto-negotiation により設定されたか、マニュアルで設定されたかを示す。
  - Power through media dependent interface (MDI) TLV — LAN デバイスの電源制御機能を示す。
  - Link aggregation TLV — LLDPDU を送信するポートに関連したリンクがアグリゲートかのうかどうかを示す。また、現在のリンクがアグリゲートされたか、そしてアグリゲートされているならアグリゲートポート ID を提供する。
  - Maximum Ethernet frame size TLV — デバイスの MAC 及び PHY で実装されている利用可能な最大フレームサイズを示す。

NOTE
内蔵 DCB スイッチは、MDI TLV をサポートしていません。当該情報を含んだフレームはエラーフレームとしてカウントします。

19.3 DCBX 概要

ストレージトラフィックは、DCB により提供されるロスレス通信を要求します。Data Center Bridging(DCB) Capability Exchange Protocol (DCBX)は、より効果的なスケジューリングやリンクトラフィックに対する優先フロー制御を実現するために隣接装置と DCB 関連パラメータを交換します。
DCBX は２つのリンク間でパラメータを交換するために LLDP を使用します。DCBX は、情報交換のために LLDP の基盤上に構築されています。DCBX 交換パラメータは、組織的に規定された TLV にパッケージされます。DCBX プロトコルはリンクの他方から通知を要求します。これにより、LLDP は送受信両方有効にされます。DCBX は、制御用 TLV と機能 TLV の両方をチェックするバージョン番号を必要とします。
DCBX は次の通り、他のプロトコル及び機能と相互作用します。

- LLDP-LLDP は、RSTP や LACP のような別のレイヤ２プロトコルと並行して実行されます。DCBX は、リンクパートナー間でサポートされる機能を伝えるために、LLDP 基盤上に構築されています。DCBX プロトコルと特徴 TLV は LLDP 規格の上流規格として扱われる。
- QoS マネジメント - DCBX のリンクパートナーと交換されるケイパビリティは、ハードウェアスケジューリングや優先フロー制御を制御できるようハードウェアをセットアップするため QoS マネジメントエンティティに受け渡されます。

DCBX の QoS 規格は２つの機能に分割されます。

- Enhanced Transmission Selection
- Priority Flow Control

19.3.1 Enhanced Transmission Selection

コンバージドネットワークでは、異なるトラフィックタイプが個別にネットワーク帯域に影響を与えます。Enhanced Transmission Selection (ETS)の目的は、コンバージドトラフィックの異なる優先設定に基づき帯域を割り当てることです。例えば、プロセス間通信(IPC)トラフィックは、必要なだけ帯域を使用することが出来、帯域のチェックは行わず、LAN や SAN のトラフィックが残りの帯域を共用するなどです。表 19-1 は、IPC,LAN,SAN の３つのトラフィックグループを表しています。ETS は、トラフィックタイプに基づいて帯域を割当、更に次の通り３つのトラフィックの優先度を割り当てます。
Priority 7 のトラフィックは帯域チェックを行わないプライオリティグループ０にマッピングされる
Priority 2 と 3 は、プライオリティグループ１にマッピングされる。
Priority6,5,4,1,0 は、プライオリティグループ２にマッピングされる。
表 19-1 に示すプライオリティ設定は、スイッチのハードウェアでプライオリティグループに変換されます。

表 19-1　IPC,LAN,SAN トラフィックの ETS プライオリティグループ

Priority	Priority group	Bandwidth check
7	0	No
6	2	Yes
5	2	Yes
4	2	Yes
3	1	Yes
2	1	Yes
1	2	Yes
0	2	Yes

19.3.2 Priority Flow Control

Priority Flow Control (PFC)を使うと、コンバージリンク上のトラフィッククラスに対して、既存の LAN 特性を維持しながらあるトラフィッククラスでロスレスフレーム転送を実現することが出来ます。これは、あるインタフェース上の全てのトラフィックに影響を与える伝統的な 802.3 の PAUSE フロー制御とは異なります。
PFC は１バイトのビットマップにより定義されています。各ビットは、ユーザプライオリティを意味しています。もし、ビットが設定されているなら、フロー制御は RX/TX の双方向で有効にされます。

19.4　LLDP の設定に関する注意事項および制約事項

LLDP を設定する時には、LLDP の設定に関する注意事項および制約事項に従ってください。

- Brocade の LLDP の実装では、標準の LLDP 情報に加えて、Brocade 固有の TLV 交換をサポートして

います。

- 必須 TLVs は、常に広告されます。
- LLDP のリンクレベルのパラメータの交換は他のレイヤ 2 プロトコルに対して透過的です。LLDP のリンクレベルのパラメータは、他の利害関係のプロトコルへの LLDP によって報告されます。

NOTE

DCBX 構成は、単純に DCBX 関連の TLV を広告されるように構成することが必要です。詳細な情報は、222 ページの『19.6 LLDP の構成と管理』を参照してください。

19.5　デフォルト LLDP 設定情報

表 19-2 にデフォルト LLDP 設定情報を示します。

表 19-2　デフォルト LLDP 構成情報

パラメータ	デフォルト設定
LLDP グローバルステート	有効
LLDP 受信	有効
LLDP 送信	有効
LLDP 送信間隔	30 秒
受信情報保持時間	120 秒
広告する DCBX 関連 TLV	dctx-tlv

19.6　LLDP の構成と管理

NOTE

コンフィグレーションを格納するため、'copy running-config startup-config'コマンドを入力してください。

19.6.1　装置全体の LLDP の有効化

'protocol lldp'コマンドは、明示的にインタフェースで無効化していなければ、全てのインタフェースで LLDP を有効にします。LLDP はデフォルトで有効となっています。

LLDP を全体で有効化するために、特権実行モードで次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．LLDP 構成モードに移行します。

```
switch(config)# protocol lldp
```

19.6.2 装置全体の LLDP の無効化・リセット

'no protocol lldp'コマンドは、'protocol lldp'コマンドを使用して行われたすべての構成設定をデフォルト設定に戻します。LLDP はデフォルトで有効となっています。

LLDP を全体でリセットするために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．LLDP をリセットします。

```
switch(config)# no protocol lldp
```

LLDP を全体で無効化にするために、グローバルコンフィギュレーションモードから次の手順を実行します。

1．protocol コンフィギュレーションモードに移行するため、'protocol lldp'コマンドを入力します。

```
switch(config)# protocol lldp
```

2．LLDP を無効化します。

```
switch(conf-lldp)# disable
```

19.6.3 LLDP グローバルコマンドオプションの設定

グローバルコンフィグレーションモードから、'protocol lldp'を入力した後、プロンプトが'switch(conf-lldp)#'と表示される LLDP コンフィグレーションモードとなります。このモードでキーワードを使う場合、全てのインタフェースに適用する非デフォルトパラメータ値を設定できます。

(1) ハードウェアのシステム名称の指定

LLDP の装置でのシステム名称は、スイッチの識別に役立ちます。デフォルトでは、SNMP の MIB で指定される"host-name"が使われます。システム名称を指定することにより、LLDP でスイッチの設定をすることが簡単になることが分かるでしょう。

装置のシステム名称を指定するために、特権実行モードで次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．LLDP 構成モードに移行します。

```
switch(config)# protocol lldp
```

3．DCB スイッチのシステム名称を指定します。

```
switch(conf-lldp)# system-name Brocade_Alpha
Brocade_Alpha(conf-lldp)#
```

(2) 装置の LLDP システムディスクリプションの指定

NOTE

ディスクリプションに OS バージョンか MIB で定義する情報を使うことを推奨します。また、システ

ム名とディスクリプションの一部として#$！@などの特殊文字を使用しないでください。

装置の LLDP システムディスクリプションを指定するために、特権実行モードで次の手順を実行してください。システムディスクリプションは、隣接スイッチから参照できます。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．LLDP 構成モードに移行します。

```
switch(config)# protocol lldp
```

3．装置のシステムディスクリプションを指定します。

```
switch(conf-lldp)# system-description IT_1.6.2_LLDP_01
```

(3) LLDP のユーザディスクリプションの指定

LLDP ユーザディスクリプションを指定するために、特権実行モードで次の手順を実行してください。この設定は、ネットワーク管理の目的であり、隣接スイッチから参照できません。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．LLDP 構成モードに移行します。

```
switch(config)# protocol lldp
```

3．LLDP のユーザディスクリプションを指定します。

```
switch(conf-lldp)# description Brocade-LLDP-installed-july-25
```

(4) LLDP フレームの送受信の有効化・無効化

デフォルトでは、LLDP フレームの送受信は有効です。LLDP フレームの送受信を有効化または無効化するため、特権実行モードで次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．下記を実行するためにモードコマンドを入力します。

・LLDP フレームの受信だけを有効化する。

```
switch(conf-lldp)# mode rx
```

・LLDP フレームの送信だけを有効化する。

```
switch(conf-lldp)# mode tx
```

・全ての LLDP フレームの送受信を無効化する。

```
switch(conf-lldp)# mode no mode
```

(5) LLDP フレームの送信間隔の設定

LLDP フレームの送信間隔を設定するため、特権実行モードで次の手順を実行してください。デフォルトは 30 秒です。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力し

ます。

2．LLDP 構成モードに移行します。

```
switch(config)# protocol lldp
```

3．LLDP フレームの送信か間隔を設定します。

```
switch(conf-lldp)# hello 45
```

(6) 受信の保持時間の設定

受信デバイス情報の保持時間を設定するため、特権実行モードで次の手順を実行してください。これは､隣接情報を無効とするまでに見逃すことができる連続するLLDP helloパケットの数を指定します。デフォルトは４です。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．LLDP 構成モードに移行します。

```
switch(config)# protocol lldp
```

3．受信の保持時間を設定します。

```
switch(conf-lldp)# multiplier 6
```

(7) オプション LLDP TLV の広告

オプションの LLDP TVL を広告するために、特権実行モードで次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．LLDP 構成モードに移行します。

```
switch(config)# protocol lldp
```

3．オプションの LLDP TVL を広告するよう設定します。

```
switch(conf-lldp)# advertise optional-tlv management-address port-description
system-capabilities system-name system-description
```

(8) LLDP DCBX 関連 TLV の広告設定

デフォルトでは、スタンドアロンモードのスイッチでは、”dcbx-tlv”のみを広告します。

Brocade VCS ファブリックモードのスイッチでは、以下の TLV がデフォルトで広告されます。

- dcbx-tlv
- dcbx-fcoe-app-tlv
- dcbx-fcoe-logical-link-tlv

DCBX 関連 TLV を広告するために、特権実行モードで次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．LLDP 構成モードに移行します。

```
switch(config)# protocol lldp
```

3．下記のコマンドを使用して、DCBX 関連 TLV を広告します。

- `switch(conf-lldp)# advertise dcbx-fcoe-app-tlv`
- `switch(conf-lldp)# advertise dcbx-fcoe-logical-link-tlv`
- `switch(conf-lldp)# advertise dcbx-tlv`
- `switch(conf-lldp)# advertise dot1-tlv`
- `switch(conf-lldp)# advertise dot3-tlv`

(9) iSCSI 優先度の設定

iSCSI 優先度の設定は、DCBX iSCSI TLV で広告される優先度を設定します。
iSCSI TVL は、接続されている CEE 機能が有効となっているサーバ及びターゲットへの iSCSI トラフィックの構成パラメータを広告するだけです。スイッチでは、広告されたパラメータが iSCSI サーバやターゲットでの使用を確認も強制もしません。
iSCSI 優先度を設定するために、特権実行モードで次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．LLDP 構成モードに移行します。

```
switch(config)# protocol lldp
```

3．iSCSI 優先度を設定します。

```
switch(conf-lldp)# lldp iscsi-priority 4
```

NOTE
デフォルトの iSCSI 優先度は 4 で、別の値に iSCSI の優先度を変更しない限り表示されません。

4．TLV を広告します。

```
switch (conf-lldp)# advertise dcbx-isci-app-tlv
```

(10) LLDP プロファイルの設定

スイッチ上で最大 64 のプロファイルを設定できます。'no profile'コマンドを使用して、プロファイル全体を削除できます。
LLDP プロファイルを設定するために、特権実行モードで次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．LLDP 構成モードに移行します。

```
switch(config)# protocol lldp
```

３．プロファイル名称を設定します。

```
switch(conf-lldp)# profile UK_LLDP_IT
```

４．プロファイルのディスクリプションを指定します。

```
switch(conf-lldp-profile-UK_LLDP_IT)# description standard_profile_by_Jane
```

５．LLDP フレームの送受信を有効化します。

```
switch(conf-lldp-profile-UK_LLDP_IT)# no mode
```

６．LLDP 更新情報の送信間隔を設定します。

```
switch(conf-lldp-profile-UK_LLDP_IT)# hello 10
```

７．受信に対する保持時間を設定します。

```
switch(conf-lldp-profile-UK_LLDP_IT)# multiplier 2
```

８．オプション LLDP TLV を広告します。

```
switch(conf-lldp)# advertise optional-tlv management-address port-description
system-capabilities system-name system-description
```

９．LLDP DCBX 関連 TLV を広告します。

```
switch(conf-lldp-profile-UK_LLDP_IT)# advertise dot1-tlv
switch(conf-lldp-profile-UK_LLDP_IT)# advertise dot3-tlv
switch(conf-lldp-profile-UK_LLDP_IT)# advertise advertise dcbx-tlv
switch(conf-lldp-profile-UK_LLDP_IT)# advertise dcbx-fcoe-logical-link-tlv
switch(conf-lldp-profile-UK_LLDP_IT)# advertise dcbx-fcoe-app-tlv
switch(conf-lldp-profile-UK_LLDP_IT)# advertise dcbx-iscsi-app-tlv
```

NOTE

'dot1.tlv'と'dot3.tlv'は広告しないことを推奨します。この構成は、機能的な問題を引き起こす可能性があります。

１０．特権実行モードに戻ります。

```
switch(conf-lldp-profile-UK_LLDP_IT)# end
```

１１．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

```
switch(conf-lldp-profile-UK_LLDP_IT)# end
switch# copy running-config startup-config
```

(11) iSCSI プロファイルの設定

インタフェース個別に適用する iSCSI プロファイルを設定することが出来ます。しかし、優先ビットはインタフェース毎に手動で設定しなければなりません。'no profile name'コマンドでプロファイル全体を削除することが出来ます。

iSCSI プロファイルを設定するために、特権実行モードから次の手順を実行してください。

１．cee-map が既に作成されていない場合、cee-map を設定します。

CEE-map コマンドの設定については、『Network OS Command Reference』を参照してください。

```
switch(config)# cee-map default
switch(conf-ceemap)# priority-group-table 1 weight 50
```

```
switch(conf-ceemap)# priority-group-table 2 weight 30 pfc on
switch(conf-ceemap)# priority-group-table 3 weight 20 pfc on
switch(conf-ceemap)# priority-table 1 1 1 1 2 3 1 1
```

'priority-table'コマンドの構文：

```
priority-table PGID0 PGID1 PGID2 PGID3 PGID4 PGID5 PGID6 PGID7
```

・PGID0 は、CoS=0 に設定されたすべてのパケットのための優先順位のグループ ID を設定します。PGID 値の範囲は、DWRR 優先グループのための 0 から 7 と完全優先グループのための 15.0 から 15.7 です。
・PGID1 は、CoS=1 に設定されたすべてのパケットのための優先順位のグループ ID を設定します。PGID 値の範囲は、DWRR 優先グループのための 0 から 7 と完全優先グループのための 15.0 から 15.7 です。
・PGID2 は、CoS=2 に設定されたすべてのパケットのための優先順位のグループ ID を設定します。PGID 値の範囲は、DWRR 優先グループのための 0 から 7 と完全優先グループのための 15.0 から 15.7 です。
・PGID3 は、CoS=3 に設定されたすべてのパケットのための優先順位のグループ ID を設定します。PGID 値の範囲は、DWRR 優先グループのための 0 から 7 と完全優先グループのための 15.0 から 15.7 です。
・PGID4 は、CoS=4 に設定されたすべてのパケットのための優先順位のグループ ID を設定します。PGID 値の範囲は、DWRR 優先グループのための 0 から 7 と完全優先グループのための 15.0 から 15.7 です。
・PGID5 は、CoS=5 に設定されたすべてのパケットのための優先順位のグループ ID を設定します。PGID 値の範囲は、DWRR 優先グループのための 0 から 7 と完全優先グループのための 15.0 から 15.7 です。
・PGID6 は、CoS=6 に設定されたすべてのパケットのための優先順位のグループ ID を設定します。PGID 値の範囲は、DWRR 優先グループのための 0 から 7 と完全優先グループのための 15.0 から 15.7 です。
・PGID7 は、CoS=7 に設定されたすべてのパケットのための優先順位のグループ ID を設定します。PGID 値の範囲は、DWRR 優先グループのための 0 から 7 と完全優先グループのための 15.0 から 15.7 です。
CEE マップ構成のプライオリティテーブルは、PGID 15.0 を CoS7 専用とすることが必要です。この規制のために、PGID15.0 がプライオリティテーブル構成の最後のパラメータとして構成されることを確認してください。

〝priority-table 1 2 2 2 2 2 2 15.0〟構文の説明は、次のとおりです。

これは、2 の DWRR 優先度グループ ID を CoS=1、CoS=2、CoS=3、CoS=4、CoS=5、CoS=6 に、1 の優先度グループ ID を CoS= 0 に、完全優先グループを CoS=7 に定義したことを示

します。
これはプライオリティグループテーブルに CEE プライオリティーを割り当てる 1 つの方法です。それは 8 つ入力 CoS をそれぞれのプライオリティグループにマップします。
VCS モードでは、トラフィッククラスは、すべて絶対優先（802.1Q デフォルト）または絶対優先と DWRR トラフィッククラスの組み合わせです。

2．LLDP 構成モードに移行します。

```
switch(conf-ceemap)# protocol lldp
```

3．iSCSI のための LLDP プロファイルを作成します。

```
switch(conf-lldp)# profile iscsi_config
```

4．iSCSI TLV を広告します。

```
switch(conf-lldp-profile-iscsi_config)# advertise dcbx-iscsi-app-tlv
```

5．指定したインタフェースの構成モードに移行します。

```
switch (conf-lldp-profile-iscsi_config)# interface te 0/1
```

6．インタフェースに CEE プロビジョニングマップを適用します。

```
switch(conf-if-te-0/1)# cee default
```

7．iSCSI 用に生成した LLDP プロファイルを適用します。

```
switch(conf-if-te-0/1)# lldp profile iscsi_config
```

8．インタフェースに対する iSCSI 優先ビットを設定します。

```
switch(conf-if-te-0/1)# lldp iscsi-priority-bits 4
```

9．追加するインタフェースに対して手順 5 から 8 を繰り返します。

19.6.4 LLDP のインタフェースレベルコマンドオプションの設定

インタフェースに割り当てられるのは、一つの LLDP プロファイルだけです。もし、インタフェースレベルの lldp profile を使わないなら、グローバルコンフィグレーションが使われます。もし、グローバルコンフィグレーションが無い場合、装置のデフォルト値が使用されます。
LLDP のインタフェースレベルコマンドのオプションを設定するため、特権実行モードで次の手順を実行してください。

1．DCB インタフェースタイプとスロット番号を指定して、'interface'コマンドを入力します。

```
switch(config)# interface tengigabitethernet 0/10
```

2．インタフェースに LLDP プロファイルを適用します。

```
switch(conf-if-te-0/10)# lldp profile network_standard
```

3．特権実行モードに戻ります。

```
switch(conf-if-te-0/10)# end
```

4．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

19.6.5 LLDP 関連情報の消去

LLDP 関連情報を消去するため、特権実行モードで次の手順を実行してください。

1．LLDP 隣接情報をクリアするため、'clear'コマンドを使います。

```
switch# clear lldp neighbors interface tengigabitethernet 0/1
```

2．LLDP 統計情報をクリアするため、'clear'コマンドを使います。

```
switch# clear lldp statistics interface tengigabitethernet 0/1
```

19.6.6 LLDP 関連情報の表示

LLDP 関連情報を表示するため、特権実行モードから次の手順を実行してください。

1．LLDP 一般情報を表示するため、'show lldp'コマンドを使用します。

```
switch# show lldp
```

2．LLDP インタフェース関連情報を表示するため、'show lldp'コマンドを使用します。

```
switch# show lldp interface tengigabitethernet 0/1
```

3．LLDP 隣接情報を表示するため、'show lldp'コマンドを使用します。

```
switch# show lldp neighbors interface tengigabitethernet 0/1 detail
```

20 アクセスコントロールリスト(ACL)の設定

20.1 ACL 概要

NOTE
Network OS v3.0.0 リリースでは、入力レイヤ 2 MAC アクセス制御リスト（ACL）およびレイヤ 3 IP アクセス制御リストの両方がサポートされています。

ACL はハードウェアに対するトラフィックをフィルタし、ACL が適用されたインタフェースを経由して受信するフレームを許可したり拒否したりします。Network OS V3.0.0 でサポートされているレイヤ 2 の以下の 3 種類のインターフェースに ACL を適用することができます。

- 物理（10 ギガビットイーサネットとギガビットイーサネット）
- VLAN
- ポートチャネル（静的 LAG と動的 LAG）

各 ACL は、フレームに適用する許可と拒否のステートメント(ルール)の独特のコレクションです。インタフェースでフレームが受信されると、スイッチは、転送が許可されているフレームかを検証するためインタフェースに適用された ACL とフレームのフィールドを比較します。スイッチは、シーケンシャルに各ルールとフレームを比較し、フレームを転送するか廃棄します。
スイッチは与えられたインタフェースに設定されているオプションに関連した ACL を検査します。フレームが到着すると、ACL はインタフェースに設定された全てのオプションに関連する ACL が検査されます。MAC ACL を使って、MAC アドレスとイーサタイプに基づきトラフィックを特定しフィルタすることが出来ます。
ACL の基本的な効果は下記の通りです。

- セキュリティ手段を提供する
- トラフィックを低減させることでネットワークリソースを確保する
- 好まれざるトラフィックとユーザをブロックする
- DoS 攻撃の機会を低減する

MAC ACL は２つのタイプがあります。

- 標準 ACL - 受信フレームの送信元 MAC アドレスからトラフィックを許可及び拒否します。送信元アドレスに基づくトラフィックをフィルタする必要がある場合、標準 ACL を使います。
- 拡張 ACL -受信フレームの送信元及び受信元 MAC アドレスからトラフィックを許可及び拒否します。

MAC ACL は次のインタフェースタイプをサポートしています。

- 物理インタフェース
- 論理インタフェース(LAG)
- VLAN

20.2　デフォルト ACL 設定

スイッチ上に適用されているポリシーが一つも無い場合、これらのデフォルトの ACL ルールが Network OS で有効です。

- seq 0 は、tcp any any eq 22 を許可します。
- seq 1 は、tcp any any eq 23 を許可します。
- seq 2 は、tcp any any eq 897 を許可します。
- seq 3 は、tcp any any eq 898 を許可します。
- seq 4 は、tcp any any eq 111 を許可します。
- seq 5 は、tcp any any eq 80 を許可します。
- seq 6 は、tcp any any eq 443 を許可します。
- seq 7 は、udp any any eq 161 を許可します。
- seq 8 は、udp any any eq 111 を許可します。
- seq 9 は、tcp any any eq 123 を許可します。
- seq 10 は、tcp any any の範囲 600 から 65535 を許可します。
- seq 11 は、udp any any の範囲 600 から 65535 を許可します。

20.3　ACL 設定のガイドラインと制限

ACL を設定する場合、次のガイドラインと制約に従ってください。

- ACL ではルールの順番が重要です。最初のルールがトラフィックにマッチすると、以降の処理はフレームに適用されません。
- 標準 ACL と拡張 ACL は同じ名称にできません。
- ACL のルールリストの最後に追加されるデフォルト許可ルールがあります。この暗黙のルールは、ACL に関連付けられている順序リスト内の設定されたルールのいずれにも一致しない、すべてのレイヤ 2 ストリームを許可します。

20.4　ACL の構成と管理

NOTE

コンフィグレーションを格納するため、'copy running-config startup-config'コマンドを入力してください。

20.4.1　標準 MAC ACL の作成とルールの追加

NOTE

MAC ACL のルールに割り当てられた全てのシーケンス番号は、'sequence'コマンドで変更できます。詳細は、236 ページの『20.4.7 MAC ACL のシーケンス番号の並び替え』を参照下さい。

レイヤ 2 インターフェースに適用されるまで、MAC ACL が有効になりません。234 ページの 『20.4.3 DCB インターフェースへの MAC ACL の適用』および 234 ページの『20.4.4 VLAN インタフェースへの MAC ACL 適用』を参照してください。
MAC ACL の作成とルールを追加するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．標準 MAC ACL の作成し、ACL コンフィグレーションモードに移行します。
この例では、標準の MAC ACL の名前は "test_01"としています。

```
switch(config)# mac access-list standard test_01
switch(conf-macl-std)#
```

3．送信元 MAC アドレスでトラフィックを廃棄するよう MAC ACL にルールを追加するため、'deny' コマンドを入力します。

```
switch(conf-macl-std)# deny 0022.3333.4444 count
```

4．送信元 MAC アドレスでトラフィックを許可するよう MAC ACL にルールを追加するため、'permit' コマンドを入力します。

```
switch(conf-macl-std)# permit 0022.5555.3333 count
```

5．指定した順序で MAC ACL ルールを生成するため'seq'コマンドを入力します。

```
switch(conf-macl-std)# seq 100 deny 0011.2222.3333 count
switch(conf-macl-std)# seq 1000 permit 0022.1111.2222 count
```

6．特権実行モードに戻ります。

```
switch(conf-macl-std)# end
```

7．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

20.4.2 拡張 MAC ACL の作成とルールの追加

NOTE
MAC ACL のルールに割り当てられたすべてのシーケンス番号を変更するには、'resequence'コマンドを使用できます。詳細は、236 ページの『20.4.7 MAC ACL のシーケンス番号の並び替え』を参照下さい。

MAC ACL の名称は最大 64 文字です。レイヤ 2 インターフェースに適用されるまで、MAC ACL が有効になりません。234 ページの『20.4.3 DCB インターフェースへの MAC ACL の適用』および 234 ページの『20.4.4 VLAN インタフェースへの MAC ACL 適用』を参照してください。

拡張 MAC ACL の作成とルールを追加するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．拡張 MAC ACL の作成し、ACL コンフィグレーションモードに移行します。

```
switch(config)# mac access-list extended test_02
```

3．送信元及び宛先 MAC アドレスでトラフィックを許可するためルールを作成します。

```
switch(conf-macl-ext)# permit 0022.3333.4444 0022.3333.5555
```

4．MAC ACL にルールを挿入するために'seq'コマンドを使用します。

```
switch(conf-macl-std)# seq 5 permit 0022.3333.4444 0022.3333.5555
```

5．特権実行モードに戻ります。

```
switch(conf-macl-std)# end
```

6．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

20.4.3 DCB インターフェースへの MAC ACL の適用

適用する ACL が存在し、この DCB のインターフェースに必要な方法で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ます。ACL は、明示的に'access-group'コマンドを使用してインターフェースに適用されるまで機能しません。DCB インタフェースで受信されるフレームはフィルタされます。

NOTE

ACL がインターフェースにアクセスグループとして適用する前に、DCB インターフェースがレイヤ 2 スイッチポートとして設定する必要があります。

DCB インターフェースに MAC ACL を適用するには、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インターフェースタイプとスロット/ポート番号を指定するには、'interface'コマンドを入力します。

```
switch(config)# interface tengigabitethernet 0/1
```

3．インターフェースをレイヤ 2 スイッチポートとして設定するために、'switchport'コマンドを入力します。

4．入力方向のレイヤ 2 DCB のインターフェースに適用される MAC ACL を指定するには、'mac-access-group'コマンドを入力します。

```
switch(conf-if-te-0/1)# mac access-group test_02 in
```

20.4.4 VLAN インタフェースへの MAC ACL 適用

適用する ACL が存在し、この VLAN インターフェースに必要な方法で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ます。ACL は'access-group'コマンドを使って明確に適用されるまで機能しません。VLAN で受信されるフレームはフィルタされます。

VLAN インタフェースに MAC ACL を適用するには、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．VLAN インタフェースに MAC ACL を適用するため、'interface'コマンドを入力します。

```
switch(config)# interface vlan 50
```

3．VLAN に適用した MAC ACL を指定して'mac-access-group'コマンドを入力します。

```
switch(config-Vlan-50)# mac access-group test_02 in
```

20.4.5 MAC ACL ルールの変更

MAC ACL の存在しているルールは変更できません。その場合、一旦ルールを削除して、必要な変更を行ったルールを再作成してください。

既存のルールの間に現在のシーケンス番号付けが許すより多くのルールを加える必要がある場合、シーケンス番号を再度割り当てるために、'resequence'コマンドを使用することができます。詳細については、236 ページの 『20.4.7 MAC ACL のシーケンス番号の並び替え』を参照してください。

変更したいルールを指定するためにシーケンス番号を使います。シーケンス番号がないと、リストの最後に新しいルールが追加されて、既存のルールは変更されません。

NOTE

'permit'と'deny'キーワードにより、多くの異なるルールを作成できます。このセクションの例では、MAC ACL を修正するために必要な基本的な知識を示します。

NOTE

この例は、test_02 が"deny any any"オプションで番号 100 のルールを持っていることを想定しています。

MAC ACL を修正するため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．'test_02'という名前の ACL を指定するため、'mac'コマンドを入力します。

```
switch(config)# mac access-list extended test_02
```

3．存在するルール 100 を削除するため、'no seq'コマンドを入力します。

```
switch(conf-macl-ext)# no seq 100
```

または、新しいパラメータで番号 100 のルールを再作成するため、'seq'コマンドを入力します。

```
switch(conf-macl-ext)# seq 100 permit any any
```

20.4.6 MAC ACL の削除

DCB または VLAN インタフェイスに MAC ACL を適用する access-group が最初に削除されない限り、MAC ACL は、システムから削除することはできません。

MAC ACL を削除するため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．削除したい ACL を指定して削除するため'mac'コマンドを入力します。この例では、拡張 MAC ACL 名称は"test_02"です。

```
switch(config)# no mac access-list extended test_02
```

20.4.7 MAC ACL のシーケンス番号の並び替え

MAC ACL のルールにつけたシーケンス番号は並び替えが可能です。シーケンス番号の並び替えは、ACL にルールを挿入する時、利用可能なシーケンス番号が不足する場合に使います。デフォルトの初期シーケンス番号は 10 であり、デフォルトの増分は、標準および拡張 MAC ACL で 10 です。
最初のルールは、開始番号で指定した番号となります。各継続するルールは、先に実行されたルールより大きい番号となります。番号上の違いは、指定された増分により決定されます。開始番号と増分は 1 から 65535 の範囲です。
例えば、下記の'resequence'コマンドで示す内容は、"test_02"という名前のルールに 50 の番号を割り当て、次のルールに 55、三番目のルールに 60 のシーケンス番号を割り当てます。

```
switch# resequence access-list mac test_02 50 5
```

20.5 IP ACL

IP ACL は、スイッチへのアクセスを制御します。ポリシーは、スイッチから出力とアウトバウンド管理トラフィックを制御でききません。IP ACL は、同時に IPv4 と IPv6 をサポートしています。
IP ACL は、パケットフィルタリングファイアウォールとして、インターフェースに適用されるルールのセットです。各ルールは、トラフィックが送信元および宛先 IP アドレス、プロトコルまたはポートの組み合わせを拒否または許可するかどうかを定義します。
各 ACL は、一意の名前を持っている必要がありますが、定義する ACL の数には制限はありません。ACL は、IPv4/v6 のどちらかの一方にのみ対応するルールを含むことができます。IP のバージョン毎に、1 つの ACL を一度にインターフェース上で有効にすることができます。言い換えれば、パケットフィルタリング用に IPv4 用の ACL が一つと、IPv6 用の ACL が一つをインタフェースに有効にすることができます。
トラフィックをフィルタリングするために、インターフェースに適用した ACL の各ルールは、シーケンス番号の昇順でチェックされます。4,294,967,290 個のルールがアクセスリストに追加することができます。ACL がインターフェースに適用される時、ACL に 256 以上のルールがある場合、最も小さいものから 256 個のルールが適用されます。ACL が全くルールも含まずインターフェースに適用される場合、何も実行されず、すべての入力トラフィックがインターフェースを通過するように許可されます。
一旦 IP ACL ルールが作成されると、そのオプションは何も変更することができません。

スイッチのデフォルト設定では、1 つの IPv4 ACL と 1 つの IPv6 ACL がインターフェースに適用され、2 つの ACL で構成されています。
以下の IP アクセスリストの 2 種類があります。

- 標準：送信元 IP アドレスだけに対するルールを含みます。ルールは、そのソース IP アドレスのすべてのポートに適用できます。
- 拡張：IP プロトコル、送信元 IP、送信先 IP、送信元ポートと送信先ポートの組合せに対するルールを含みます。

20.5.1 IP ACL パラメータ

表 20-1 に IP アクセスコントロールリスト（ACL）のパラメータとその定義を示します。

NOTE

内蔵 DCBSW 上の NOS3.0 は、拡張 IP ACL ルールに対してのみサポートされているパラメータは eq パラメータです。

表 20-1　IP ACL パラメータ

ACL／ルールタイプ	IP ACL パラメータ	IP ACL パラメータ定義
標準 IP ACL	name	標準 IP アクセスコントロールリストの名前。名前は英数字で、63 を超える文字を含めることはできません。
標準 IP ACL ルール	seq	ルールのシーケンス番号。番号は 0 から 4294967290 までででなければなりません。
	permit/deny	ルールで指定された組み合わせのためのトラフィックを許可または拒否するかどうかを指定します。
	any/host	入力トラフィックをフィルタリングする必要があるホストの IP アドレス。
拡張 IP ACL	name	拡張 IP アクセスコントロールリストの名前。名前は英数字で、63 を超える文字を含めることはできません。
拡張 IP ACL ルール	seq	ルールのシーケンス番号。番号は 0 から 65535 までででなければなりません。
	permit/deny	ルールで指定された組み合わせのためのトラフィックを許可または拒否するかどうかを指定します。
	protocol	フィルタリング対象の IP パケットのタイプを示します。
	any/host	着信トラフィックをフィルタリングする必要があるホストの IP アドレス。
	any	出力または発信トラフィックの制御がブロックされているホストの IP アドレス。出力と発信トラフィックがブロックされるため、宛先アドレスは常に "any"（また、ホストの仮想 IP アドレスもカバーしています）。
	port-number	フィルタが適用されるため、送信元または宛先ポートを示します。これは UDP と TCP の両方に適用されます。番号は 0 から 65535 までです。
	range	ACL ルールを介してフィルタされている必要があり、複数の宛先ポートがある場合は、開始ポートと終了ポートを指定する範囲のパラメータを使用します。
	eq	ACL ルールを介してフィルタしなければならない唯一の宛先ポートがある場合、eq パラメータを使用します。
	dscp value	受信したパケットの dscp 値に対して、指定された値を比較します。有効な値の範囲は 0 から 63 までです。
	ack, fin, rst, sync, urg, psh	TCP フラグの任意の組み合わせを指定することができます。
拡張 IP ACL ルール	Log	フィルタに一致するパケットは CPU に送信され、対応するログエントリが生成されます。オプションのログパラメータは、ログメカニズムを有効にします。このオプションは、許可と拒否でのみ使用可能です。

20.5.2 標準 IP ACL の作成

標準 IP ACL を作成するには、グローバルコンフィギュレーションモードで次の手順を実行します。

1. コンフィギュレーションモードに移行するには、'ip access-list standard'コマンドを使用します。

```
switch(config)# ip access-list standard stdACL3
```

2. ACL のためのルールを入力するには、'seq'コマンドを使用します。複数のルールを入力することができます。

```
switch(config-ip-std)# seq 5 permit host 10.20.33.4
switch(config-ip-std)# seq 15 deny any
```

3. グローバルコンフィギュレーションモードに戻るには、'exit'コマンドを使用します。変更は自動的に保存されます。

```
switch(config-ip-std)# exit
switch(config)#
```

20.5.3 拡張 IP ACL の作成

拡張 IP ACL を作成するには、グローバルコンフィギュレーションモードで次の手順を実行します。

1. コンフィギュレーションモードに移行するには、'ip access-list extended'コマンドを使用します。

```
switch(config)# ip access-list extended extdACL5
```

2. ACL のためのルールを入力するには、'seq'コマンドを使用します。複数のルールを入力することができます。

```
switch(config-ip-ext)# deny udp any any range 10 25
switch(config-ip-ext)# seq 5 deny tcp host 10.24.26.145 any eq 23
switch(config-ip-ext)# seq 7 deny tcp any any eq 80
switch(config-ip-ext)# seq 15 permit tcp any any
```

3. グローバルコンフィギュレーションモードに戻るには、'exit'コマンドを使用します。変更は自動的に保存されます。

```
switch(config-ip-std)# exit
switch(config)#
```

NOTE

range パラメータを使用する場合は、'seq'を指定することはできません。'seq'を指定しないルールは、シーケンス番号が自動的に割当てられ、定義済みルールに追加される(後に評価される)ことになります。従って、優先したいルールで range パラメータを使用する場合は、最初に評価する順番に定義してください。

20.5.4 管理インターフェースへの IP ACL の適用

IP ACL を適用するには、グローバルコンフィギュレーションモードで次の手順を実行します。

1. 管理インターフェースのためのコンフィギュレーションモードに移行するには、'interface'コマンドを使用します。

```
switch(config)# interface Management 1/0
```

2．IPv4 標準 ACL を適用するには、'ip access-group'コマンドを使用します。

```
switch(config-Management-1/0)# ip access-group stdACL3 in
```

3．IPv6 標準 ACL を適用するには、'ip access-group'コマンドを使用します。

```
switch(config-Management-1/0)# ipv6 access-group stdV6ACL1 in
```

4．IPv4 拡張 ACL を適用するには、'ip access-group'コマンドを使用します。

```
switch(config-Management-1/0)# ip access-group extdACL5 in
```

5．グローバルコンフィギュレーションモードに戻るには、'exit'コマンドを使用します。変更は自動的に保存されます。

```
switch(config-ip-std)# exit
switch(config)#
```

NOTE

拡張 ACL を着信及び発信トラフィックに適用する場合、ルールが同一であっても、異なる拡張 ACL を作成して各々を着信または発信トラフィックに適用してください。

20.5.5 IP ACL 設定の表示

IP ACL の設定を表示するには、特権実行モードで'show running-config ip access-list'コマンドを使用します。

```
switch# show running-config ip access-list
ip access-list standard stdACL3
 seq 5 permit host 10.20.33.4
 seq 7 permit any
!
ip access-list extended extdACL5
 seq 5 deny tcp host 10.24.26.145 any eq 23
 seq 7 deny tcp any any eq 80
 seq 10 deny udp any any range 10 25
 seq 15 permit tcp any any
```

21 QoS の設定

21.1 Standalone QoS

スタンドアロン QoS は、スイッチからスイッチへのトラフィックの流れを制御する機能を提供します。異なる用途で使われる異なるトラフィックが存在するネットワークにおいて、QoS の目的はトラフィックタイプ毎に仮想パイプを提供することです。スイッチを通過するトラフィックは、イーサのマルチキャストトラフィックかユニキャストトラフィックに分類できます。マルチキャストトラフィックは、送信元は一つですが複数の宛先に転送されます。ユニキャストトラフィックは、一つの送信元から一つの宛先に転送されます。
入力ポートから出力ポートへ流れる全てのトラフィックは、送信先ポートと CoS の優先レベルに基づいて QoS がセットされます。untrust インタフェースは、接続先が QoS をサポートしていないや管理セグメントに接続する場合に使います。

QoS の機能は以下の通りです。

- リライト ― 優先度や VLAN ID のような有用なヘッダフィールドのリライトやマーキングが可能
- キューイング ― 転送待ちのフレームを一時メモリに保留する。入力ポート、出力ポート、定義されたユーザのプライオリティレベルに基づきキューが選択される。
- 輻輳制御 ― キューが一杯になって全てのバッファが枯渇した時、フレームは破棄されます。これは、アプリケーションのスループットに影響を与えます。輻輳制御技術は、逆にネットワークスループットに影響することなく、キュー溢れのリスクを軽減するために使われます。輻輳制御機能としては、IEEE802.3x の Pause、Tail Drop、Priority Flow Control(PFC)があります。
- マルチキャストレート制御 ― 多くのマルチキャストアプリケーションは輻輳制御技術に適合できません。そしてスイッチデバイスによるフレーム複製はこの問題を悪化させます。マルチキャストレート制御は、マルチキャストトラフィックの影響を最小限にするようフレーム複製を制御します。
- データセンタブリッジングーDCB は、単一の相互接続技術の上に、データセンター内の LAN、SAN、および IPC 等の様々なアプリケーションの融合を可能にする拡張イーサネットについて記述します。

21.2 リライト

フレームのヘッダフィールドのリライトは、一般的にはエッジデバイスにより実行されます。隣接デバイスが信頼できず、フレームをマーキングすることが出来ない場合か、異なる QoS を使用する場合に、ネットワークに入るもしくは出る場合にフレームにリライトが必要です。
フレームリライトは、CoS と VLAN の組で取り扱います。送出するフレームの CoS リライトは後のキューイングの章で述べる各フレームに結び付られたユーザプライオリティマッピングに基づいて行われます。

21.3　キューイング

キューの選択は、設定されたユーザプライオリティに対して受信フレームをマッピングにより始まります。その後、各ユーザプライオリティマッピングはスイッチの８つのユニキャストまたは８つのマルチキャストトラフィッククラスキューの１つへ割り当てられます。

21.3.1　ユーザプライオリティマッピング

受信フレームをユーザプライオリティにマッピングする方法は幾つかあります。
もし、近隣デバイスが QoS に対応していないまたは適切に QoS を設定できない場合、インタフェースは untrust とみなされます。全てのトラフィックは信頼できるインタフェースに明確なポリシーをもってユーザプライオリティにマッピングされるべきです。もし、マッピングされない場合は、IEEE802.1Q のデフォルトプライオリティマッピングが使われます。もしインタフェースに QoS 設定が可能な信頼できるものなら、CoS ヘッダフィールドが解釈されます。

スタンドアロンモード：

- 全ての受信プライオリティ７の tag 付きパケットはキュー７(TC7)にカウントされる。
- untag フレームはキュー７(TC7)にカウントされる。

NOTE
この章で述べられているユーザプライオリティマッピングは、ユニキャスト及びマルチキャストトラフィックの両方に適用されます。

(1)　untrust インタフェースに対するデフォルトユーザプライオリティ
レイヤ２の QoS において、untrust に設定された場合は、デフォルトのユーザプライオリティである０にマッピングされるのがデフォルトの動作です。これはベストエフォートであることを意味していいます。
表 21-1 は、レイヤ２での QoS における untrust ユーザプライオリティのマッピングです。

表 21-1　untrust インタフェースのデフォルトユーザプライオリティ値

入力フレームの CoS 値	ユーザプライオリティ
0	port <user priority> (default 0)
1	port <user priority> (default 0)
2	port <user priority> (default 0)
3	port <user priority> (default 0)
4	port <user priority> (default 0)
5	port <user priority> (default 0)
6	port <user priority> (default 0)
7	port <user priority> (default 0)

NOTE
untag フレームは CoS 値 0 と解釈されます。

ユーザプライオリティマッピングを使うことにより、デフォルトのユーザプライオリティマッピングを上書きすることが出来ます。隣接デバイスが trust で、QoS 設定機能が利用できるならば、レイヤ２の QoS の信頼は CoS 値と IEEE802.1Q のデフォルトマッピングが適用されます。
表 21-2 は、802.1Q のデフォルトマッピングに準拠したレイヤ２CoS ユーザプライオリティ生成テーブルを示しています。もし、CoS 値の変更が必要であれば、ポート毎のデフォルトユーザプライオリティテーブルを変更することが出来ます。

表 21-2　IEEE802.1Q のデフォルトプライオリティマッピング

入力フレームの CoS 値	ユーザプライオリティ
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

(2) QoS の trust モードでの構成方法
QoS の trust モードは入力トラフィックのユーザプライオリティマッピングを制御します。CoS モードは入力フレームの CoS 値に基づいてユーザプライオリティを設定します。もし、入力パケットが優先度付き tag フレームでなければ、デフォルトの CoS 値に戻ります。

NOTE
CEE マップがインタフェースに適用された場合、’qos trust’コマンドは使用できません。CEE マップは CoS trust モードのインタフェースに対して適用できます。

QoS trust モードを構成するために、特権実行モードから次の手順を実行してください。

１．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

２．イーサネットインタフェースを指定します。

```
switch(config)# interface tengigabitethernet 2/1/2
```

３．インタフェースモードを cos 'trust'に設定します。

```
switch(conf-if-te-2/1/2)# qos trust cos
```

NOTE
インタフェースから QoS trust モードを無効にするには、'no qos trust cos'を入力します。

4．特権実行モードに戻ります。

```
switch(conf-if-te-2/1/2)# exit
```

5．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

(3) CoS trust の確認

適用された CoS trust を確認するには、グローバルコンフィギュレーションモードから次のコマンドを入力します。tengigabitethernet 0/2 は、インターフェース名です。

```
switch(config)# do show qos interface tengigabitethernet 0/2
```

(4) ユーザプライオリティマッピングの構成方法

ユーザプライオリティマッピングを構成するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

2．イーサネットインタフェースを指定します。

```
switch(config)# interface tengigabitethernet 1/2/2
```

3．インターフェースを優先度 3 に設定します。

```
switch(conf-if-te-1/2/2)# qos cos 3
```

4．特権実行モードに戻ります。

```
switch(conf-if-te-1/2/2)# end
```

5．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

(5) CoS-to-CoS 変換 QoS マップの作成

CoS-to-CoS 変換マップを作成するために特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

2．変換マップの名を指定してマップを作成します。下記の例では、'test'を使用しています。

```
switch(config)# qos map cos-mutation test 0 1 2 3 4 5 6 7
```

3．running-config file を startup-config file に格納するため、`do copy’コマンドを実行します。

```
switch(config)# do copy running-config startup-config
```

(6) CoS-to-CoS 変換 QoS マップの適用

CoS-to-CoS 変換 QoS マップを適用するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

2．イーサネットインタフェースを指定します。

```
switch(config)# interface tengigabitethernet 2/1/2
```

3．CoS-to-CoS 変換マップを有効化または変更を適用する。下記の例では'test'を使用しています。

```
switch(conf-if-te-2/1/2)# qos cos-mutation test
```

NOTE

インターフェースからの変換マップを無効にするには、'no qos cos-mutation name'を入力します。

4．入力トラフィックに対して trust モードを指定します。

入力トラフィックのユーザプライオリティマッピングを適用する入力の QoS trust モードを指定するこのコマンドを使います。trust モードでない場合、全ての入力パケットのプライオリティは、インタフェースのデフォルト CoS 値で上書きされます。CoS モードは入力データの CoS 値に基づいてユーザプライオリティをセットします。もし、入力パケット優先 tag ではない場合、インタフェースのデフォルト CoS 値に戻されます。

```
switch(conf-if-te-2/1/2)# qos trust cos
```

5．特権実行モードに戻ります。

```
switch(conf-if-te-2/1/2)# end
```

6．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

(7) CoS-to-CoS 変換 QoS マップの確認

適用された QoS のマップを確認するには、グローバルコンフィギュレーションモードから、次のオプションのいずれかまたは両方を使用することができます。

1．'do show qos maps qos-mutation'コマンドおよびマップ名を使用して、特定のマップのための QoS マッピングを確認します。

```
switch(config)# do show qos maps qos-mutation test
```

2．qos-mutation パラメータで'do show qos maps'コマンドを使用して、すべての QoS マッピングを確認します。

```
switch(config)# do show qos maps qos-mutation
```

(8) DSCP trust モードの設定

QoS trust モードの様に、Differentiated Services Code Point（DSCP）trust モードは着信トラフィックのユーザ優先度マッピングを制御します。ユーザ優先度は、着信した DSCP 値に基づいています。この機能が有効になっていない場合、パケットの DSCP 値は無視されます。

DSCP 信頼が有効になっている時、表 21-3 は、デフォルト DSCP 優先度マッピングのユーザプライオリティを示しています。

表 21-3　デフォルト DSCP 優先度マッピング

DSCP 値	ユーザプライオリティ
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

NOTE

264 ページの『21.9 VCS モードのレイヤ 3 機能の制限事項』のもとに、この機能の VCS モードでの使用の制限に注意してください。

DSCP trust モードを設定するには、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

2．イーサネットインタフェースを指定します。

```
switch(config)# interface tengigabitethernet 10/0/2
```

3．インターフェースモードを‘qos trust dscp’に設定します。

```
switch(conf-if-te-10/0/2)# qos trust dscp
```

NOTE

インタフェースの DSCP trust モードを無効にするには、'no qos trust dscp'を入力します。

4．特権実行モードに戻ります。

```
switch(conf-if-te-10/0/2)# end
```

5．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

(9) DSCP trust モードの確認

適用された DSCP trust を確認するには、グローバルコンフィギュレーションモードから次のコマンドを入力します。tengigabitethernet 10/0/2 は、インターフェース名です。

```
switch(config)# do show qos running-config interface tengigabitethernet 10/0/2
```

(10) DSCP-to-CoS 変換マップの作成

入力インタフェースで DSCP-to-COS 変換マップを設定することにより、発信 802.1P CoS プライオリティ値を再割り当てするために、入力パケットの着信 DSCP 値を使用することができます。次の手順を使用してください。

NOTE

264 ページの『21.9 VCS モードのレイヤ 3 機能の制限事項』を参照し、この機能の VCS モードでの使用の制限に注意してください。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

2．マップ名を指定して、dscp-to-cos マップを作成します。DSCP 値を CoS 値にマップすることができるように、以下のコマンドはマップ名として'test'を使用し、dscp-cos マップモードでシステムを置きます。

```
switch(configure)# qos map dscp-cos test
```

3．一旦、システムが設定されマップための dscp-cos マップモードになったら、次の例のようにマークパラメータを使用している送信CoSプライオリティ値に着信DSCP値をマッピングすることができます。

```
switch(dscp-cos-test)# mark 1,3,5,7 to 3
switch(dscp-cos-test)# mark 11,13,15,17 to 5
switch(dscp-cos-test)# mark 12,14,16,18 to 6
switch(dscp-cos-test)# mark 2,4,6,8 to 7
```

これは、以下をセットします：

・DSCP 値 1、3、5、7 は CoS プライオリティ 3 として出力に設定されています。
・DSCP 値 11、13、15、17 は CoS プライオリティ 5 として出力に設定されています。
・DSCP 値 12、14、16、18 は CoS プライオリティ 6 として出力に設定されています。
・DSCP 値 2、4、6、8 は CoS プライオリティ 7 として出力に設定されています。

4．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

(11)インターフェースへの DSCP-to-CoS マップの適用

インタフェースへの DSCP-to-CoS 変換マップを適用するには、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

2．イーサネットインタフェースを指定します。

```
switch(config)# interface tengigabitethernet 1/1/2
```

3．DSCP-to-CoS 変換マップに加えられた変更をアクティブにするか、適用されます。下記の例では'test'を使用しています。

```
switch(conf-if-te-1/1/2)# qos dscp-cos test
```

NOTE

インタフェースからマップを無効にするには、'no qos dscp-cos name'を入力します。

４．着信トラフィックの DSCP trust モードを指定します。
受信インタフェースを DSCP trust モードに指定するためこのコマンドを使用します。これにより、着信トラフィックのユーザ優先度マッピングを制御することができます。untrust モードは、DSCP に基づいてパケットを分類しません。DSCP trust モードでは、着信した DSCP 値に基づいてパケットを分類します。着信パケットがタグ付けされた優先度である場合は、頼れるものは、CoS 値に基づいてパケットを分類することです。

```
switch(conf-if-te-1/1/2)# qos trust dscp
```

５．特権実行モードに戻ります。

```
switch(conf-if-te-1/1/2)# end
```

６．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

(12) DSCP-to-CoS 変換マップの確認

DSCP-to-CoS マップを確認するには、グローバルコンフィグレーションモードから次のオプションのいずれかまたは両方を使用することができます。

１．'do show qos maps dscp-cos'コマンドおよびマップ名を使用して、特定のマップに DSCP マッピングを確認します。

```
switch(config)# do show qos maps dscp-cos test
```

２．dscp-cos パラメータのみで'do show qos maps'コマンドを使用して、すべての DSCP マッピングを確認します。

```
switch(config)# do show qos maps dscp-cos
```

３．'show qos interface'コマンドを使用してインターフェースを指定することにより、インターフェースの DSCP-to-CoS 変換マッピングを確認します。

```
switch(config)# show qos interface te 1/1/2
```

21.3.2 トラフィッククラスマッピング

内蔵 DCB スイッチは、アプリケーションデータの異なる優先度に対して、分離とサービス制御のために８つのユニキャストトラフィッククラスをサポートしています。トラフィッククラスは０から７に割り当てられます。大きい番号ほど高い優先度となります。

トラフィッククラスマッピングの段階では、キュー選択を行います。

- マッピングとは、例えば１バイト(256 値)のユーザプライオリティを 8 つにマッピングするように、多対１に変換することといえます。
- ユーザプライオリティとトラフィッククラスには、一様な関連はありません。

(1) ユニキャストトラフィック

表 21-4 は、IEEE802.1Q のデフォルトマッピングに準拠するための CoS ベースユーザプライオリティマッピングをサポートした、レイヤ２のデフォルトトラフィッククラスマッピングを示しています。

表 21-4　ユニキャストトラフィッククラスマッピングのデフォルトユーザプライオリティ

ユーザプライオリティ	トラフィッククラス
0	1
1	0
2	2
3	3
4	4
5	5
6	6
7	7

各ポートに対するこれらデフォルトトラフィッククラスマッピングは、変更が可能です。一旦トラフィッククラスマッピングが実行されると、入出力ポートの全てのキューイングに対して絶えず駅用されます。

(2) マルチキャストトラフィック

内蔵 DCB スイッチは、アプリケーションデータの異なる優先度に対する分離とサービス制御のために８つのマルチキャストトラフィッククラスをサポートしています。トラフィッククラスは０から７に割り当てられます。大きい番号ほど高い優先度となります。トラフィッククラスマッピングの段階では、キュー選択を行います。

表 21-5 は、IEEE802.1Q のデフォルトマッピングに準拠するための CoS ベースユーザプライオリティマッピングをサポートした、レイヤ２のデフォルトトラフィッククラスマッピングを示しています。

表 21-5　マルチキャストトラフィッククラスマッピングのデフォルトユーザプライオリティ

ユーザプライオリティ	トラフィッククラス
0	1
1	0
2	2
3	3
4	4
5	5
6	6
7	7

一旦トラフィッククラスマッピングが実行されると、入出力ポートの全てのキューイングに対して絶えず適用されます。'CoS-to-traffic class-map'または'DSCP-to-traffic class-map'のいずれかでインタフェースを設定できます。

(3) CoS-to-Traffic-Class マッピング

CoS-to-Traffic-Class をマッピングするため、特権実行モードから次の手順を実行してください。

NOTE

CoS-to-Traffic-class-map の作成は、スタンドアロンモードだけで利用できます。

1．グローバルコンフィグレーションモードに入ります。

```
switch# configure terminal
```

2．名称とマッピングを指定することにより、CoS-Traffic-Class マッピングを作成します。

```
switch(config)# qos map cos-traffic-class test 1 0 2 3 4 5 6 7
```

3．特権実行モードに戻ります。

```
switch(config)# end
```

4．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

(4) インタフェースへの CoS-to-Traffic-Class マッピングの適用

CoS-to-Traffic-Class マッピングを有効化するため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに入ります。

```
switch# configure terminal
```

2．インタフェースを指定します。

```
switch(config)# interface tengigabitethernet 12/2/2
```

3．名称を指定して CoS-to-Traffic-Class マッピングを有効化します。下記の例では'test'を使用しています。

```
switch(conf-if-te-12/2/2)# qos cos-traffic-class test
```

NOTE

インタフェースからの変換マップを無効にするには、'no qos cos-traffic-class'を入力します。

4．特権実行モードに戻ります。

```
switch(conf-if-te-12/2/2)# end
```

5．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

(5) CoS-to-Traffic-Class マッピングの確認

CoS-to-Traffic-Class のマッピングを確認するには、グローバルコンフィギュレーションモードから、次のオプションのいずれかまたは両方を使用することができます。

- 'do show qos maps cos-traffic-class'コマンドを使用し、マップ名を指定して、CoS-Traffic-Class マッピングを確認します。

```
switch(config)# do show qos map cos-traffic-class test
```

- cos-traffic-class だけの'do show qos maps'コマンドを使用して、すべての COS-to-Traffic-Class マッピングを確認します。

```
switch(config)# do show qos maps cos-traffic-class
```

- 'show qos interface'コマンドを使用しインタフェースを指定して、インタフェースのための CoS-Traffic-Class のマッピングを確認します。

```
switch(config)# do show qos interface te 12/2/2
```

(6) DSCP-to-Traffic-Class マッピング

入力 DSCP 値は、DSCP-to-Traffic-Class マップを使用して、入力インターフェースのトラフィックを特定のトラフィッククラスに分類するために使用することができます。DSCP-to-Traffic-Class をマッピングするには、特権実行モードで次の手順を実行します。

NOTE

264 ページの『21.9 VCS モードのレイヤ 3 機能の制限事項』を参照し、この機能の VCS モードでの使用の制限に注意してください。

1．グローバルコンフィグレーションモードに入ります。

```
switch# configure terminal
```

2．以下のコマンドは、作成したマップのマッピングを設定することができるように、マップ名として'test'を使用し、dscp-traffic-class モードに移行します。

```
switch(config)# qos map dscp-traffic-class test
```

3．一旦、システムが設定されマップのための dscp-traffic-class モード（このケースでは、dscp-traffic-class-test）になったら、次の例のようにマークパラメータを使用して、トラフィッククラスに DSCP 値をマッピングすることができます。

```
switch(dscp-traffic-class-test) mark 1,3,5,7 to 3
switch(dscp-traffic-class-test) mark 11,13,15,17 to 5
switch(dscp-traffic-class-test) mark 12,14,16,18 to 6
switch(dscp-traffic-class-test) mark 2,4,6,8 to 7
```

これは、以下をセットします：

・DSCP 値 1、3、5、7 はトラフィッククラス 3 にマッピングされます。
・DSCP 値 11、13、15、17 はトラフィッククラス 5 にマッピングされます。
・DSCP 値 12、14、16、18 はトラフィッククラス 6 にマッピングされます。
・DSCP 値 2、4、6、8 はトラフィッククラス 7 にマッピングされます。

4．特権実行モードに戻ります。

```
switch(dscp-traffic-class-test) end
```

5．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

(7) インタフェースへの DSCP-to-Traffic-Class マッピングの適用

DSCP-to-Traffic-Class マッピングを有効にするには、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに入ります。

```
switch# configure terminal
```

2．インタフェースを指定します。

```
switch(config)# interface tengigabitethernet 1/1/2
```

3．DSCP-to-Traffic-Class マッピングを有効にします。この場合、'test'がマップ名です。

```
switch(conf-if-te-1/1/2)# qos dscp-traffic-class test
```

NOTE

インタフェースから DSCP-to-Traffic クラスマップを無効にするには、'no qos dscp-traffic-class name' を入力します。

4．特権実行モードに戻ります。

```
switch(conf-if-te-1/1/2)# end
```

5．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

(8) DSCP-to-Traffic-Class マッピングの確認

DSCP-to-Traffic-Class マッピングを確認するには、グローバルコンフィギュレーションモードから、次のオプションのいずれかまたは両方を使用することができます。

- 'do show qos maps dscp-traffic-class'コマンドを使用し、マップ名を指定して、DSCP-Traffic-Class マッピングを確認します。

```
switch(config)# do show qos maps dscp-traffic-class test
```

- dscp-traffic-class パラメータだけの'do show qos maps'コマンドを使用して、すべての DSCP-Traffic-Class マッピングを確認します。

```
switch(config)# do show qos maps dscp-traffic-class
```

- 'show qos interface'コマンドを使用し、インタフェースを指定して、インタフェースのための DSCP-to-Traffic-Class マッピングを確認します。

```
switch(config)# show qos interface te 1/1/2
```

21.4 輻輳制御

キューが、例えばリンクのオーバーサブスクリプションやダウンストリームデバイスからのバックプレッシャーなどのいくつかの理由により、一杯になり始めることがあります。継続する長時間のキューへの滞留は、一般にネットワークで輻輳の兆しであり、キューイングによる遅延とフレーム損失によりアプリケーション性能に影響を及ぼします。

輻輳制御は、輻輳が発生した場合どのようにシステムが対応するかを定義し、ネットワークが輻輳状態に入るのを防ぐために行う対策を有効にすることまでを含みます。

21.4.1 Tail drop

Tail drop キューイングは輻輳制御の最も基本的な形態です。フレームは FIFO でキューイングされ、バッファメモリが枯渇するまでキューイングされます。これは、特別な QoS 設定がない場合のデフォルトの動作です。

基本的な Tail drop アルゴリズムは、キューと関連付けられる複数の優先度やトラフィック毎の廃棄閾値という考えはありません。キューの深さが閾値を越えた場合、優先度を持ったフレームを受信しても廃棄されます。

図 21-1 は、低優先度のトラフィックが全くバッファメモリを使わないことを保証するために、本機能をどのように使うかを示しています。閾値は、また、各トラフィッククラスに対する最大のキュー遅延を制限するためにも使うことが出来きます。加えて、もしポートに対する閾値の合計がバッファメモリの 100%以下に設定した場合は、単一ポートが共有メモリプール全体を占有しないことを保証することができます。

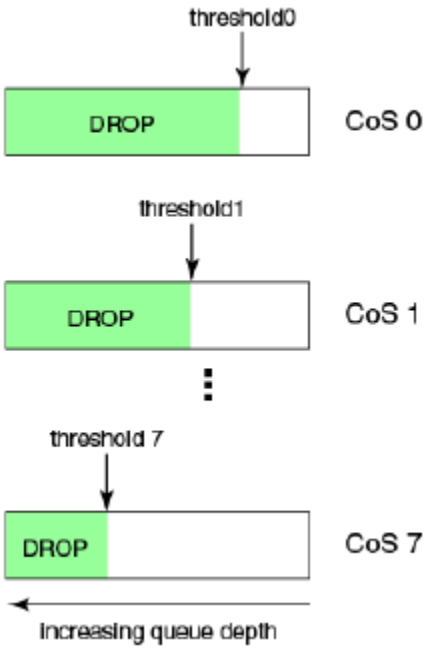

図 21-1 キューの深さ

Tail drop アルゴリズムは優先度別の破棄閾値をサポートするように拡張できます。入力ポートの CoS キューの深さが閾値に達すると、関連付けられたプライオリティ値で到着するどんなフレームも破棄されます。図 21-1 は、優先度の低いトラフィックが全体的にバッファメモリを全て消費しないことを保証するために、この機能を活用する方法について説明します。閾値は、また、各トラフィッククラスの最大キューイング遅延を関連することになります。加えて、ポートの閾値の合計がバッファメモリの 100%以下に設定されている場合、単一の CoS 値がポートに割り当てられた共有メモリプール全体を独占しないようにすることができます。

(1) TailDrop 閾値の変更

Tail drop の閾値を変更するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに入ります。

```
switch# configure terminal
```

2．各マルチキャストトラフィッククラスに対する Tail drop 閾値を変更します。例では、1000pkt が使われています。

```
switch(config)# qos rcv-queue multicast threshold 1000 1000 1000 1000 1000 1000 1000
1000 1000
```

3．特権実行モードに戻ります。

```
switch(config)# end
```

4．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

21.4.2 CoS 閾値の設定

すべてのポートには、１つのポート Tail drop 閾値とプライオリティ毎の他の 8 つの閾値値の合計 9 つの CoS 閾値が関連付けられています。すべてのプライオリティからのトラフィックに対する公正なバッファ配分を与えるために、ポートバッファは異なるプライオリティ間で割り当てられます。これは、プライオリティ毎の Tail drop 閾値により実現されます。ポート Tail drop 閾値は、ポートに指定されたバッファの量を表し、プライオリティ毎の Tail drop 閾値(ここからは CoS Tail drop 閾値と呼びます)は、各 CoS に割り当てられるバッファを表します。

プライオリティに割り当てられているバッファが完全に消耗している時は、常にそのプライオリティに着信するすべてのトラフィックが廃棄されます。プライオリティ毎の tail drop 閾値が存在しない場合には、バッファは先入れ先出しの基本に基づき消費され、結果として全てのプライオリティ間で不公平に共有されることとなります。もし、どのプライオリティのトラフィックが多く見られるかが分かったら、それらのプライオリティに十分な数のバッファを与えることが、パケット破棄の数を低減する結果となります。

このように、標準プライオリティ値を使う代わりに、全 8 つのプライオリティの合計値で 100%を超えないように 0%から 100%まで任意の閾値をどこにでも割り当てることができます。

例えば、次の例に示すように、priorities 5 5 5 5 50 20 2 8 とすると合計 100%となります。

```
switch(conf-if-te-0/1)# qos rcv-queue cos-threshold 5 5 5 5 50 20 2 8
switch(conf-if-te-0/1)# do show qos in te 0/1
Interface TenGigabitEthernet 0/1
CoS-to-Traffic Class map 'default'
       In-CoS:  0  1  2  3  4  5  6  7
 ------------------------------------------------------
 Out-CoS/TrafficClass: 0/1 1/0 2/2 3/3 4/4 5/5 6/6 7/7
Per-Traffic Class Tail Drop Threshold (bytes)
    TC:   0   1   2   3   4   5   6   7
-------------------------------------------------------------------
Threshold: 10180 10180 10180 10180 101808 40723  4072 16289
```

Tail drop 閾値は、100%を超えることは出来ませんが、下回ることは可能です。例えば、入力した Tail drop

閾値が 100%未満の場合は、バッファ割り当ては、設定された内容に従い割り当てられます。

21.4.3 イーサネット Pause(Ethernet pause)

イーサネット Pause は、隣接デバイスへの送信規制のための IEEE802.3 で規定される仕組みです。Pause メッセージはオプションの MAC 層を使うことによって送信されます。Pause フレームは、512bit 時間単位の Pause 期間を示す２バイトの値を持っています。デバイスが Pause フレームを受信すると、送信中のフレーム転送が完了した後、指定された時間インタフェースからのデータ送信を停止しなければなりません。標準的な仕組みによりフレームロスを低減するために、この機能は使えます。しかしながら、Pause メカニズムは、数ホップはなれた送信元を選んで送信規制することや、VLAN や優先度毎に使用することはできません。そのため全てのトラフィックを抑止します。

イーサネット Pause は下記の特徴を持ちます。

- 全ての構成パラメータはインタフェース毎に個別に指定することが出来る
- Pause On/Off は、TX と RX 別々に指定することが出来る。auto-negotiation を無効にすることにより抑止することができます。
- Pause は入力(受信)キューに依存して生成される。キューレベルは、入力ポート単位に決定されます。各入力ポートの上限及び下限閾値を指定できます。もし、更にフレームを受信してキュー長がまだ下限閾値以上ならば、更に Pause フレームが生成されます。一旦、キュー長が下限閾値以下となれば、Pause の生成は終了します。
- Pause を受信して実行されると、Pause フレームで指定された期間、ポートに関連付けられた出力キューの伝送は保留されます。

(1) 1Gbps ポーズネゴシエーション

1Gbps ローカルポートがすでにオンラインで、'qos flowcontrol'コマンドが発行されると、Pause 設定は、すぐにローカルポートで有効になります。しかし、リンクが切り換えられると、Pause は再ネゴシエートされます。ローカルポートは、最新の QoS フロー制御設定をアドバタイズします。オートネゴシエーションが完了すると、ローカルポートの Pause 設定は、表 21-6 に示されているように、802.3 Clause 28B に従って、Pause ネゴシエーションの結果に応じて変更されることがあります。

表 21-6　Pause ネゴシエーション結果

広告された LOCAL cfg	広告された REMOTE cfg	ネゴシエーション結果
Rx=off Tx=on	Rx=on Tx=on	asymmetrical: LOCAL Tx=on --> pause --> REMOTE Rx=on
Rx=on Tx=on	Rx=off Tx=on	asymmetrical: LOCAL Rx=on <-- pause <-- REMOTE Tx=on
Rx=on Tx=n/a	Rx=on Tx=n/a	symmetrical : LOCAL Tx/Rx=on <-- pause --> REMOTE Tx/Rx=on
Rx=n/a Tx=n/a	Rx=off Tx=off	disable pause both sides

(2) イーサネット Pause の有効化

ここでは、フロー制御を設定し、加えてイーサネットポーズフレームを有効にします。接続しているデバイスでフロー制御パラメータを設定し、オプションを"auto"にしたままとすることをお勧めします。

NOTE

イーサネット Pause オプションは、スタンドアロン･モードでのみ使用できます。

イーサネット Pause を有効化するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに入ります。

```
switch# configure terminal
```

2．イーサネットインタフェースを指定します。

```
switch(config)# interface tengigabitethernet 3/0/2
```

3．インターフェースの TX と RX の両方のイーサネット Pause を有効化します。

```
switch(conf-if-te-3/0/2)# qos flowcontrol tx on rx on
```

NOTE

インタフェースのイーサネット Pause を無効にするには、'no qos flowcontrol'を入力します。

4．特権実行モードに戻ります。

```
switch(conf-if-te-3/0/2)# end
```

5．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

21.4.4 イーサネットプライオリティフロー制御

イーサネットプライオリティフロー制御（PFC）は、イーサネットポーズの基本的な拡張機能です。ポーズ MAC 制御メッセージは、8 つの 2 バイトのポーズ値とその値が有効であるかを示すためにビットマスクで拡張されます。各ポーズ値はベースポーズプロトコルと同様に解釈されていますが、それぞれが対応するイーサネット優先/クラスレベルに適用されます。

たとえば、ポーズ値 0 は、プライオリティ 0 に適用され、ポーズ値 1 は、プライオリティ 1 に適用されます。これは、リンク上のすべてのトラフィックが中断され、イーサネットのポーズメカニズムの一つの欠点に対処しています。しかし、その他のイーサネットポーズの制限は残ったままです。

イーサネットプライオリティフロー制御は、次の機能が含まれています。

- 各入力ポートに 8 つの上限と下限の閾値が存在する以外は上記のイーサネットポーズで述べたように全てが正確に動作します。つまりキューレベルは、優先付けされた入力ポート毎に動作することを意味しています。
- ポーズオン/オフがプライオリティ毎に TX と RX に独立して指定することができます。
- イーサネット MAC に指定されるポーズ時間は全てのプライオリティをカバーする単一の値です。
- イーサネット Pause またはイーサネットプライオリティフロー制御は互換性がないため、リンクの両端での設定は同じでなければなりません。

(1) イーサネット PFC の有効化

イーサネット PFC を有効にするには、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに入ります。

```
switch# configure terminal
```

2．イーサネットインタフェースを指定します。

```
switch(config)# interface tengigabitethernet 1/1/2
```

3．インタフェースのイーサネット PFC を有効にします。

```
switch(conf-if-te-1/1/2)# qos flowcontrol pfc 3 tx on rx on
```

NOTE

インタフェースのイーサネット PFC を無効にするには、' no qos flowcontrol pfc cos value'を入力します。

4．特権実行モードに戻ります。

```
switch(conf-if-te-1/1/2)# end
```

5．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

21.5　マルチキャストレート制限

マルチキャストレート制限はマルチキャストフレームの複製制御とトラフィックの影響を抑制するメカニズムを提供します。マルチキャストレート制限は各マルチキャスト受信キューの出力に適用します。レート制限は、受信キューが共通なので、入力時の受信キュー(第一段階拡張)と出力時の受信キュー(第二段階拡張)に均等に適用されます。それぞれのトラフィッククラスに最大マルチキャストフレームレートを各々制限し、システムのトータルマルチキャスト出力レートを抑制するためにポリシーを設定できます。

マルチキャストレート制限の特徴は下記の通りです。

- 全ての構成パラメータは全体に適用されます。マルチキャストレート制限は、マルチキャスト拡張キューに複製されたフレームが存在するため、マルチキャスト受信キューに適用されます。同一の物理キューは受信キューの入力と出力両方に使われます。これにより、レート制限はキューイング時の入力と出力の両方に適用されます。
- ４種類のマルチキャストレート制限値をサポートしており、各トラフィッククラスに対応します。レート制限値は PPS(packets per second)で最大マルチキャスト拡張レートを示します。

21.5.1　受信キューのマルチキャストレートリミットの生成

受信キューのマルチキャストレートリミットを生成するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに入ります。

```
switch#configure terminal
```

2．最大マルチキャストフレーム拡張レートの下限を設定します。本例では、レートは 10000PPS までです。

```
switch(config)#qos rcv-queue multicast rate-limit 10000
```

3．特権実行モードに戻ります。

```
switch(config)#end
```

4．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

21.6　スケジューリング

スケジューリングは、フレームを転送するために滞留している複数のキューを調停します。内蔵 DCB スイッチでは、絶対優先(Strict Priority:SP)スケジューリングと欠損荷重ラウンドロビン(Deficit Weighted Round Robin:DWRR)スケジューリングの２つのアルゴリズムをサポートしています。
また、SP-to-DWRR を使うことで、トラフィッククラスの数を自由に選択することが出来ます。同一トラフィッククラスに複数のキューが存在すると、スケジューリングはこれら等しい優先キューを考慮に入れます。

21.6.1　絶対優先(Strict priority:SP)スケジューリング

SP(Strict priority)は、遅延を重視するトラフィックに対する対応を容易にするために使用されます。
SP スケジューラーは低優先度のトラフィッククラスを転送する前に、最高優先キューに滞留する全てのフレームを転送します。このタイプのサービスの問題は、キューが低優先度のトラフィックで使い尽くされるポテンシャルがあることです。

図 21-2 は、２つの SP キューでサービスする SP スケジューラーでのフレームスケジュール順序を示している。高い番号を持つキューの SP2 が高い優先度を持っている。

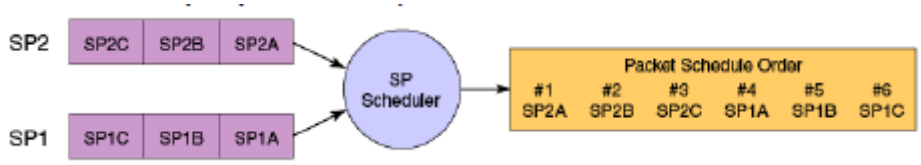

図 21-2 ２つのキューでの SP スケジューリング

21.6.2　欠損荷重ラウンドロビン(Deficit weighted round robin:WRR)スケジューリング

WRR スケジューリングは、ネットワーク帯域の共有を制御することを容易にするために使用されます。

WRR はそれぞれのキューに重み付けを行います。その値は、キューに割り付けられた帯域の合計を決定します。スケジュールのラウンドロビンの挙動は、次のキューにデータが移動する前に総数を制限して送信したり、最低優先度がサービスされた後に最高優先度のキューに戻るように、各キューに対してサービスします。
図 21-3 は、２つの WRR キューを提供している WRR スケジューラに対して、フレームをスケジュールする順序を示しています。高い番号のキューは高い優先度(WRR2)と扱われ、重み付けは２つのキューでネットワーク帯域が２：１に配分されることを示しています。図 21-3 の WRR2 は帯域の６６％を受信し、WRR1 は３３％受信します。
WRR スケジューリングは、使用される余分な帯域を追跡して、キューを通る次のサイクルに割り当てられる帯域幅より余分な帯域を差し引きます。このように、帯域の利用率が長い期間にわたってキューの重み付けが統計的に一致するようになります。

図 21-3 ２つのキューでの WRR スケジューリング

DWRR スケジューリングは WRR スケジューリングの改善版です。DWRR スケジューリングは、キューが帯域割当を越える場合は使用された余剰分を記憶しておき、後続のスケジューリングでキューの帯域割当を削減します。このように、実際の帯域利用が WRR スケジューリングに比べて定義されたレベルにより近くなります。

21.6.3 トラフィッククラスのスケジューリングポリシー

トラフィッククラスは 0 から 7 の番号をもっており、大きい番号をもつトラフィッククラスは高い優先度として扱われます。内蔵 DCB スイッチでは、SP-to-WR キューの数を自由に決めることが出来ます。SP スケジューリングキューの数は N(SP1 から 8)の範囲で指定できます。その際、高い優先度のトラフィッククラスは SP サービスとして構成され、残りの 8 つは WRR サービスとなります。表 21-7 はサポートしているスケジューリング構成の組合せを示しています。SP4 を使うために QoS キューを構成する場合は、トラフィッククラス 7 は SP4 を、トラフィッククラス 6 は SP3 を、その他はリストに示す通りに使われます。異なるトラフィッククラスが同一キューを通過する場合は、SP スケジューリングマッピングを使います。

表 21-7　サポートしているスケジューリング構成

トラフィッククラス	SP0	SP1	SP2	SP3	SP4	SP5	SP6	SP8
7	WRR8	SP1	SP2	SP3	SP4	SP5	SP6	SP8
6	WRR7	WRR7	SP1	SP2	SP3	SP4	SP5	SP7
5	WRR6	WRR6	WRR6	SP1	SP2	SP3	SP4	SP6
4	WRR5	WRR5	WRR5	WRR5	SP1	SP2	SP3	SP5
3	WRR4	WRR4	WRR4	WRR4	WRR4	SP1	SP2	SP4
2	WRR3	WRR3	WRR3	WRR3	WRR3	WRR3	SP1	SP3
1	WRR2	WRR2	WRR2	WRR2	WRR2	WRR2	WRR2	SP2
0	WRR1	WRR1	WRR1	WRR1	WRR1	WRR1	WRR1	SP1

図 21-4 はフレームスケジューラを SP+WRR の組合せシステムに拡張したものが適切にストレートフォワードとなることを示しています。全ての SP キューは WRR より厳密により高い優先度として扱われ、それらは最初にサービスされます。一旦、全ての SP キューから転送されると、通常の WRR スケジューリングの動作が空ではない WRR キューに適用されます。

図 21-4 SP スケジューラと WRR スケジューラ

21.6.4　QoS キューのスケジューリング

利用するスケジューリングを指定するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに入ります。

```
switch# configure terminal
```

2. 利用するスケジューリングアルゴリズムと帯域マッピングに対するトラフィッククラスを指定します。

```
switch(config)# qos queue multicast scheduler dwrr 10 20 20 10 10 10 10 10
```

3．特権実行モードに戻ります。

```
switch(config)# end
```

4．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

21.6.5　マルチキャストキュースケジューリング

マルチキャストトラフィッククラスは 0 から 7 までの番号を持ち、大きい番号のトラフィッククラスは高い優先度として扱われます。マルチキャストトラフィッククラスから同等のユニキャストトラフ

ィッククラスへの固定マッピングは、キュースケジューリングの振る舞いを選択するために適用されます。表 21-8 は、等価性マッピングが適用されたマルチキャストトラフィッククラスを示します。一旦、マルチキャストトラフィッククラスと同等のマッピングが適用されると、スケジューリングとスケジューラの構成は同等のユニキャストトラフィッククラスから継承されます。正確なマッピングの等価性の詳細については、表 21-8 を参照下さい。

表 21-8　マルチキャストトラフィッククラス同等のマッピング

マルチキャストトラフィック クラス	等価ユニキャストトラフィック クラス
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

ユニキャストのキューへの入力と出力は、SP+WRR サービスと同等のサービスレベルで複数の物理キューとを同時にサポートする複合スケジューラを利用します。マルチキャストは、マルチキャスト拡張が追加キューに追加されます。マルチキャストトラフィッククラスはユニキャストのサービスレベルに相当しますので、それらはそれらと同等のユニキャストサービスポリシーとまったく同じように扱われています。

(1) QoS マルチキャストキューのスケジューリング

QoS マルチキャストキューをスケジューリングするために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに入ります。

```
switch#configure terminal
```

2．利用するスケジュールポリシーと帯域マッピングに対するトラフィッククラスを指定します。

```
switch(config)# qos queue multicast scheduler dwrr 10 20 20 10 10 10 10 10
```

3．特権実行モードに戻ります。

```
switch(config)# end
```

4．running-config file を startup-config file に格納するため、`copy’コマンドを実行します。

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

21.7　データセンタブリッジマップの構成

DCB の QoS はフレームの分類、優先度とトラフィッククラス(queue)マッピング、輻輳制御、スケジューリングをカバーしています。DCB プロビジョニングモデルのもと、これらの機能の全てが、Priority

Group Table と Priority Table という２つの構成テーブルを使うことで構成されます。
DCB Priority Group Table は、各プライオリティグループ ID(PGID)と、スケジュールポリシー(Strict Priority versus DWRR, DWRR weight, relative priority)を定義し、一部輻輳制御(PFC)構成を定義します。
DCB Priority Group Table は 16 のエントリがあります。表 21-9 は、デフォルトの DCB Priority Group Table 設定を示しています。

NOTE
PFC が有効になっている優先キューにマッピングできる CoS は一つだけです。CoS 番号は、優先キュー番号と同じにしておくべきです。もし、この制約を破った場合、エラーメッセージが表示され、Priority Group Table がデフォルト値に戻ります。
CEE マップが適用されているインタフェースが CNA と接続されると、絶対優先 PGID(PGID 15.0 ～ PGID 15.7)だけが許容されます。

表 21-9　デフォルト DCB Priority Group Table 設定

PGID	帯域%	PFC
15.0	—	N
15.1	—	N
15.2	—	N
15.3	—	N
15.4	—	N
15.5	—	N
15.6	—	N
15.7	—	N
0	0	N
1	0	N
2	0	N
3	0	N
4	0	N
5	0	N
6	0	N
7	0	N

DWRR に対して、絶対優先は PGID 値から直接適用されます。プレフィックス 15 を持った全ての PGID は、絶対優先スケジューリングポリシーが適用され、０から７の範囲の全ての PGID は DWRR スケジューリングポリシーが適用されます。Priority Group 間の相対的な優先度は、PGID 15.0 が最も高く、PGID 7 が最も低くなっている通り、テーブルにリストされたエントリ順となります。輻輳制御の設定は、PFC 欄をオン/オフ切替えることにより部分的に指定されます。これは、輻輳制御が部分的に提供されることを示しており、Priority Group にマッピングされる優先度の組が知られていないからで、DCB Priority Table に引き継がれます。
DCB Priority Table は、Priority Group への各 CoS マッピングを定義します。そして、PFC 設定を完成させます。DCB Priority Table は８つの列があります。表 21-10 は、デフォルト DCB Priority Table の設定を示します。

表 21-10　デフォルト DCB Priority Table 設定

CoS	PGID
0	15.6
1	15.7
2	15.5
3	15.4
4	15.3
5	15.2
6	15.1
7	15.0

21.7.1　CEE マップの生成

CEE マップを生成するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

2．CEE マップを生成します。マップ名称は"default"だけが使えます。

```
switch(config)# cee-map default
```

3．特権実行モードに戻ります。

```
switch(config)# end
```

4．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

21.7.2　Priority Group Table の定義

Priority Group Table マップを定義するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

2．DCB マップを生成します。マップ名称は"default"だけが使えます。

```
switch(config)# cee-map default
```

3．PGID 0 の DCB マップを定義します。

```
switch(config-cee-map-default)# priority-group-table 0 weight 50 pfc on
```

4．PGID 1 の DCB マップを定義します。

```
switch(config-cee-map-default)# priority-group-table 1 weight 50 pfc off
```

5．特権実行モードに戻ります。

```
switch(config-cee-map-default)# end
```

6．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

21.7.3　Priority-Table マップの定義

Priority-Table マップを定義するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

2．'cee-map'コマンドを使用して定義するために、DCB マップの名前を指定します。この例では、'default'で使用されています。

```
switch(config)# cee-map default
```

3．マップを定義します。

```
switch(config-cee-map)# priority-table 1 1 1 0 1 1 1 15.0
```

NOTE

priority-table の定義の詳細については、『Network OS Command Reference　3.0』の‘cee-map (configuration)’コマンドを参照してください。

4．特権実行モードに戻ります。

```
switch(config-cee-map)# end
```

5．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

21.7.4　インタフェースへの DCB プロビジョニングマップの適用

DCB プロビジョニングマップを適用するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

2．イーサネットインタフェースを指定します。この例では、101/0/2 を使っています。

```
switch(config)# interface tengigabitethernet 101/0/2
```

3．インタフェースに DCB マップを適用します。

```
switch(conf-if-te-101/0/2)# cee default
```

NOTE

インタフェースのマップを無効にするには、'no cee'を入力します。

4．特権実行モードに戻ります。

```
switch(conf-if-te-101/0/2)# end
```

5．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

21.7.5　DCB マップの確認

CoS DCB マップを確認するには、グローバルコンフィギュレーションモードから'show cee maps default'コマンドを使用します。

```
switch# show cee maps default
```

21.8　Brocade VCS ファブリック QoS

Brocade VCS ファブリック QoS は、わずかですがユーザ設定が必要です。変更する唯一のオプションは、ファブリックプライオリティとロスレスプライオリティだけです。
Brocade VCS ファブリックは、'7'のマッピングプライオリティとファブリックプライオリティを予約しています。上流から Brocade VCS クラスタに入る予約されたプライオリティを使ったトラフィックは、自動的に低いプライオリティに置換されます。
マッピングまたはファブリックプライオリティの変更は、必要ありません。デフォルトでは、再割当のプライオリティ値は'0'に設定されています。
Brocade VCS モードでは、

- 受信する全ての優先度 7 の tag 付パケットは、エッジポートで破棄されます。
- tag 無し制御フレームはキュー7(TC7)で受付けられます。

Brocade VCS クラスタでの全てのスイッチは、一致した再割当のプライオリティ値と同じ priority-group-table 値でなければなりません。

21.8.1　VCS ファブリック QoS の設定

Brocade VCS ファブリックで再設定されるプライオリティを設定するため、グローバルコンフィグレーションモードから次の手順を実行してください。

1．CEE マップコンフィグレーションモードに移行するため、'cee-map'コマンドを入力します。

```
switch(config)# cee-map default
```

2．Brocade VCS ファブリック QoS のロスレスプライオリティを設定するため、'remap lossless priority'コマンドを使用します。デフォルトロスレスプライオリティは 0 です。

```
switch(config-cee-map-default)# remap lossless-priority priority 2
```

3．Brocade VCS ファブリック QoS のファブリックプライオリティを設定するため、'remap fabric priority'コマンドを使用します。デフォルトファブリックプライオリティは 0 です。

```
switch(fabric-cee-map-default)# remap fabric-priority priority 2
```

4．グローバルコンフィグレーションモードに戻るため'exit'コマンドを使います。

```
switch(config-cee-map)# exit
```

5．受信データインタフェースを指定します。

```
switch(config)# interface tengigabitethernet 22/0/1
```

6．インタフェースに CEE プロビジョニングマップを適用します。

```
switch(conf-if-te-22/0/1)# cee default
```

21.9　VCS モードのレイヤ 3 機能の制限事項

スイッチが VCS モードの時には、ロスレスプライオリティとファブリックプライオリティは、あらゆるレイヤ 3 QoS マーキングおよびクラスから分離される必要があります。したがって、スイッチが VCS モードで動作している時、特定の制限が一部のレイヤ 3 DSCP QoS 機能に適用されます。
以下は、VCS モードで適用可能なレイヤ 3 DSCP-Traffic-Class、DSCP-CoS マップ、およびの DSCP trust

機能を使用するための制限です。DSCP 変換マップは、VCS モードに影響されません。

- CoS trust のためにあるように、DSCP trust は VCS モードでは無効になります。
- VCS モードには、デフォルト DSCP マップがありません。DSCP trust がスタンドアロンモードで有効になっている場合、デフォルトのマップが発生します。
- 非デフォルトの DSCP-Traffic-Class マップには、次の制限があります。
  - DSCP 値は、Traffic Class 7 に分類することができません。
  - DSCP 値は、デフォルト Traffic Class 3 によって、ロスレストラフィックを伝送キューに分類することができません。
- 非デフォルトの DSCP-CoS マップでは、次の制限があります。
  - DSCP 値は、CoS 7 にマークすることができません。
  - DSCP 値は、デフォルト CoS 3によってロスレスプライオリティをマークすることができません。
- ロスレスプライオリティは、CEE マップを介して識別されます。
- DSCP ベースマーキングまたは分類を有効にするには、デフォルト以外の SCP-Traffic-Class マップと DSCP-CoS マップがインターフェースに適用されなければなりません。
- インターフェースに DSCP-Traffic-Class または ADSCP-CoS マップを適用するには、CoS およびトラフィッククラス値がロスレスプライオリティとして再マーキングする必要があります。例えば、DSCP-Traffic-Class マップ"abcd"が作成される時、それはデフォルトの内容を持つことになります。インターフェースに適用される時、ファブリックとロスレスプライオリティがマップで使用されることをエラーが表示し、インターフェースで適用することはできません。
- 有効な DSCP-Traffic-Class マップと DSCP-CoS マップがインタフェースに適用される時、DSCP trust が設定されているマップで有効にされます。

22 802.1x ポート認証の設定

22.1 802.1x プロトコル概要

802.1x プロトコルは、クライアントベースの認証ソフトウェア(サプリカント)とサーバ上の認証データベースと認証装置間で通信するポートベースの認証アルゴリズムです。ここでの想定は、認証装置が内蔵 DCB スイッチの場合です。認証装置として、内蔵 DCB スイッチは認証されないネットワークアクセスを拒否します。
新しいサプリカントを検出すると、内蔵 DCB スイッチはポートを有効化し、"unauthorized"とマークします。この状態で、802.1x のトラフィックだけが許可されます。HDCP や HTTP といった全ての他の通信はブロックされます。内蔵 DCB スイッチは、EAP-request をサプリカントに送信します。サプリカントは、EAP-response パケットを応答します。内蔵 DCB スイッチは、RADISUS 認証サーバへ EAP-response パケットを転送します。もし、証明書が RADIUS サーバデータベースで認証されれば、サプリカントは保護されたネットワークリソースへアクセスできます。

NOTE
802.1x ポート認証は、LAG (Link Aggregation Group)や LAG に参加しているインタフェースはサポートしていません。

NOTE
'EAP-MD5', 'EAP-TLS', 'EAP-TTLS', 'PEAP-v0'プロトコルは、RADIUS サーバでサポートされ、認証スイッチへ転送されます。

サプリカントがログオフした時、ポートを"unauthorized"状態に戻す内蔵 DCB スイッチに'EPA-logoff' メッセージを送信します。

22.2 802.1x 設定のガイドラインと制限

802.1x を設定する場合は、次の 802.1x 構成ガイドラインと制約事項に従ってください。

- 装置全体で 802.1x を無効化すると、802.1x 認証が有効化されている全てのインタフェースポートは、自動的に'force-authorized port-control'に切り替わります。

22.3 802.1x 認証設定作業

このセクションでの作業は、802.1x を動作させるために必要な共通操作を記述しています。802.1x で利用可能なコマンドの解説は、『Network OS Command Reference』を参照下さい。

22.3.1 スイッチと CNA/NIC 間認証の設定

'radius-server'コマンドは、第一 RADIUS サーバへ接続しようとします。もし、RADIUS サーバが接続

可能でなかったら、次の RADIUS サーバに問合せに行きます。しかし、もし RADIUS サーバに接続できたが認証が失敗した場合、認証プロセスは次のサーバをチェックしません。
認証を設定するため次のステップを実行します。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

2．認証サーバとして RADIUS をスイッチに追加するため、'radius-server'コマンドを使います。このコマンドは、追加のサーバに対して繰り返し実行します。しかし、このコマンドは新しい RADIUS サーバをアクセスリストの先頭に移動します。

```
switch(config)# radius-server host 10.0.0.5
```

3．装置で 802.1x 認証を有効化します。

```
switch(config)# dot1x enable
```

4．修正するインタフェースを選択するため、'interface'コマンドを使用します。

```
switch(config)# interface tengigabitethernet 1/12
```

5．802.1x 認証を有効化するため、'dot1x authentication'コマンドを使います。

```
switch(conf-if-te-1/12)# dot1x authentication
```

6．特権実行モードに戻ります。

```
switch(conf-if-te-1/12)# end
```

7．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

22.4　802.1x のインタフェース固有の管理作業

装置で 802.1x ポート認証プロトコルを設定することは必須で、各インタフェースに対して 802.1x を有効化し、カスタマイズすることが必要です。
802.1x が 266 ページの『22.3 802.1x 認証設定作業』で有効化され、設定されたので、インタフェースの設定をするため必要なカスタマイズをするためにこのセクションにある作業を行います。

22.4.1　802.1x readiness check

802.1x readiness check は、すべてのスイッチポートで 802.1x アクティビティを監視し、802.1x をサポートするポートに接続されているデバイスに関する情報を表示します。スイッチのポートに接続された装置が 802.1x 対応であるかどうかを判断するには、この機能を使用します。
802.1x readiness check は、802.1x に設定することができ、すべてのポート上で許可されています。'dot1x force-unauthorized'コマンドによって設定されたポートでは、 readiness check は使用できません。
802.1x 対応ポートで'dot1x test eapol-capable'コマンドを設定し、リンクがアップになっても、そのポートは、802.1x 機能について接続されたクライアントを照会します。クライアントが通知パケットで応答した場合、802.1x に対応しています。クライアントがタイムアウト期間内に応答した場合、RASlog メッセージが生成されます。クライアントが問い合せに応答しない場合、クライアントは、802.1x 対応ではありません。syslog メッセージは、クライアントが EAPOL 対応していないことを示して生成さ

れます。

スイッチの readiness check を可能にするために、これらのガイドラインに従ってください。

- 802.1x がスイッチ上で有効にされる前に readiness check が通常使用されます。
- 802.1x の readiness test の進行中に、802.1x 認証を開始することはできません。
- 802.1x 認証がアクティブである間、802.1xreadiness test を開始することはできません。
- 802.1xreadiness はインターフェース毎にチェックすることができます。一度にすべてのインタフェースの readiness check は、サポートされていません。
- 802.1x テストのタイムアウトは、'show dot1x'コマンドで表示されます。

この例では、スイッチの readiness check がポートを照会するのを可能にする方法を示しています。また、それに接続されているデバイスが 802.1x 対応であることを確認する照会ポートから受信した応答を示しています。

```
switch# dot1x test eapol-capable interface gigabitethernet 0/13


DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet0/13 is
EAPOL capable.
```

22.4.2 特定ポートの 802.1x の設定

特定ポートの 802.1x ポート認証を設定するため、特権実行モードで次のステップを実行します。修正が必要なポートに対して、この作業を繰り返してください。

1. グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2. 修正するインタフェースを選択するため、'interface'コマンドを使用します。
   ```
   switch(config)# interface tengigabitethernet 1/12
   ```
3. 802.1x 認証を有効にするため、'dot1x authentication'コマンドを使用します。
   ```
   switch(conf-if-te-1/12)# dot1x authentication
   ```
4. 特権実行モードに戻ります。
   ```
   switch(conf-if-te-1/12)# end
   ```
5. running-config を startup-config へ格納するため、'copy'コマンドを入力します。
   ```
   switch# copy running-config startup-config
   ```

22.4.3 特定ポートの 802.1x タイムアウトの設定

NOTE

タイムアウトを修正することは自由ですが、デフォルト値のままにしておくことを推奨します。

特定ポートの 802.1x タイムアウト属性を設定するため、特権実行モードで次の手順を実行します。修正したいインタフェースに対して、この作業を繰り返します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．修正するインタフェースを選択するため、'interface'コマンドを使用します。

```
switch(config)# interface tengigabitethernet 1/12
```

3．タイムアウト値を設定します。

```
switch(conf-if-te-1/12)# dot1x timeout supp-timeout 40
```

4．特権実行モードに戻ります。

```
switch(conf-if-te-1/12)# end
```

5．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

22.4.4 特定ポートの 802.1x 再認証の設定

特定ポートの 802.1x ポート再認証機能を設定するため、特権実行モードで次の手順を実行します。修正したいインタフェースに対して、この作業を繰り返します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．修正するインタフェースを選択するため、'interface'コマンドを使用します。

```
switch(config)# interface tengigabitethernet 1/12
```

3．インタフェースに対して 802.1x 認証を有効にします。

```
switch(conf-if-te-1/12)# dot1x authentication
```

4．インタフェースに対して再認証機能を設定します。

```
switch(conf-if-te-1/12)# dot1x reauthentication
switch(conf-if-te-1/12)# dot1x timeout re-authperiod 4000
```

5．特権実行モードに戻ります。

```
switch(conf-if-te-1/12)# end
```

6．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

22.4.5 特定ポートの 802.1x ポート制御の設定

特定ポートの 802.1x ポート制御機能を設定するため、特権実行モードで次の手順を実行します。修正したいインタフェースに対して、この作業を繰り返します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．修正するインタフェースを選択するため、'interface'コマンドを使用します。

```
switch(config)# interface tengigabitethernet 1/12
```

3．インタフェースに対して 802.1x 認証を有効にします。

```
switch(conf-if-te-1/12)# dot1x authentication
```

4．ポート認証モードを、auto, force-authorized, force-unauthorized に設定します。

```
switch(conf-if-te-1/12)# dot1x port-control
auto/force-authorized/force-unauthorized
```

5．特権実行モードに戻ります。

```
switch(conf-if-te-1/12)# end
```

6．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

22.4.6 特定ポートの再認証

特定ポートに接続されたサプリカントを再認証するために、特権実行モードで次の手順を実行します。修正したいインタフェースに対して、この作業を繰り返します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．修正するインタフェースを選択するため、'interface'コマンドを使用します。

```
switch(config)# interface tengigabitethernet 1/12
```

2．dot1x が既に有効化されているポートで再認証を開始します。

```
switch# dot1x reauthenticate
```

3．特権実行モードに戻ります。

```
switch(conf-if-te-1/12)# end
```

4．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

22.4.7 特定ポートの 802.1x の無効化

特定ポートの 802.1x 認証を無効化するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．修正するインタフェースを選択するため、'interface'コマンドを使用します。

```
switch(config)# interface tengigabitethernet 1/12
```

3．802.1x 認証を無効にするため、'no dot1x port-control'を使用します。

```
switch(conf-if-te-1/12)# no dot1x authentication
```

4．特権実行モードに戻ります。

```
switch(conf-if-te-1/12)# end
```

5．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

22.4.8 装置の 802.1x を無効化

装置全体の 802.1x 認証を無効化するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力し

ます。

2．802.1x 認証を無効にするため、'no dot1x enable'を使います。

```
switch(config)# no dot1x enable
```

3．特権実行モードに戻ります。

```
switch(config)# end
```

4．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

22.4.9 802.1x 設定の確認

802.1x の設定を確認するため、特権実行モードで次の手順を実行します。

1．dot1x 設定情報を見るため、'all'オペランド付で'show dot1x'コマンドを使用します。

```
switch# show dot1x all
```

2．特定のインタフェースの 802.1x 設定を確認するため、'interface'オペランド付で'show dot1x'コマンドを使用します。

```
switch# show dot1x interface tengigabitethernet 1/12
```

3．特定ポートの 802.1x 認証統計情報を確認するために、'statistics interface'オペランド付で'show dot1x'コマンドを使用します。

```
switch# show dot1x statistics interface tengigabitethernet 1/12
```

4．特定ポートに関連した認証の診断情報を確認するために、'diagnostics interface'オペランド付で'show dot1x'コマンドを使用します。

```
switch# show dot1x diagnostics interface tengigabitethernet 1/12
```

5．確立されたセッションのすべての統計情報を確認するには、'session-info interface'オペランド付きで'show dot1x'コマンドを使用します。

```
switch# show dot1x session-info interface tengigabitethernet 1/12
```

23 sFlow の設定

23.1 sFlow プロトコル概要

sFlow プロトコルは、高速スイッチネットワークの監視機能の業界標準技術です。sFlow 規格は、デバイス上で動作する sFLow エージェントと中央サーバで動作する sFlow コレクタからなります。
sFlow エージェントは､sFlow データグラムにフローサンプルとインターフェースカウンタを結合して、一定間隔で sFlow コレクタに転送します。データグラムは、限定されるわけではありませんが、パケットヘッダ、入力インターフェースと出力インターフェース、サンプリングパラメータ、およびインタフェースカウンタから成ります。パケットサンプリングは、一般的に ASIC で実行されます。sFlow コレクタは、異なるデバイスから受信した sFlow データグラムを分析し、トラフィックフローのネットワーク全体ビューを生成します。
sFlow データグラムは、sFlow のバージョン、エージェントの IP アドレス、シーケンス番号、1 つのサンプルとプロトコル情報に関する情報を提供します。
sFlow エージェントは２つの操作形式を使います。

- インタフェースカウンタの時間ベースのサンプリング
- スイッチパケットの統計サンプリング

23.1.1 インタフェースフローサンプル

フローの採取は、一定間隔で定義された sFlow コレクタへ転送されるランダムパケットに基づいて、DCB スイッチの装置全体か一つのポートかの何れかに対して行われます。例えば、4096 回毎のパケットが解析と保存のため sFlow コレクタに転送されます。サンプリングレートが適応され、sFlow エージェントは、内部効率を最大化するため自由にサンプリングをスケジュールできます。

NOTE
ランダムサンプリングのタイプは、概算のフローレートを提供するのみで、精度はありません。

23.1.2 パケットカウンタサンプル

ポーリング間隔は、特定インタフェースの sFlow オクテットとパケットカウンタが、どの位の頻度でコレクタに送信ささされるかを定義します。しかし、sFlow エージェントは内部の効率を最大限にするため自由にポーリングをスケジュールできます。

23.2 装置での sFlow プロトコル設定

最初はスイッチ全体での sFlow を設定し、それから、特定ポートの sFlow を有効化して個別の設定をすることを推奨します。詳細は、273 ページの『23.3 sFlow のインタフェース個別管理の作業』を参照下さい。

sFlow を装置で有効化することは、全てのポートで動作させることではありません。sFlow は必要とする全てのポートで明示的に有効化されなければなりません。詳細は、274 ページの『23.3.1 特定インタフェースの sFlow の有効化とカスタマイズ』を参照下さい。

NOTE
sFlow の CLI コマンドの情報は、『Network OS Command Reference』を参照下さい。

装置で sFlow を設定するために、グローバルコンフィグレーションモードで次のステップを実行してください。

1. sFlow プロトコルを装置全体で有効化します。

```
switch(config)# sflow enable
```

2. sFlow コレクタサーバの IP アドレスを指定します。必要に応じて、ポート番号を指定することができます。

```
switch(config)# sflow collector 192.10.138.176 6343
```

3. 秒単位で sFlow polling ingerval を設定します。

```
switch(config)# sflow polling-interval 35
```

4. sFlow sample-rate を設定します。

```
switch(config)# sflow sample-rate 4096
```

5. 特権実行モードに戻ります。

```
switch(config)#end
```

6. 'show sflow'コマンドを使って、sFlow の設定を確認します。

```
switch# show sflow
sFlow services are:          enabled
Global default sampling rate:     4096 pkts
Global default counter polling interval: 1 secs
Collector server address:       192.10.138.176:6343
Number of samples sent:        30
```

7. 正確な読み取りを確実にするために、既存の sFlow 統計情報をクリアします。

```
switch# clear sflow statistics
```

23.3 sFlow のインタフェース個別管理の作業

装置の sFlow 設定の後、sFlow は必要とするインタフェース全てで明示的に有効化する必要があります。

NOTE
インタフェースポートの sFlow が有効化されたとき、サンプリングレートとポーリング間隔は装置設定が引き継がれます。

23.3.1 特定インタフェースの sFlow の有効化とカスタマイズ

NOTE

SPAN および sFlow は、同時に有効にすることはできません。

インタフェースで sFlow を有効化し、カスタマイズするには、特権実行モードで次の手順を実行します。このタスクは、sFlow データが既にグローバルレベルで有効にされているものと仮定し、272 ページの 『23.2 装置での sFlow プロトコル設定』を参照してください。

1. DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを入力します。

```
switch(config)# interface tengigabitethernet 0/16
```

2. sFlow polling interval を設定します。

```
switch(conf-if-te-0/16)# sflow polling interval 35
```

3. インタフェースで sFlow を有効化するために'sflow enable'コマンドを使います。

```
switch(conf-if-te-0/16)# sflow enable
```

4. sFlow sample-rate を設定します。

```
switch(conf-if-te-0/16)# sflow sample-rate 8192
```

5. 指定したインタフェースの sFlow 設定を確認します。

```
switch# show sflow interface tengigabitethernet 12/0/53
sFlow info for interface TenGigabitEthernet 12/0/53
-------------------------------------------------
Configured sampling rate:          32768 pkts
Actual sampling rate:             65536 pkts
Counter polling interval:          20 secs
Samples received from hardware:     291
Port backoff-threshold :           6
Counter samples collected :        10
```

23.3.2 特定インタフェースの sFlow の無効化

特定ポートの sFlow を無効化するため、インタフェースコンフィグレーションモードで次のステップを実行します

1. インタフェースの sFlow を無効化します。

```
switch(conf-if)# no sflow enable
```

2. 特権実行モードに戻ります。

```
switch(conf-if)# end
```

3. 指定したインタフェースの sFlow 設定を確認します。

```
switch# show sflow interface tengigabitethernet 0/12
```

NOTE

特定インタフェースの sFlow 設定を無効化することによって、その他のインタフェースのサンプリング情報が正しく採取できなくなった場合は、次の手順で sFlow の再設定を行い回復してください。

1．全てのインタフェースを一旦停止します。(モニタ対象の全インタフェースに対し実施します。)

```
switch(config)# interface tengigabitethernet 0/1
switch(config-if)# shutdown
```

2．当該インタフェースを再開します。(モニタ対象の全インタフェースに対し実施します。)

```
switch(config-if)# no shutdown
```

3．sFlow プロトコルを装置全体で一旦無効化します。

```
switch(config-if)# exit
switch(config)# no sflow enable
```

4．sFlow プロトコルを装置全体で再度有効化します。

```
switch(config)# sflow enable
```

5．インタフェースの sFlow を無効化します。(モニタ対象の全インタフェースに対し実施します。)

```
switch(config)# interface tengigabitethernet 0/1
switch(conf-if)# no sflow enable
```

6．『23.3.1 特定インタフェースの sFlow の有効化とカスタマイズ』に倣って、再度 sFlow 設定を再定義してください。

23.3.3 sFlow のためのハードウェアサポートマトリックス

表 23-1 は、ハードウェアでサポートされる sFlow 機能を説明します。

表 23-1　sFlow 機能サポート

機能	内蔵 DCB スイッチモジュール
sFlow global configurations for enabling sFlow, polling interval, collector, and sample rate	すべてサポート
sFlow data source interface	10Gbps インタフェースのみサポート
sFlow data source: Front port trunks and VLANs	非サポート
sFlow scanning for inbound, outbound, or both directions on a port	inbound のみサポート
sFlow counter polling support on per-port, per-VLAN, or per-trunk	per-port の counter polling のみサポート
All standard if_counters and Ethernet counters	サポート
Multiple collector configuration	非サポート
Extended Gateway, Extended router, and NAT/MPLS/URL header formats	非サポート
Subagent-ID	ゼロ（0）埋め
Agent IP address	Management IP
Maximum packets per second	96 pkts/sec/ASIC
Sample rate calculation	ドロップされたパケットは、サンプル生成に使用される計算のためにカウントされます。（エラーと ACL ドロップされたパケット）
Maximum sFlow raw packet header size	128 bytes ソフトウェアはパケットを切り捨てます。
SPAN and sFlow configurations	SPAN および sFlow は、同時に有効にすることはできません。

24 スイッチドポートアナライザ(SPAN)設定

24.1 スイッチドポートアナライザプロトコルの概要

スイッチドポートアナライザ(SPAN:Switched Port Analyzer)は、あるスイッチポートのネットワークパケットのコピーをネットワーク監視用の別のスイッチポートに送るためスイッチ上の機能です。もし、特定ポートを通るトラフィックを監視したい場合、SPAN はアナライザに接続したポートにパケットをコピーします。通常、このトラフィックは受信または送信パケットに限定されますが、Network OS は送信元ポートの双方向のトラフィックモニタも可能です。

24.1.1 SPAN の制限

SPAN 接続の制限は下記の通りです。

- ミラーポートはスイッチのどのポートでも可能です。
- スイッチ当たり一つのポートだけが、受信ミラー用の宛先ポートとして設定できます。
- スイッチ当たり一つのポートだけが、送信ミラー用の宛先ポートとして設定できます。
- ミラーポートは、通常トラフィックを転送するために設定できません。
- 同一ポートを複数のポートにミラーすることはできません。
- チップ上の異なるポートがすでにミラーリングの任意のタイプの宛先ポートとして設定されている場合、ポートは双方向ミラーリングの宛先ポートにすることはできません。
- ポートが双方向のミラーリングの宛先ポートとして設定されている場合、そのチップ上の他のポートがミラーリングのあらゆるタイプの宛先ポートを行うことはできません。
- 宛先のミラーポートは、10G でのみ使用できます。もし複数のポートや同一ポーとの両方向のフローが同一のミラーポートにミラーされた場合、10G 分のミラートラフィックのみがミラーされ、残りは破棄されます。
- 送信元ポートは、トラフィックバーストを受信し、宛先のミラーポートがすべてのバーストを処理することはできない場合、バーストトラフィックの一部がミラー化されません。
- ISL ポートのミラーリングはサポートされません。
- LAG またはポートチャネルインタフェースのミラーリングはサポートされませんが、LAG メンバーをミラー化できます。
- TRILL ポートは、送信元ポートまたは宛先ポートとして指定することはできません。
- ポーズフレームはミラーリングされません。
- ASIC は、トランクのミラーリングをサポートしていますが、トランクポートのミラーリングはサポートされていません。トランクをミラーリングするには、個別にすべてのメンバポートのミラーリングを有効にする必要があります。
- マルチキャストおよびブロードキャストの統計情報が不正確にミラーリングされたトラフィックの TX ポート上で更新されます。
- 'shutdown'および'no shutdown'を除くすべてのコマンドは、宛先のミラーポートでブロックされて

います。

- ポートが正常先のミラーポートに指定された場合、インターフェースカウンタがクリアされます。
- 'show interface'コマンドは 、"Receive Statistics"と"Rate Info (Input)"の宛先ミラーポートのための情報を隠蔽します。
- ポートの MTU はその宛先にミラーポートを作成する前に 2500 バイトのデフォルト値に設定する必要があります。ポートが正常に送信先ミラーとして指定されると、そのポートの MTU は自動的に 9208 バイトの最大値に設定されます。ポートが非送信先ミラーになると、MTU はデフォルト値に復元されます。
- ポートミラーリングを設定するには、任意の物理的なフロントエンドのユーザ設定可能なポートでサポートされています。送信元ポートは LAG、VLAG、VLAN、または他のユーザーの構成の一部にすることができます。
- 24 ミラーセッションの最大数は、スタンドアロンおよびファブリッククラスタモードでサポートされています。
- 512 セッションの最大数は管理クラスタモードでサポートされます。

24.2　入力 SPAN の設定

入力パケットだけに SPAN を設定するため、グローバルコンフィグレーションモードで次の手順を実行します。

1．モニタセッションをオープンし、セッション番号を割り当てます。

```
switch(config)# monitor session 1
```

2．受信パケットに対する'rx'パラメータを指定し、ソースポートと宛先ポートを設定します。

```
switch(config-session-1)# source tengigabitethernet 1/0/15 destination
tengigabitethernet 1/0/18 direction rx
```

3．オプション設定：'description'コマンドでモニタセッションにラベルを付加します。

```
switch(config-session-1)# description Hello World!
```

4．ステップ１から２を必要なポートに対して繰り返します。
モニタセッションは一つのソースポートしか定義できません。追加ポートのために、別のモニタセッションを作成しなければなりません。

24.3　出力 SPAN の設定

出力パケットだけに SPAN を設定するため、グローバルコンフィグレーションモードで次の手順を実行します。

1．モニタセッションをオープンしセッション番号を割り当てます。

```
switch(config)# monitor session 1
```

2．送信パケットに対する'tx'パラメータを指定し、ソースポートと宛先ポートを設定します。

```
switch(config-session-1)#source tengigabitethernet 1/0/15 destination
tengigabitethernet 1/0/18 direction tx
```

3．オプション設定：'description'コマンドでモニタセッションにラベルを付加します。

```
switch(config-session-1)# description Hello World!
```

4．ステップ１から２を必要なポートに対して繰り返します。
モニタセッションは一つのソースポートしか定義できません。追加ポートのために、別のモニタセッションを作成しなければなりません。

24.4　双方向に対する SPAN の設定

両方向のパケットに SPAN を設定するため、グローバルコンフィグレーションモードで次の手順を実行します。

1．モニタセッションをオープンしセッション番号を割り当てます。

```
switch(config)# monitor session 1
```

2．両方向のため'both'パラメータを指定し、ソースポートと宛先ポートを設定します。

```
switch(config-session-1)# source tengigabitethernet 1/0/15 destination
tengigabitethernet 1/0/18 direction both
```

3．オプション設定：'description'コマンドでモニタセッションにラベルを付加します。

```
switch(config-session-1)# description Hello World!
```

NOTE
次のエラーが表示される場合は、先行する前に、宛先ポートで LLDP を無効にします。

% Error: Destination port cannot be in L2/L3/Qos/ACL/802.1x/LAG

member/Lldp/Port-profile/non-default-MTU

4．ステップ１から２を必要なポートに対して繰り返します。
モニタセッションは一つのソースポートしか定義できません。追加ポートのために、別のモニタセッションを作成しなければなりません。

24.5　セッションから SPAN 接続の削除

SPAN セッションから一つの接続を削除するため、グローバルコンフィグレーションモードで次の手順を実行します。

1．モニターセッションの定義済みの設定を表示します。

```
switch# show monitor session 1
```

2．定義済みのモニターセッションを開きます。

```
switch(config)# monitor session 1
```

3．特定のポート接続を削除するため'no'オプションを使います。

```
switch(config-session-1)# no source tengigabitethernet 1/0/15 destination
tengigabitethernet 1/0/18 direction both
```

4．接続が削除されたかを確かめるためモニターセッションを表示します。

```
switch# show monitor session 1
```

24.6　SPAN セッションの削除

SPAN セッションを削除するため、グローバルコンフィグレーションモードで次の手順を実行します。

1．モニターセッションの定義済みの設定を表示します。

```
switch# show monitor session 1
```

2．'config'コマンドを使って、コンフィグレーションモードに入ります。

3．'no'オプションを使って、定義済みのモニターセッションを削除します。

```
switch(config)# no monitor session 1
```

4．'exit'コマンドで特権実行モードに戻ります。

5．接続の削除を確認するため、モニターセッションを再度表示します。

```
switch# show monitor session 1
```

25 Network OS レイヤ 3 ルーティング機能

25.1 インバンド管理の概要

内蔵 DCB スイッチ上のインバンド管理を使用すると、レイヤ 3 対応のフロントエンドイーサネットポートを介してスイッチモジュールを管理することができます。管理トラフィックとデータトラフィックが同一の物理ポートを使用するため、インバンド管理インタフェースは、比較的簡単に設定でき、最もコスト効果の高い管理ソリューションです。したがって、管理トラフィックをサポートするため特別なインフラは必要ありません。欠点は、データネットワーク内の任意の問題が管理されたデバイスへの接続が失われ、管理機能の損失を引き起こす可能性があるということです。したがって、インバンド管理が利用できなくなった時のために、アウトバンドでの最終手段として、ネットワーク内の任意のデバイス専用のシリアル接続または管理専用のネットワーク(アウトバンド管理)を構築することを強く推奨お勧めします。
インバンド管理は、ファームウェア、SNMP ポーリング、SNMP トラップ、トラブルシューティング、およびアウトオブバンド管理インターフェースでは使用できない設定のダウンロードなどの管理作業を容易にします。表 25-1 は、インバンド管理で使用できるアプリケーションのいくつかを示します。アプリケーションのリストは、全ケースを網羅しているものではありません。

表 25-1 インバンド管理用にサポートされるアプリケーション

アプリケーション	説明
FWDL	外部サーバから FTP または SCP を使用してリモートデバイスにファームウェアをダウンロードします。
SCP	Secure Copy Protocol（SCP）を使ってファイルを転送します。
SSH	Secure Shell アプリケーションを介してデバイスに接続します。
SNMP	Secure Network Management Protocol（SNMP）を使用してデバイスを管理します。
telnet	telnet を使用してデバイスに接続します。

25.1.1 前提条件

管理ステーションは、IP アドレスおよび管理ネットワークまでのルートを取得することができなければなりません。静的 IP アドレスを使用するか、動的または DHCP などのプロトコルを介して IP アドレスを得るために、管理ステーションを構成することができます。デフォルトゲートウェイは、管理ステーションから管理ネットワークへのすべてのパケットを転送するために使用することができます。53 ページの『3.5 イーサネット管理インタフェースの構成』を参照してください。

加えて、IP ルートとサブネットを設定する必要があります。管理アクセス用に設定したフロントエンドイーサネットポートは、ターゲットデバイスとの通信を可能にするために実装された IP 転送を使用してルータとして動作します。管理ステーションと管理対象デバイスが別々のサブネットにある場合、

通信が行われるようにネットワーク全体に IP ルートを設定する必要があります。スタティックルーティングなどを使用するように管理インターフェースを設定することができます。

- スタティックルーティングを使用するインバンド管理インターフェースを設定するには、290 ページの『27.3 スタティックルートの設定』を参照してください。

Network OS V3.0.0 以降が稼動しているスイッチでは、インバンド管理がレイヤ 2 またはレイヤ 3 ネットワークを介してデバイスを管理するため、VCS モードでサポートされています。スタンドアロンモードでは、管理ステーションはスタンドアロンモードの別のノードに直接接続します。Network OS v3.0.0 以前のファームウェアが稼働しているスイッチでは、インバンド管理はスタンドアロンモードでのみサポートされています。

インバンド管理は、特別なコンフィギュレーションコマンドを必要としません。なぜなら、管理用トラフィックは、既存の IP ルーティングインフラストラクチャに乗り、インバンド管理インターフェースを設定するために必要なコマンドは、ターゲットデバイスへの接続を提供するために、静的または動的なルーティングプロトコルでサポートされる IP インターフェースを設定するコマンドと同じだからです。

25.1.2 サポートインタフェース

インバンド管理は、表 25-2 に示すインターフェースでサポートされます。これらの各インターフェースに使用できるコンフィギュレーションオプションの詳細については、『Network OS Command Reference』の'interface'コマンドのマニュアルを参照してください。

表 25-2　インバンド管理のためのポート構成

インタフェース	アドレス指定	説明
Management (Ma)	rbridge-id/slot	管理インタフェース
GigabitEthernet (Gi)	rbridge-id/slot/port	1Gb イーサネット物理インタフェース
TenGigabitEthernet (Te)	rbridge-id/slot/port	10Gb イーサネット物理インタフェース
Port-channel (Po)	interface-id（スタンドアローンモードの IP または Po）	ポートチャネルインタフェース
Virtual Ethernet (Ve)	interface-id（VLAN ID 対応）	仮想イーサネットインタフェース

NOTE

Virtual Ethernet (Ve)インタフェースは、レイヤ 3 スイッチに設定された Virtual LAN (VLAN)に関連付けられた論理ポートです。外部ルータを使用せずに、1 つのレイヤ 3 VLAN から別の VLAN にトラフィックを中継するレイヤ３スイッチ機能を有効にするため仮想インタフェース上にルーティングパラメータを設定することが出来ます。Ve インターフェースを設定する前に、対応する VLAN を設定する必要があります。

25.2　スタンドアロンインバンド管理インターフェースの設定

図 25-1 は、スタンドアロンモードでインバンド管理インターフェースの構成を示します。この例では、Switch-A と Switch-B のための管理ステーション IP アドレスとイーサネットポートインタフェース IP アドレスのすべてが、同じサブネット内にあり、管理ステーションと Switch-A を介して Switch-B に接続するためのルーティングプロトコルは必要ではありません。サーバまたはワークステーションの管理ステーションは、物理的に付けられた switch-A に接続し、switch-A が物理的に接続した switch-B に接続することができます。

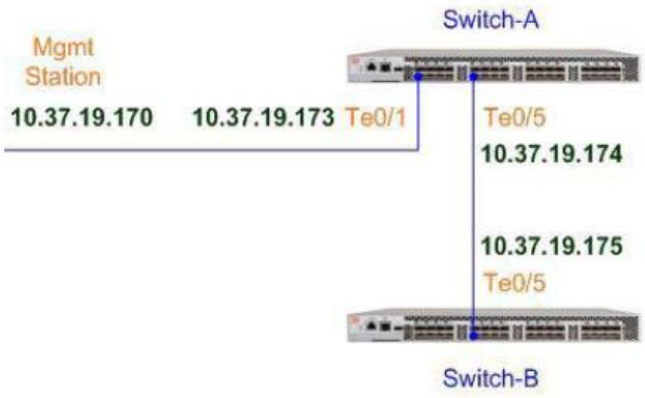

図 25-1 スタンドアロンモードの管理ステーションとネットワークデバイスの通信

図 25-1 に示す構成では、次の操作をサポートします。

- 管理ステーションから Switch-A に SSH または telnet セッションを介して接続する。
- 管理ステーションと Switch-A 間で Secure Copy Protocol（SCP）または FTP を使用してファイルを転送する。
- Switch-A と Switch-B 間で Secure Copy Protocol（SCP）を使用してファイルを転送する。
- Switch-A と Switch-B の間で、表 25-1 のアプリケーションのいずれかを使用する。

25.2.1　スタンドアロンモードでのインバンド管理インタフェースの供給

次の手順は、図 25-1 に示すように、インバンド管理インターフェースを設定します。

1．利用可能な場合、シリアルコンソールを介して、または管理インタフェースを介してスイッチに接続します。
2．グローバルコンフィギュレーションモードを入力するために、'configure terminal'コマンドを入力します。
3．'interface'コマンドに続いて設定したいインタフェースのタイプを入力します。
スタンドアロンインバンド管理インターフェースの場合、物理的なユーザーポート（1GbE、10GbE）だけは、IP アドレスで設定する必要があります。VLAN または VE のインタフェースのいずれかを設定する必要はありません。
4．インタフェースに IPv4 アドレスを設定するには、'ip address IPv4_address/prefix_length'コマンドを入力します。

NOTE
プライマリ IP アドレスのみ、設定する必要があります。セカンダリ IP アドレスはサポートされていません。

5．バイト単位でインタフェースの IP Maximum Transmission Unit (MTU)を設定するために、'ip mtu'コマンドを入力します。
6．Address Resolution Protocol（ARP）のためのインタフェースタイムアウトパラメータ値を分単位で設定するために、'arp-ageing-timeout'コマンドを入力します。デフォルトのタイムアウト値は 4 時間です。
7．未使用の ARP エントリを削除するには、'no-refresh'オプションで'do clear-arp-cache'コマンドを入力して、ARP キャッシュをクリアします。
8．'ip proxy-arp'コマンドを使用してインターフェース毎にプロキシ ARP を設定します。
9．'show ip interface'コマンドを使用してコンフィギュレーションを表示します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# interface TenGigabitEthernet 1/0/1
switch(conf-if-te-10/1)# no shutdown
switch(conf-if-te-1/0/1)# ip address 1.1.1.1/24
switch(conf-if-te-1/0/1)# ip mtu 1200
switch(conf-if-te-1/0/1)# arp-ageing-timeout 300
switch(conf-if-te-1/0/1)# do clear-arp-cache no-refresh
switch(conf-if-te-1/0/1)# ip proxy-arp
switch(conf-if-te-1/0/1)# exit

switch# show ip interface TenGigabitEthernet 1/0/1
TenGigabitEthernet 10/1 is up protocol is up
Primary Internet Address is 1.1.1.1/24 broadcast is 1.1.1.255
IP MTU is 1200
Proxy Arp is Enabled
```

```
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
```

25.3　スタンドアロンインバンド管理インタフェースの基本設定

次の設定は、管理ステーションから C1 を介して RB1 へのインバンド管理接続を確立します。この例の目的のため、C1 と RB1 は、スタンドアロンモードで動作します。

1．シリアル接続を介し RB1 でフロントエンドイーサネットポートを設定します。
   a．シリアルコンソールを使用して、RB1 に接続します。
   b．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
   c．'interface vlan vlan_id'コマンドを使用してフロントエンドイーサネットポートを設定します。
   d．RBridge サブコンフィギュレーションモードを開始するため、'rbridge-id rbridge-id'コマンドを入力します。
   e．仮想イーサネットインタフェース（VE）を設定するために、'interface ve ve_id'コマンドを入力します。VE ID は、既存の VLAN ID に対応している必要があります。
   f．インタフェースの IP アドレスを入力します。
   g．インタフェースを有効にするため、'no shutdown'コマンドを入力します。
   h．RB1 が VCS ファブリックの一部ではなくスタンドアロンモードであるかを確認するため、'do show vcs'コマンドを入力します。

```
RB1# configure terminal
Entering configuration mode terminal.
RB1(config)# interface vlan 2
RB1(config)# rbridge-id 1
RB1(config-rbridge-id-1)# interface ve 2
RB1(config-Ve-2)# ip address 2.2.2.17/24
RB1(config-Ve-2)# no shutdown
RB1(config--Ve2)# exit
RB1(config)# do show vcs

state   : Disabled
```

2．C1 は、ノード RB1 の管理ステーションと自動的に telnet 接続します。
3．C1 と管理ステーションとの間および C1 と RB1 との間のインバンド管理接続を確認します（スタンドアロンテスト）。
   a．SSH セッションを使用して、管理インタフェースを介して C1 に接続します。
   b．C1 に、C1 から RB1 への telnet 接続を確立します。

```
C1# telnet 2.2.2.17/24
```

```
Trying 2.2.2.17...
Connected to 2.2.17.24.
Escape character is '^]'.
```

現在、RB1 にログインしている（プロンプトの変化に注意してください）。

c．RB1 で telnet の通知を確認します。

```
RB1# 1970/01/01-02:16:27, [SEC-1203], 13406, M1, INFO, RB1, Login
information: Login successful via TELNET/SSH/RSH. IP Addr: 2.2.17.24
```

d．C1 から telnet のインバンド管理接続を介して、RB1 はスタンドアロンモードであることを確認します。

```
RB1# show vcs


state   : Disabled
```

現在、C1 への管理インタフェース SSH 接続を介して、RB1 のインバンド管理機能（例えば、ファームウェアのダウンロードまたは SNMP 管理）を実行することができます。

26 IP ルートポリシー

26.1 IP ルートポリシーの概要

IP ルートポリシーでは、ルートまたは IP サブネットが 1 サブシステムから別のサブシステムに転送されるかを制御します。マッチするルートに応じて、ターゲットサブシステムに許可または拒否することができるように、IP ルートポリシーでは、許可または拒否のアクションを実行することができます。さらに、IP ルート･ポリシーは、一致したルートおよび IP サブネットペアの特性を変更するために使用することができます。
サポートされる IP ルートポリシーには、プレフィックスリストと'route-map'の 2 つのタイプがあります。

26.1.1 IP プレフィックスリスト

IP プレフィックスリストは、その名前によって識別されます。各 IP プレフィックスリストは、1 つ以上のインスタンスから構成されます。
以下は、IP プレフィックスリストの例を示します。

```
switch(config)# rbridge-id 12
switch(config-rbridge-id-12)# ip prefix-list test seq 1 deny 1.2.0.0/16 ge 17 le 30
switch(config-rbridge-id-12)# ip prefix-list test seq 2 permit 1.1.0.0/16
```

プレフィクスリストインスタンスの整合条件は、1）IP サブネットプレフィクスと 2）プレフィックス（マスク）長(オプション)の２つの部分から構成されます。ge はマスク長の下限値を示し、le はマスク長の上限値を示します。全く ge も le も指定されていない場合は、サブネットプレフィックスの長さが正確に一致しなければなりません。
上記の例では、このルートがサブネット 1.2.0.0/16 内にあり、そのマスク長は 17 と 30 の間であれば、ルートは、インスタンス 1 に一致すると見なされます。つまり、ルート 1.2.1.0/24 と一致しているが、ルート 1.2.1.1/32 は、マスク長のため一致しません。
`route-map'と同様で一致を検出したときに、各プレフィクスリストのインスタンスは、そのインスタンス ID で指定された順番で見られます。検索は、最初に一致した時点で終了します。プレフィクスリスト内に一致するものが見つけられないルートが拒否されます。
現時点では、プレフィクスリストは、単独で使用されません。IP プレフィクスリストは、'route-map'の一致条項の一部として使用することができます。この文脈では、`permit'は、このパターンに一致することを示し、'deny'は、このルートパターンと一致しないことを示します。

26.1.2 Route-map

`route-map'は、その名前によって識別されます。各'route-map'は、1 つ以上のインスタンスから構成されます。各'route-map'インスタンスは、0 以上のマッチング条件と、0 以上のセット条件からなります。

現時点では、'route-map'インスタンスは巨大な定義の固まりです。つまり、エンドユーザは、そのインスタンスを経由して'route-map'を追加したり削除したりする必要があります。たとえば、'route-map'を削除する際に、エンドユーザは、そのすべてのインスタンスで、この'route-map'を削除する必要があります。'route-map'インスタンスで複数の一致条件が含まれる場合があります。すべての一致条件が満たされる場合にだけ、インスタンスの全体的なマッチング条件が成立します。
以下は、'route-map'の例を示します。

```
switch(config-rbridge-id-12)# route-map test deny 1
switch(config-route-map-test/deny/1)# match interface tengigabitethernet 12/0/1
switch(config-route-map-test/deny/1)# exit
switch(config-rbridge-id-12)# route-map test permit 2
switch(config-route-map-test/permit/2)# match ip next-hop prefix-list pre-test
switch(config-route-map-test/permit/2)# set tag 5000
```

インスタンス 1 は、ネクストホップインターフェースが te 0/1 となる任意のルートのエントリを拒否し、インスタンス 2 は、ネクストホップがプレフィクスリストの事前テストで指定された IP サブネットに一致するルートのエントリを許可にします。また、一致した各ルートは、そのタグを 5000 に設定し、保持します。

NOTE

`route-map'インスタンスはマッチング条件を含める必要はありません。それは、このインスタンスの一致条件が常に成立することを意味します。
`route-map'インスタンスで 1 つ以上の設定条件が含まれる場合があります。すべての設定条件は、適用可能なときに一致したルートに適用されます。
`route-map'が適用される時、各インスタンスはインスタンス ID 順に並んだように見えます。もし、一致すると、インスタンスのアクションが適用され、アクションが許可されている場合は、その設定条件が適用されます。検索は、最初に一致した時点で終了します。'route-map"route-map'に一致するものを見つけられないルートは拒否されます。

27 IP ルート管理

27.1 IP ルート管理の概要

IP ルート管理は、Brocade デバイスが IP パケットを転送するための最適なルートを選択するためのルーティングテーブル内の異なる発信元からのルートとネクストホップを管理するソフトウェアを指す用語です。このルート管理ソフトウェアは、システムの起動時に自動的に起動して取得するため、事前の設定が必要ありません。
IP ルート管理は、レイヤ 3 のために構成されているすべてのプラットフォーム上で動作し、以下を提供します。

- 他のプロトコルから提出されたルートを維持します。
- ルート再配布をサポートしています。
- ルータ識別をサポートしています。
- Forwarding Information Base（FIB）までのルートを選択し、同期させます。
- FIB にレイヤ 3 インタフェースを同期します。
- 仮想イーサネット（VE）、ルータポート、ループバックおよび管理のレイヤ 3 インタフェースをサポートしています。

NOTE
IP ルート管理は、IPv4 のみのルートをサポートします。

27.2 IP ルート管理の最適なルートを決定する方法

IP ルート管理に追加されたルートの発信元は以下の通りです。

- スタティック構成されたルート：直接ルートをルートテーブルに追加することができます。IP ルートテーブルにルートを追加する時、スタティック IP ルートを作成します。スタティックルートのデフォルトの管理距離は 1 です。
- スタティック構成されたルート：直接ルートをルートテーブルに追加することができます。IP ルートテーブルにルートを追加する時、スタティック IP ルートを作成します。スタティックルートのデフォルトの管理距離は 1 です。
- インタフェースコンフィギュレーションから直接接続されたルート：IP インタフェースを追加する場合は、Brocade デバイスは自動的にネットワーク用のルートを作成します。直接接続されたルートの管理距離はゼロです。

管理距離は、接続されたルート以外のルートタイプに設定することができます。IP ルート管理は、より低い管理距離を持つルートが望ましいです。

27.3　スタティックルートの設定

rbridge コンフィギュレーションモードで'ip route'および'ipv6 route'コマンドを使用して IP ルート管理へスタティックルートを追加することができます。これらのコマンドを使用してルートを追加するには、ネクストホップゲートウェイまたは出力インターフェースのいずれかを指定できます。

27.3.1　ネクストホップゲートウェイの指定

ネクストホップゲートウェイとして 207.95.6.157 を使用して、207.95.7.0 へのスタティックルートを設定するには、次の例に示すように、Rbridge サブコンフィギュレーションモードで'ip route'コマンドを使用します。

```
switch (config)# rbridge-id 30
switch (config-rbridge-id-30)# ip route 207.95.7.0/24 207.95.6.157
```

以下の例は、IPv6 を用いた同じコマンドです。

```
switch (config)# rbridge-id 30
switch (config-rbridge-id-30)# ipv6 route fe80::21b:edff:fe0b:3c00/64
fe80::21b:edff:fe0b:3c00
```

27.3.2　出力インターフェースの指定

tengigabitethernet ポートを持つスタティック IP ルートを設定するには、次の例に示すように、'ip route'コマンドを入力します。

```
switch (config)# rbridge-id 30
switch (config-rbridge-id-30)# ip route 192.128.2.0/24 te 101/4/1
```

コマンドは、宛先ネットワーク 192.128.2.0/24 のためのスタティック IP ルートを設定します。イーサネットポートがネクストホップとしてゲートウェイ IP アドレスの代わりに指定されているので、Brocade デバイスは、192.128.2.0/24 ネットワークのためのトラフィックを tengigabitethernet ポート 101/4/1 に転送します。

以下の例は、IPv6 を用いた同じコマンドです。

```
switch (config)# rbridge-id 30
switch (config-rbridge-id-30)# ipv6 route fe80::21b:edff:fe0b:3c00/64 te 101/4/1
```

27.3.3　デフォルトルートの指定

デフォルトルートがすべてゼロのプレフィックス/ネットマスクが設定されています（具体的には、0.0.0.0/ 0）。デフォルトルートは、ゼロの宛先プレフィックスを持つ特殊なスタティックルートの例で、他に一致するルートを持っていない全てのトラフィックはデフォルトルートを使用して転送されます。207.95.6.157 のネクストホップでデフォルトルートを設定するには、以下の'ip route'コマンドを入力します。

```
switch(config)# rbridge-id 30
switch(config-rbridge-id-30)# ip route 0.0.0.0/0 207.95.6.157
```

27.4　他のルーティングコマンド

すべての IP ルーティング関連のコマンドの詳細については、『Network OS Command Reference』を参照してください。
例えば：

- 'ip route'コマンドを使用すると、'route-map'でのルートフィルタリングのためのルートのタグ値の指定を許可するオプションを提供します。コマンドはまた、コストメトリックを指定するためのオプションを提供します。
- 'ip load-sharing'コマンドで、8 本までの等価パスをまたいで IP トラフィックのバランスをとれるようになります。
- 'ip route next-hop-recursion'コマンドは、Brocade デバイスに、他のルートを 10 もの再帰的なレベル検索を用いて、ルートを解決することを可能とします。

28 VRRP の設定

28.1 仮想ルータの概要

仮想ルータは LAN 内のルータに冗長性を提供するために、Virtual Router Redundancy Protocol（VRRP）を使用することができる物理的なルータの集まりです。2 つ以上の VRRP 設定されたルータは、仮想ルータを作成することができます。各 VRRP ルータは、LAN インターフェースあたり最大 255 の仮想ルータに参加することができます。

VRRP は、参加しているホストへ動的な仮想 IP ルータを割り当てることによって、静的なデフォルトルート環境でのシングルポイント障害を排除します。仮想ルータ内のすべてのルータのインタフェースは、同じ IP サブネットに属している必要があります。異なる LAN 上の別のアドレスマッピングを持つ Virtual Router ID (VRID)を再利用することに対して制限がありません。

図 28-1 は、いくつかの基本的な VRRP の概念を説明するための基本的な VRRP の設定を示しています。Router1 と Router2 は、一つの仮想ルータを構成するように設定できる 2 つの物理的なルータです。この仮想ルータは、Host1 に冗長なネットワークアクセスを提供します。Router1 に障害が発生した場合、Router2 は、サブネットのデフォルトゲートウェイを提供することができます。

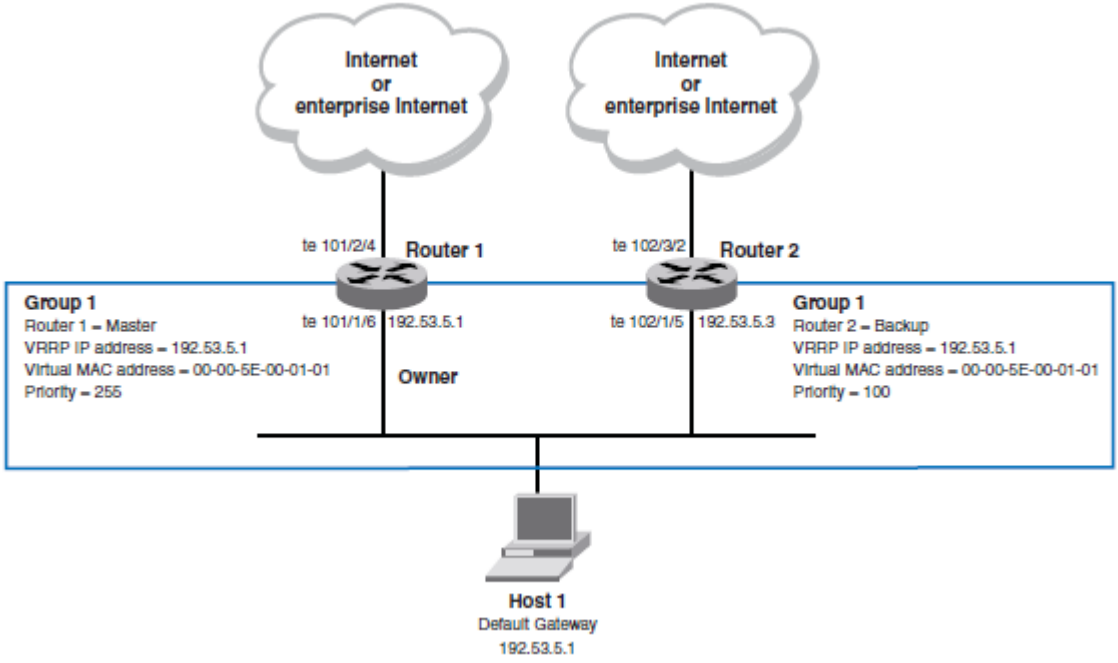

図 28-1 基本的な VRRP の設定

図 28-1 に示す仮想ルータは Group1 として識別されます。仮想ルータの物理的なルータでパケットを転送します。この物理的なルータはマスタルータと呼ばれています。

一般的な VRRP 関連のいくつかの用語や概念を以下に記述します。

- Virtual Router—LAN 内のルータに冗長性を提供するために VRRP または VRRP-E のどちらかのプロトコルを使用することができる物理的なルータの集まりです。

NOTE
この章の大部分の情報は VRRP と VRRP-E にあてはまります、したがって、「VRRP」という語は VRRP または VRRP-E を意味するのにしばしば用いられます。2 つのプロトコルの違いがあるところでは、これらの違いは明示的に記述されています。

- Virtual Router Group—同じ仮想ルータに割り当てられている物理的なルータのグループ。
- Virtual Router Address—バックアップしているアドレス：
  - VRRP の場合：仮想ルータの IP アドレスは VRRP インタフェース上で設定されている実際の IP アドレスと同じサブネットに属している必要があり、VRRP インタフェース上に設定され、実際の IP アドレスと同じにすることができます。
  - VRRP-E の場合：仮想ルータの IP アドレスは VRRP-E インタフェース上に設定されている実際の IP アドレスと同じサブネットに属している必要がありますが、VRRP-E インタフェース上に設定されている実際の IP アドレスと同じにすることはできません。
- Owner—この用語は、VRRP-E に対してではなく、VRRP プロトコルにのみ適用されます。Owner は、仮想ルータに割り当てた IP アドレスが実際のインターフェースの IP アドレスとなっている物理ルータです。Owner は、仮想ルータに対応するどんな IP アドレスを持ったパケットに応答します。Owner は、デフォルトでマスタ（以下の "Master"を参照してください。）であり、最高のプライオリティ（255）を持っています。
- Master—仮想ルータに対応するどんな IP アドレスを持ったパケットに応答物理的なルータ。VRRP の場合、物理的なルータの実際のインターフェースの IP アドレスが仮想ルータの IP アドレスであるならば、この物理的なルータが常にマスタです。VRRP-E の場合は、プライオリティが最高のルータがマスタになります。'priority'コマンドは、物理的なルータのプライオリティを設定するために使用されます。
- Backup—仮想ルータに属しているが、マスタでないルータ。マスタが使用できなくなると、その後、プライオリティが最も高い（設定値）を使用してバックアップルータが新しいマスタになります。デフォルトで、ルータは 100 のプライオリティが与えられます。

28.2 ガイドライン

- 仮想ルータは、仮想クラスタスイッチング（VCS）環境で設定する必要があります。
- 内蔵 DCB スイッチは、VRRP および VRRP-E をサポートしています。
- 内蔵 DCB スイッチは、2 つの VRRP プロトコルをサポートしています。
  - Standard VRRP — 標準ルータ冗長プロトコル。VRRP v2 は IPv4 環境をサポートしています。また、Standard VRRP は、RFC3768 に準拠しています。
  - VRRP-E (Extended) —標準に準拠しておらず、VRRP と相互運用できない標準 VRRP と類似した Brocade 独自のプロトコル
- サポートしているポート：

- VRRP の場合： TenGigabitEthernet、Gigabitethernet と ve。
- VRRP-E の場合： ve ポートのみ。

- IPv4 のみサポートが提供されます。 IPv6 と VRRPv3 はサポートされません。
- サポートされる構成は、VRRP と VRRP-E のインスタンスで最大数は、128 です。インタフェースごとにサポートされる VRRP / VRRP-E のインスタンスの最大数は 16 です。インスタンスは、ルータに設定されたセッションです。
- 仮想ルータのセッションあたりの仮想 IP アドレスの最大数は、VRRP が 16 個で VRRP-E が 1 個です。

28.3 VRRP / VRRP-E パケットの動作

VRRP および VRRP-E が ARP と VRRP 制御パケットを取り扱う方法にいくつかの違いがあります。

28.3.1 Gratuitous ARP

VRRP の場合、VRRP ルータがマスタになったときに一度だけ送信されます。
VRRP-E の場合、VRRP-E の制御パケットは、仮想 MAC アドレスを使用しないため、仮想ルータマスターにより 2 秒ごとに送信されます。

マスタが送信する Gratuitous ARP の送信元 MAC アドレスは、仮想 MAC アドレスです。

マスターまたはバックアップのいずれかのルータが ARP 要求または応答パケットを送信すると、送信者の MAC アドレスはルータインタフェースの MAC アドレスです。一つの例外は、Owner が ARP 要求または応答パケットを送信する場合、送信者の MAC アドレスは仮想 MAC アドレスです。
マスターだけは、仮想ルータ IP アドレスに対する ARP 要求に応答します。この要求を受信する任意のバックアップルータは、マスターに要求を転送します。

28.3.2 VRRP 制御パケット

VRRP の場合、VRRP 制御パケットは、IP プロトコルタイプ 112（VRRP のために予約済み）で、VRRP マルチキャストアドレス 224.0.0.18 に送信されます。
VRRP-E の場合、制御パケットは、ポート 8888 宛ての UDP パケットで、すべてのルータのマルチキャストアドレス 224.0.0.2 に送信されます。

28.3.3 VRRP 制御パケットの送信元 MAC

VRRP の場合、仮想 MAC アドレスが送信元です。
VRRP-E の場合、物理 MAC アドレスが送信元です。

28.4　VRRP の基本的な構成例

いくつかのコマンドを入力して、292 ページの図 28-1 に示す IPv4 の VRRP 設定を実装することができます。このセクションでは、292 ページの図 28-1 に示すように、各ルータを設定するための情報が含まれています。

28.4.1　VRRP のマスターとしての Router 1 の設定

1．Router 1 スイッチ（この例では、ホスト名の SW1）コンソールから、特権実行モードで、コンフィグレーションモードに移行するために、'configure'コマンドを入力します。

```
sw1# configure
```

2．R-bridge ID を使用して、rbridge-id コマンドを入力します。（'do show vcs'コマンドを実行した時にどれかがその横にアスタリスクが付いています）

```
sw1(config)# rbridge-id 101
```

3．全体の VRRP および VRRP-E の両方のプロトコルを有効にします。

```
sw1(config-rbridge-id-101)# protocol vrrp
```

4．Router 1 の tengigabitethernet インタフェースリンクを設定します。

```
sw1(config-rbridge-id-101)# int te 101/1/6
```

5．Router 1 のイーサネットリンクインタフェースの IP アドレスを設定するには、次のコマンドを入力します。

```
sw1(conf-if-te-101/1/6)# ip address 192.53.5.1/24
```

6．Group 1 と呼ばれるグループに Router 1 を割り当てるには、次のコマンドを入力します。

```
sw1(conf-if-te-101/1/6)# vrrp-group 1
```

NOTE

1～255 の範囲でグループ番号を割り当てることができます。

7．仮想ルータの IP アドレスを割り当てるには、次のコマンドを入力します。

```
sw1(config-vrrp-group-1)# virtual-ip 192.53.5.1
```

NOTE

VRRP の場合、IP アドレスを持つ仮想ルータグループの IP アドレスと同じで物理ルータには、所有者とマスターになります。しかし、VRRP-E の場合、マスターとして設定するルータに最高のプライオリティを割り当てるには、'priority'コマンドを使用します。

28.4.2　VRRP のバックアップとしての Router 2 の設定

1．Router 2 スイッチ（この例では、ホスト名の SW2）コンソールから、特権実行モードで、コンフィグレーションモードに移行するために、'configure'コマンドを入力します。

```
sw2# configure
```

2．R-bridge ID を使用して、rbridge-id コマンドを入力します。（'do show vcs'コマンドを実行した時にどれかがその横にアスタリスクが付いています。）

```
sw2(config)# rbridge-id 102
```

3．全体の VRRP および VRRP-E の両方のプロトコルを有効にします。

```
sw2(config-rbridge-id-102)# protocol vrrp
```

4．Router 2 の tengigabitethernet インタフェースリンクを設定します。

```
Sw2(config-rbridge-id-102)# int te 102/1/5
```

5．Router 2 のイーサネットリンクの IP アドレスを設定するには、次のコマンドを入力します。

```
sw2(conf-if-te-102/1/5)# ip address 192.53.5.3/24
```

NOTE

このルータは、Router 1 へのバックアップルータになります。

6．Router 1 と同じ VRRP グループに Router 2 を割り当てるには、次のコマンドを入力します。

```
sw2(conf-if-te-102/1/5)# vrrp-group 1
```

7．Group 1 の仮想 IP アドレスを割り当てるには、Router 1 に使用したのと同じ仮想 IP アドレスを使用します。

```
sw2(config-vrrp-group-1)# virtual-ip 192.53.5.1
```

28.4.3　基本構成のための VRRP-E の相違点

292 ページの図 28-1 に示すように 2 つのルータを設定していた場合は、VRRP-E に固有の以下の項目を考慮する必要があります。

- 'rotocol vrrp'コマンドは、VRRP と同様に VRRP-E を有効にします。'protocol-vrrp-extended'と呼ばれるコマンドはありません。
- VRRP-E のグループコマンドは、'vrrp-extended-group <group-id>'です。
- VRRP-E 仮想ルータは、VE のインタフェース上でのみ設定することができます。

28.5　先取りの有効化

より高いプライオリティ値を持つ別のバックアップルータに、マスターとして動作するバックアップルータを先取りさせておくことができます。
デフォルトでは、VRRP の場合有効になっており、VRRP-E の場合、無効になっています。

NOTE

VRRP のための先取りが無効になっている場合、Owner のルータが常にアクティブマスターを先取りするため、Owner のルータは影響を受けません。

次の例に示すように仮想ルータの先取りを有効にするには、仮想ルータグループコンフィギュレーションモードで、'preempt-mode'コマンドを実行します。

```
switch(config-vrrp-group-5)# preempt-mode
```

28.6　VRRP および VRRP-E でのトラックポートとトラックプライオリティの使用

トラックポートを使用すると、ルート経路のもう一方の端のインタフェースの状態を監視することができます。同じ VRRP グループ内の別の仮想ルータが引き継ぐことができるように、もし出口経路のインタフェースがダウンした場合、トラックポートは仮想ルータのプライオリティを下げることができます。

28.6.1　ルール

- トラックのプライオリティは、VRRP/ VRRP-E のプライオリティより低くなければなりません。
- 先取りが有効になっている場合、ルータプライオリティの動的変更はマスタの切り替えをトリガすることができます。VRRP の適用時のみ、ルータが所有者である場合は、支配力の切り替えが発生しません。
- 仮想ルータの追跡することができるインタフェースの最大数は 16 です。
- ポートトラッキングは、物理インタフェースおよびポートチャネルで許可されます。

28.6.2　トラックプライオリティの例

例として、292 ページの図 28-1 を使用して、インタフェース 101/2/4 を追跡するように、Router1 上の ve 10 インタフェースを設定できます。次に、101/2/4 がダウンした場合、インターフェース ve 10 は、トラックポートプライオリティ値によって Router1 の VRRP の優先度を下げることができます。バックアップルータは、この変化を感知して、新しいマスターになるために交渉します。このように、ネットワークからマスターに連続的な経路を提供します。

次の手順を実行します。

1．インタフェースコンフィグレーションモードに移行するために、以下のコマンドを入力します。

```
switch(config)# int ve 10
```

2．グループコンフィギュレーションモードを開始するために、次のコマンドを実行します。

```
switch(conf-Ve-10)# vrrp-group 1
```

3．トラックポートとプライオリティを設定するために、次のコマンドを実行します。

```
switch(config-vrrp-group-1)# track te 101/2/4 priority 60
```

28.7　ショートパスフォワーディングの使用（VRRP-E のみ）

Brocade デバイスが VRRP-E マスタールータを回避して、バックアップルータのインタフェースを介して、直接宛先にパケットを転送できるように、VRRP-E はサーバ仮想化機能に対する VRRP-E 拡張を使って強化されました。これは、ショートパスフォワーディングと呼ばれています。ショートパスフォワーディングが有効になっている場合にのみ、バックアップルータは VRRP-E のセッションに参加します。

VRRP-E アクティブ－アクティブロードバランシングは、パスを決定するために転送先 MAC アドレスをハッシュすることで、入力 RBridge で実行されます。VCS 内のすべてのノードは、すべての VRRP-E

のセッションおよび各セッションの参加 RBridges を認識しています。
ショートパスフォワーディングが有効になっている場合は、トラフィックがクライアントに到達するためにショートパス転送のパス（図 28-2 の破線）を通過します。仮想 IP アドレスのローカルサブネットからのすべてのパケットは、VRRP-E のマスタールータにルーティングされます。

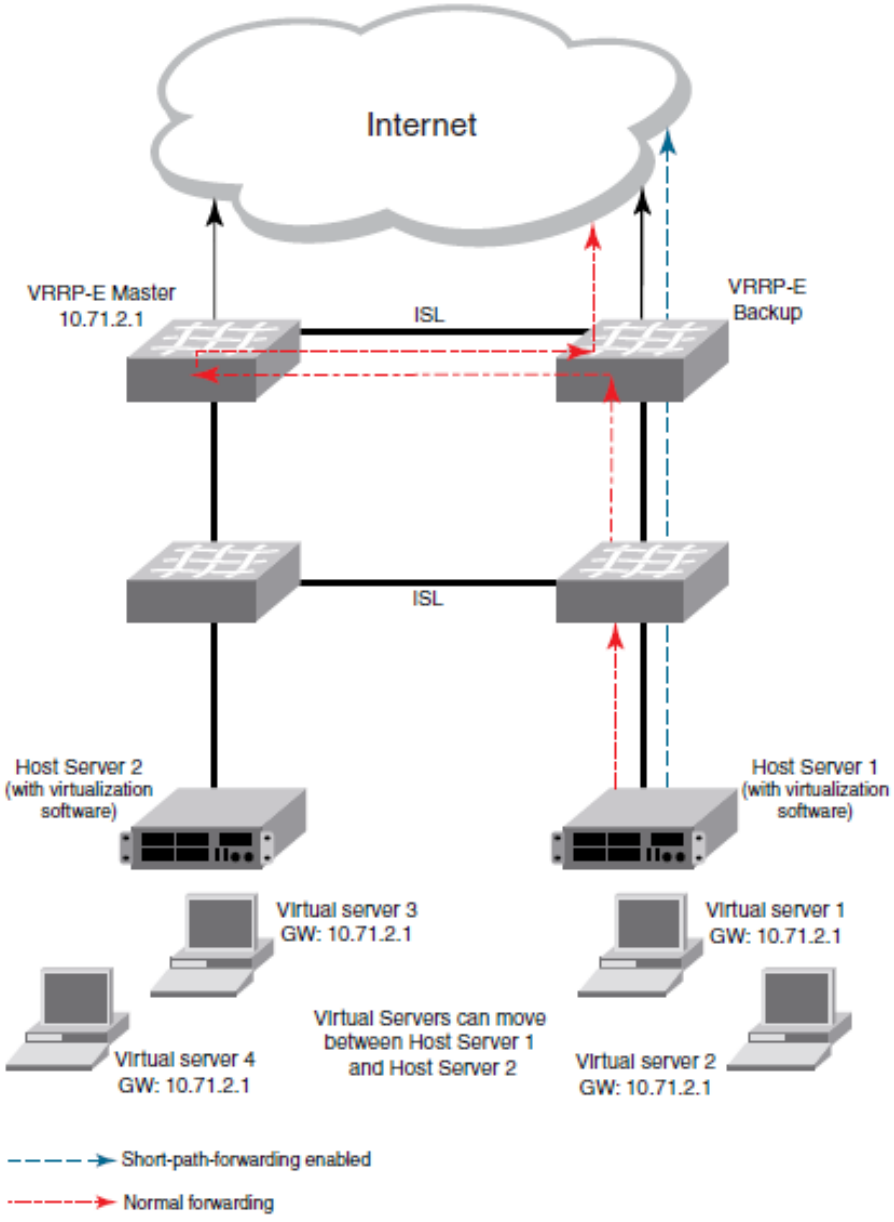

図 28-2 ショートパスフォワーディング

28.7.1 ショートパスフォワーディングの有効化

VRRP-E グループのコンフィギュレーションレベルの下で、ショートパスフォワーディングを有効にするオプションがあります。
例えば、次の手順に従います。

1．スイッチコンフィグレーションモードでは、’int ve’コマンドを実行します。

```
switch(config)# int ve 10
```

2．インタフェイスコンフィギュレーションモードでは、'vrrp-extended-group'コマンドを実行します。

```
switch(config-Ve-10)# vrrp-extended-group 100
```

3．グループコンフィギュレーションモードでは、'short-path-forwarding'コマンドを実行します。

```
switch(config-vrrp-extended-group-100)# short-path-forwarding
```

28.7.2 ショートパスフォワーディングによるパケットルーティング

VRRP-E のショートパスフォワーディングを有効にする場合は、仮想 IP アドレスのローカルサブネットから送信されたすべてのパケットは、マスタルータへ転送される代わりに WAN にルーティングされます。

28.8 VRRP/VRRP-E のためのマルチグループ構成

図 28-3 は、一般的に採用される仮想ルータの設定を示しています。この設定は、2 つの仮想ルータグループを構成することによる冗長構成を紹介しています。 ー 最初のグループは、マスターとして Router 1 とバックアップとしての Router 2 を持ち、第 2 のグループは、マスターとして Router 2 とバックアップとして Router 1 を持ちます。この種の構成は、マルチグループ VRRP と時々呼ばれます。

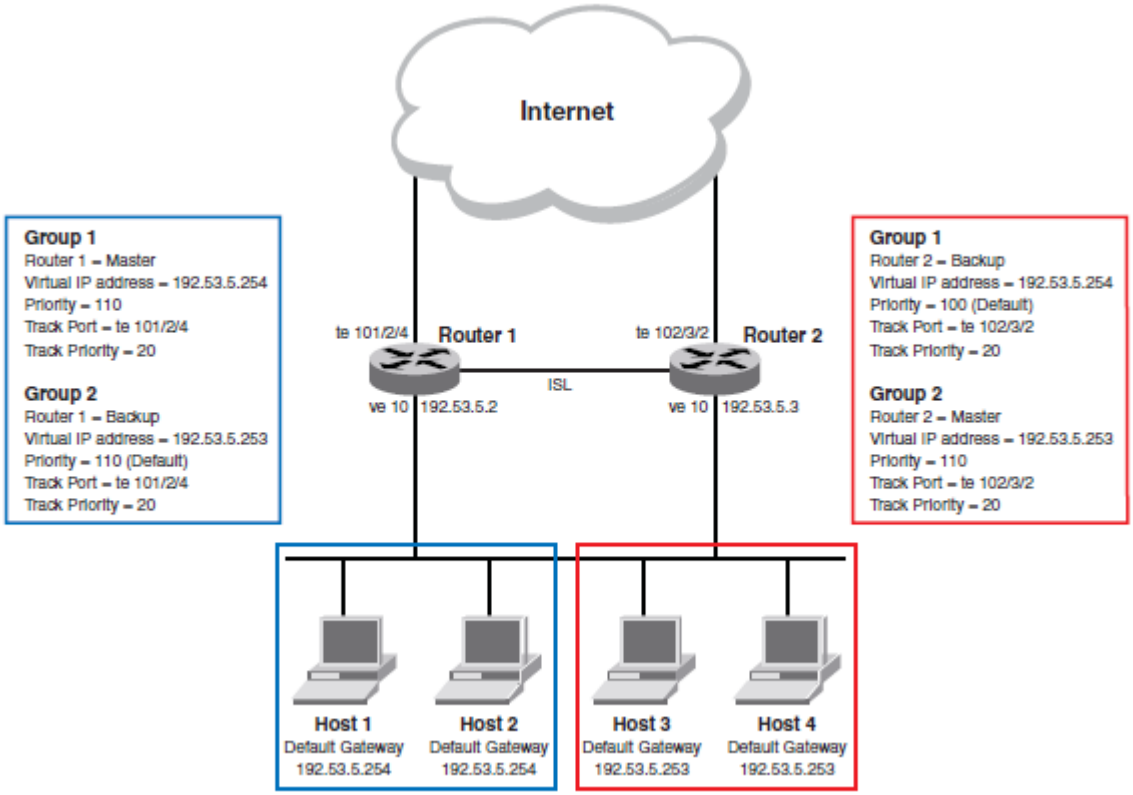

図 28-3 VRRP/VRRP-E のマルチグループ構成

この例では、Router 1 と Router 2 は、冗長性をホストに提供するだけでなく、負荷分散するために、VRRP-E を使います。負荷分散は、2 つの VRRP-E のグループを作成することによって達成されます。各グループは独自の仮想 IP アドレスを持っています。半分のクライアントは、デフォルトゲートウェイとして、Group 1 の仮想 IP アドレスを指し、残り半分は、デフォルトゲートウェイとして、Group 1 の仮想 IP アドレスを示します。これは、アウトバウンドインターネットトラフィックの一部が Router 1 を通過できるようになり、残りの部分が、Router 2 を通過できるようになります。

Router 1 は、Group 1 のマスター（マスタープライオリティ = 110）で、Router 2 は、Group 1 のバックアップ（バックアッププライオリティ = 100）です。Router 1 と Router 2 の両方のインターネットへのアップリンクをトラックします。Router 1 でアップリンク障害が発生した場合、そのバックアップのプライオリティは 20（トラックポートプライオリティ= 20）デクリメントされ 90 となり、インターネット宛てのすべてのトラフィックは、代わりに Router 2 を経由して送られます。

同様に Router 2 は、Group 2 のためのマスター（マスタープライオリティ = 110）で、Router 1 は、Group 2 のためのバックアップ（バックアッププライオリティ = 100）です。Router 1 と Router 2 の両方のインターネットへのアップリンクをトラックします。Router 2 でアップリンク障害が発生した場合、そのバックアップのプライオリティは 20（トラックポートプライオリティ= 20）デクリメントされ 90 となり、インターネット宛てのすべてのトラフィックは、代わりに Router 1 を経由して送られます。

28.8.1 マルチグループ仮想ルータクラスタの設定

300 ページの図 28-3 に示す構成を実装するには、最初の仮想ルータグループのマスターとして機能する 1 つの VRRP-E ルータと第二の仮想グループのバックアップを構成します。次に、最初の仮想グループのバックアップとして機能する 2 番目の VRRP-E ルータと 2 番目の仮想グループのマスターを構成します。

NOTE

この例では、VRRP-E のためのものです。『Network OS Command Reference』を調べることによって決定することができ、VRRP のためのマイナーな構文の違いがあります。

28.8.2 最初の仮想ルータグループのマスターとして Router 1 の設定

VCS が有効になっていることを確認して、次に、これらの手順を実行します。

1. R-bridge ID を使用して、'rbridge-id'コマンドを入力します。（'do show vcs'コマンドを実行した時にどれかがその横にアスタリスクが付いています。）

```
sw101(config)# rbridge-id 101
```

2. 全体に VRRP-E プロトコルを設定するには、次のコマンドを入力します。

```
sw101(config-rbridge-id-101)# protocol vrrp
```

3. Router 1 のための VE インタフェースリンクを設定するために、次のコマンドを入力します。

```
sw101(config-rbridge-id-101)# int ve 10
```

4. Router 1 のための VE のリンクの IP アドレスを設定するために、次のコマンドを入力します。

```
sw101(conf-Ve-10)# ip address 192.53.5.2/24
```

5. Group 1 と呼ばれる VRRP-E グループに Router 1 を割り当てるために、次のコマンドを入力します。

```
sw101(conf-Ve-10)# vrrp-extended-group 1
```

6. 20 のトラックプライオリティを使用して、インタフェース ve15 のためのトラッキングポートとして、tengigabitethernet ポート 101/2/4 を設定するには、次のコマンドを入力します。

```
sw101(config-vrrp-extended-group-1)# track te 101/2/4 priority 20
```

7. 仮想ルータの IP アドレスを設定するために、'virtual-ip'コマンドを入力します。

```
sw101(config-vrrp-extended-group-1)# virtual-ip 192.53.5.254
```

NOTE

'virtual-ip'コマンドで入力したアドレスは、インタフェース上で設定されている実際の IP アドレスと同じにすることはできません。（VRRP-E のみ）。

8. マスターとして Router 1 を設定するために、デフォルト（100）より高い値にプライオリティを設定します。

```
sw101(config-vrrp-group-1)# priority 110
```

28.8.3 第二の仮想ルータグループのバックアップとして Router 1 の設定

1. R-bridge ID を使用して、'rbridge-id'コマンドを入力します。（'do show vcs'コマンドを実行した

時にどれかがその横にアスタリスクが付いています。）

```
sw101(config)# rbridge-id 101
```

2．Router 1 のための VE インタフェースリンクを設定するために、次のコマンドを入力します。

```
sw101(config-rbridge-id-101)# int ve 10
```

3．Group 2 と呼ばれるグループに Router 1 を割り当てるために、次のコマンドを入力します。

```
sw101(config-Ve-10)# vrrp-extended-group 2
```

4. 20 のトラックプライオリティを使用して、インタフェース ve 10 のトラッキングポートとして、tengigabitethernet ポート 101/2/4 を設定するには、次のコマンドを入力します。

```
sw101(config-vrrp-extended-group-2)# track te 101/2/4 priority 20
```

5．仮想ルータの IP アドレスを設定するために、'virtual-ip'コマンドを使用します。

```
sw101(config-vrrp-extended-group-2)# virtual-ip 192.53.5.253
```

NOTE

'virtual-ip'コマンドで入力したアドレスは、インタフェース上で設定されている実際の IP アドレスと同じにすることはできません。（VRRP-E のみ）。

28.8.4 最初の仮想ルータグループのバックアップとして Router 2 の設定

VCS が有効になっていることを確認して、次に、これらの手順を実行します。

1．R-bridge ID を使用して、'rbridge-id'コマンドを入力します。（'do show vcs'コマンドを実行した時にどれかがその横にアスタリスクが付いています。）

```
sw102(config)# rbridge-id 102
```

2．全体に VRRP-E プロトコルを設定するには、次のコマンドを入力します。

```
sw102(config-rbridge-id-102)# protocol vrrp
```

3．Router 2 のための VE インタフェースリンクを設定するために、次のコマンドを入力します。

```
sw102(config-rbridge-id-102)# int ve 10
```

4．Router 2 のための VE のリンクの IP アドレスを設定するために、次のコマンドを入力します。

```
sw102(conf-Ve-15)# ip address 192.53.5.3/24
```

5．Group 1 と呼ばれる VRRP-E グループに Router 2 を割り当てるために、次のコマンドを入力します。

```
sw102(conf-Ve-15)# vrrp-extended-group 1
```

6．20 のトラックプライオリティを使用して、インタフェース ve15 のためのトラッキングポートとして、tengigabitethernet ポート 102/3/2 を設定するには、次のコマンドを入力します。

```
sw102(config-vrrp-extended-group-1)# track te 102/3/2 priority 20
```

7．仮想ルータの IP アドレスを設定するために、'virtual-ip'コマンドを入力します。

```
sw102(config-vrrp-extended-group-1)# virtual-ip 192.53.5.252
```

NOTE

'virtual-ip'コマンドで入力したアドレスは、インタフェース上で設定されている実際の IP アドレスと同じにすることはできません。（VRRP-E のみ）。

28.8.5 第二の仮想ルータグループのマスターとして Router 2 の設定

1．R-bridge ID を使用して、'rbridge-id'コマンドを入力します。（'do show vcs'コマンドを実行した時にどれかがその横にアスタリスクが付いています。）

```
sw102(config)# rbridge-id 102
```

2．Router 2 のための VE インタフェースリンクを設定するために、次のコマンドを入力します。

```
sw102(config-rbridge-id-102)# int ve 15
```

3．Group 2 と呼ばれる VRRP-E グループに Router 2 を割り当てるために、次のコマンドを入力します。

```
sw102(conf-Ve-15)# vrrp-extended-group 2
```

4．20 のトラックプライオリティを使用して、インタフェース ve15 のためのトラッキングポートとして、tengigabitethernet ポート 102/3/2 を設定するには、次のコマンドを入力します。

```
sw102(config-vrrp-extended-group-2)# track te 102/3/2 priority 20
```

5．仮想ルータの IP アドレスを設定するために、'virtual-ip'コマンドを入力します。

```
sw102(config-vrrp-extended-group-2)# virtual-ip 192.53.5.251
```

NOTE

'virtual-ip'コマンドで入力したアドレスは、インタフェース上で設定されている実際の IP アドレスと同じにすることはできません。（VRRP-E のみ）。

6．マスターとして Router 2 を設定するには、デフォルト（100）よりも高い値にプライオリティを設定します。

```
sw102(config-vrrp-extended-group-2)# priority 110
```

29 IGMP の設定

29.1 IGMP の概要

VLAN の定義されたレイヤ２スイッチを介したマルチキャストコントロールパケットとデータ転送は、VLAN に所属する全てのポートで受信したマルチキャストパケットのレイヤ２転送により、最も容易に実現されます。しかし、この単純なアプローチは帯域的に効率的ではありません。メンバポートの一部だけがマルチキャストパケットの受信に関連するデバイスに接続されているわけでないからです。最悪のシナリオは、一つの VLAN メンバだけが受信データに関連している場合でも、データは多くのメンバーポートを備えた VLAN の全てのポート(例えば 24 ポート全て)に転送されてしまいます。そのようなシナリオでは、高いレートのマルチキャストデータトラフィックを受けるスイッチのスループット損失に至る場合があります。
Internet Group Management Protocol (IGMP) snooping は、VLAN のポートに無駄にマルチキャストを転送する問題を効果的に解決することが出来るレイヤ２スイッチによるメカニズムです。
Snooping は、受信した Join/Leave という IGMP 制御パケットから、VLAN に属するポートでのマルチキャストデータトラフィックの転送状態を学習することを意味します。レイヤ２スイッチはまた、CLI により静的に転送状態を設定する方法も持っています。

NOTE
Network OS 3.0.0 は、IGMPv1/v2 スヌーピングをサポートしています。Network OS 3.0.0 は、レイヤ 3 IGMP 機能をサポートしていません。

29.1.1 アクティブ IGMP snooping

IGMP snooping は、フィルタリングなしで IGMP トラフィックを単純に監視するので、通常は受動的な機能です。しかし、アクティブ IGMP snooping は、マルチキャストルーター上の負荷を低減するために、積極的に IGMP パケットをフィルタします。アップストリームトラフィックは、最小限の情報量だけを送信するためにフィルタされます。スイッチは、ダウンストリームでアクティブなリスナーの数を気にすることなく、ルータが VLAN に対して一つだけのエントリを持つことを保証します。
アクティブ IGMP snooping では、ルーターが VLAN の最近のメンバについて知っているだけです。もし、VLAN に２つのアクティブなリスナーがあって、オリジナルのメンバーが VLAN から離脱すると、スイッチはルーターの VLAN ステータスを変更無しのままとするので、この情報を必要ではないと判断します。次にルーターから、型通りの問合せがありますが、スイッチはアクティブなリスナーがいないことを想定することを避けるために残りのホストからの応答を転送します。

29.1.2 Multicast ルーティング

マルチキャストルーターは、接続された各物理ネットワーク上のメンバのグループを学習するために IGMP を使います。マルチキャストルーターは、接続されたそれぞれのネットワークのマルチキャスト

グループメンバのリストと各メンバーのタイマーを保持します。

NOTE
“マルチキャストグループメンバー”は、利用可能な接続されたネットワーク上のマルチキャストグループのメンバーが少なくともーつあることを意味します。

ホストがマルチキャストルーティンググループに参加するには２つの方法があります。

- 要求されていない IGMP join リクエストを送信する
- マルチキャストルーターからの一般的な問合せに対する応答として IGMP join リクエストを送信する

リクエストの応答では、スイッチはその VLAN に対してレイヤ２フォワーディングテーブルにエントリを作成します。その他のホストが同じマルチキャストに対して join リクエストを送信すると、スイッチは存在するテーブルエントリにそれらを追加します。一つのエントリだけが、各マルチキャストグループに対してレイヤ２フォワーディングテーブル上に VLAN 毎に生成されます。
IGMP snooping は、マルチキャストグループ当たりーつのホスト join メッセージをとマルチキャストルーターにこのメッセージを送ることを除いて、全てを抑止します。スイッチは、指定されたマルチキャストグループ宛のマルチキャストトラフィックを、join メッセージを受信したインタフェースへ転送します。

29.1.3 vLAG および LAG プライマリポート

vLAG および LAG の現在の DCE の実装では、いわゆるプライマリポートの概念を持っています。vLAG および LAG のメンバポートの 1 つがプライマリポートとなり、LAG または VLAG から出力するすべてのマルチキャストトラフィックは、プライマリポートで送信されます。したがって、通常のハッシュベースのフォワーディングは、マルチキャストトラフィックでは実行されず、トラフィックやデータを制御します。図 29-1 に示すように、rbridge R1 が Po10 のグループ G1 で IGMP join リクエストを受信した場合を考えます。これにより、Po10 がグループ G1 のために IGMP レシーバのリストに加えられることになります。次に、vLAG のプライマリポートが R4 と S1 を接続するリンクとなった場合を考えます。このように、元々の Join リクエストは R1 で受信されましたが、何れのマルチキャストトラフィックは、R1 からでなく R4 から vLAG Po10 からグループ G1 の出力となるよう、クラスタでは受信されます。

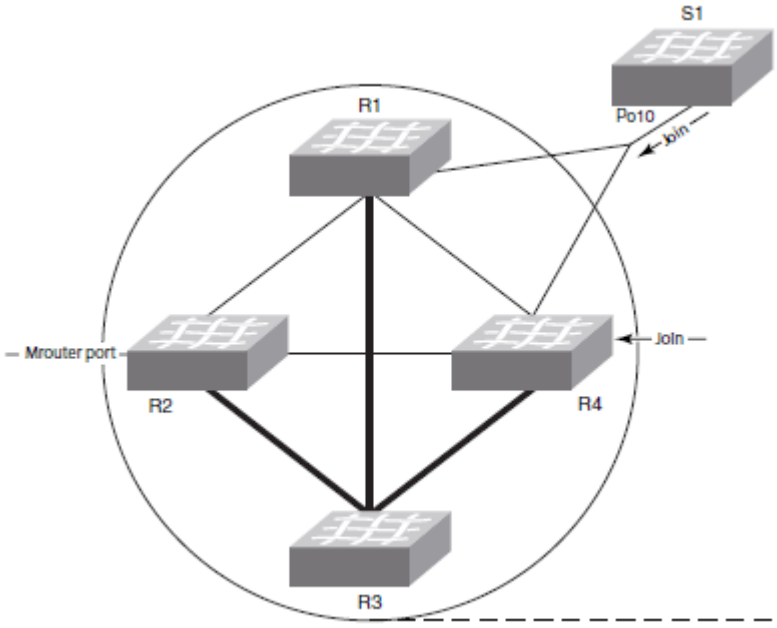

図 29-1 Brocade VCS ファブリックモードの IGMP スヌーピング

vLAG プライマリポートが変わった場合、例えば図 29-1 の R4 と S1 の間のリンクがダウンした場合、マルチキャストトラフィックは vLAG 上の新しいプライマリポートから出します。上記のケースでは、新しいプライマリポートは、R1 と S1 を接続するリンクとなります。

29.2 IGMP snooping の構成

デフォルトでは、IGMP snooping は全ての VLAN インタフェースで無効です。このセクションでのコマンドに関する完全な情報は、『Network OS Command Reference』を参照下さい。
内蔵 DCB スイッチでの IGMP を設定するため次の手順を使います。

1. グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2. 全てのインタフェースで IGMP を有効化するため、'ip igmp snooping enable'コマンドを入力します。このコマンドは、IGMP snooping が全てのインタフェースで有効であることを保証します。

   ```
   switch(config)# ip igmp snooping enable
   ```
3. VLAN インタフェース番号を選択するため、'interface'コマンドを入力します。

   ```
   switch(config)# interface vlan 10
   ```
4. VLAN に対するデフォルト IGMP クエリヤー機能を活性化します

   ```
   switch(config-vlan-10)# ip igmp snooping querier enable
   ```
5. オプション：追加機能と共に IGMP クエリヤー機能を活性化します。

29.3 IGMP snooping クエリヤーの設定

マルチキャストトラフィックが、Protocol-Independent Multicast (PIM)や IGMP が定義されていないた

め、中継されないなら VLAN に IGMP snooping クエリヤーを使います。
IGMP snooping クエリヤーは、IP マルチキャストトラフィックを受信しようとするスイッチからの IGMP レスポンスの契機となる IGMP クエリーを送信します。IGMP snooping は、適切な転送アドレスをマップするため、これらのレスポンスをリッスンします。
このセクションのコマンドに関する完全な情報は『Network OS Command Reference』を参照下さい。
IGMP snooping クエリヤーを設定するため、次の手順を使います。

1. グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2. VLAN インタフェース番号を選択するために、'interface'コマンドを入力します。

```
switch(config)# interface vlan 25
```

3. VLAN の IGMP クエリヤー機能を活性化します。値の範囲は、1 から 18000 秒の範囲で指定できます。デフォルトは、125 秒です。

```
switch(config-vlan-25)# ip igmp query-interval 125
```

4. 最後のメンバクエリー間隔を設定します。値の範囲は、1000 から 25500 ミリ秒です。デフォルトは 1000 ミリ秒です。

```
switch(config-vlan-25)# ip igmp last-member-query-interval 1000
```

5. Max Response Time(MRT)を設定します。1 から 25 秒までが指定可能です。デフォルトは 10 秒です。

```
switch(config-vlan-25)# ip igmp query-max-response-time 10
```

6. VLAN に対する IGMP クエリヤー機能を活性化します。

```
switch(config-vlan-25)# ip igmp snooping querier enable
```

29.4 IGMP の監視

IGMP トラフィックの性能監視により、スイッチ上の潜在的な問題も診断することが可能となります。これは、マルチキャストをリクエストしているホストにだけ IP マルチキャストトラフィックを転送するよう設定することで、より効果的に帯域を利用することを助けます。
このセクションのコマンドに関する完全な情報は『Network OS Command Reference』を参照下さい。
IGMP snooping を監視するため、次の手順を使います。

1. グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2. IGMP マルチキャストグループの全ての情報を表示するため、'show ip igmp groups'コマンドを入力します。全てのインタフェースや特定のインタフェースの全てのグループまた特定インタフェースの特定グループの設定されたエントリを含む全てのグループの IGMP データベースを表示するため、このコマンドを使います。

```
switch# show ip igmp groups
```

3. VLAN やインタフェースの IGMP 統計情報を表示するため、'show ip igmp statistics'コマンドを使用します。

```
switch# show ip igmp snooping statistics interface vlan 1
```

4. 全ての VLAN や特定の VLAN のマルチキャストルーター(mrouter)ポートに関連する情報を表示するため、'show ip igmp mrouter'コマンドを使用します。

```
switch# show ip igmp snooping mrouter
- or -
switch# show ip igmp snooping mrouter interface vlan 10
```

5. IGMP 統計情報を見直す時は、必要なコレクションを作成するため、306 ページの『29.2 IGMP snooping の構成』または 306 ページの『29.3 IGMP snooping クエリヤーの設定』を参照下さい。

NOTE

IGMP CLI コマンドの追加の情報は、『Network OS Command Reference』を参照下さい。

29.5 IGMP スケーラビリティ

このセクションでは、スイッチ操作のさまざまなモードで Network OS のための IGMP Snooping 機能のスケーラビリティの限界と、スケーラビリティの限界を説明する際に関与するさまざまな測定基準を説明しています。

IGMP の測定基準値は次のとおりです。

- サポートされる IGMP グループの最大数－この測定基準値は、利用できるハードウェア資源（例えば、MGID、構成リプレイおよび eNS 配布帯域幅）に基づいて計算されます。
- IGMP Snooping 構成でサポートされる VLAN の最大数－この測定基準は、スイッチ上で実行されている IGMP のソフトウェアプロセス、eNS 分布幅の一般的なクエリーパケットの生成容量の数によって制限されます。
- スイッチ当たりの最大 IGMP パケット処理速度－この測定基準によって記述されるスケーラビリティ番号は、スイッチで実行している IGMP ソフトウェアプロセスで処理できるパケット数の上限を示唆しています。パケットが複数のポート/ VLAN からの着信であれば、同じ処理帯域幅は共有されます。
- Brocade VCS ファブリッククラスタ当たり最大 IGMP パケット処理速度－この測定基準は、論理的 Brocade VCS ファブリックスイッチに着信する最大 IGMP パケットレートの上限を指定します。それは、Brocade VCS ファブリッククラスタ内のノード数の eNS 配布帯域幅によって制限されます。

29.5.1 スタンドアローンモード

スタンドアロンモードでは、孤立したボックスとして VDX スイッチ機能は、おそらく、TOR スイッチとして接続されます。表 34-1 は、測定基準レベルを記述します。

表 29-1 スタンドアロンモードの測定基準

測定基準	境界	コメント
サポートされる IGMP グループの最大数	2000	Join リクエストは、同じスイッチの 4 つのポートで送信されます。
IGMP 構成でサポートされる VLAN の最大数	128	
スイッチ毎の最大 IGMP パケット処理速度	512 パケット／秒	

29.5.2 Brocade VCS ファブリッククラスタモード

データセンターでフラットレイヤ 2 ネットワークをサポートする場合は、VDX スイッチがクラスタを形成するために、任意の順序で接続することができます。クラスタに含まれるノードの数は、4 つのノードから 24 ノードの範囲です。表 29-2 と表 29-3 は、測定基準レベルを記述します。

表 29-2　4 ノードクラスタの測定基準

測定基準	境界	コメント
サポートされる IGMP グループの最大数	2000	Join リクエストは、同じスイッチの 4 つのポートで送信されます。
IGMP 構成でサポートされる VLAN の最大数	128	
スイッチ毎の最大 IGMP パケット処理速度	512 パケット／秒	
Brocade VCS ファブリッククラスタ当たり最大 IGMP パケット処理速度	512 パケット／秒	

表 29-3　20 ノードクラスタの測定基準

測定基準	境界	コメント
サポートされる IGMP グループの最大数	2000	Join リクエストは、同じスイッチの 4 つのポートで送信されます。
IGMP 構成でサポートされる VLAN の最大数	128	
スイッチ毎の最大 IGMP パケット処理速度	512 パケット／秒	
Brocade VCS ファブリッククラスタ当たり最大 IGMP パケット処理速度	512 パケット／秒	

30 トラブルシュート

30.1 トラブルシュート概要

この章は、内蔵 DCBSW を使用中に発生するかもしれない問題を解決する秘訣や手順を提供しています。また、共通のトラブルシュートツールを幾つか紹介しています。

30.2 問題解決情報の収集

次の情報は、保守員・ベンダーに問合せする際、問題の調査・解決に役に立つ情報です

- ネットワーク構成図と接続情報
- 問題に至った手順や事象の記録
- 事象発生時に動作していたアプリケーション、管理用エージェントやスクリプトのリスト
- 内蔵 DCBSW のログファイル(supportsave)
- もし SFP トランシーバに関連した問題であれば'show media'コマンドの出力結果
- お客様自身でトラブルシュートのために実行したコマンドの出力結果
- Wireshark やその他アナライザを使ってキャプチャしたネットワークトレース情報
- もし TACACS に関連した問題であれば、TACACS サーバのバージョン情報

30.2.1 supportsave データの採取

'copy support'コマンドは、診断コマンドを実行するだけでなく、core dump、トレースやその他関連データを採取します。同じ操作で、コマンドは全てのこれらの情報をリモートホストへコピーします。一度リモートホストにコピーすると、ベンダでの障害解析を進めることが出来ます。
supportsave を採取するために、次の手順を実行してください。

1．スイッチにログインする。
2．特権実行モードで、supportsave を採取するために'copy support'コマンドを入力します。
'copy support'コマンドは、FTP または SCP を使って supportsave をリモートサーバにコピーするオプションを持っています。単一のコマンドラインまたは、対話モードでコマンドを実行することが出来ます。
次の例は、FTP を使ってリモートサーバへコピーするために単一のコマンドラインモードで supportsave を実行しています。

```
switch# copy support ftp host 10.38.33.131 user admin directory 108
Password: *****
```

次の例は、FTP を使った対話モードの例です。

```
switch# copy support-interactive
Server Name or IP Address: 10.38.33.131
Protocol (ftp, scp): ftp
```

```
User: admin
Password: *****
Directory:/home/admin/support
VCS support [y/n]? (y): y
```

30.2.2 トラブルシュートのアプローチ

このセクションでは、トラブルシュート方法の概要を述べます。

1．スイッチが全ての必要なライセンスをインストール済みかチェックします。

- ライセンスには、VCS Fabric license や FCoE license があります。
- ライセンスタイプは、VCS Fabric(３つ以上のノード用のライセンス)や FCoE です。
- VCS Fabric ライセンスは、２つ以下の VCS ファブリッククラスタでは必要ありません。
- FCoE ライセンスは、インストールされた VCS ファブリックモードが有効でなければなりません。
- FCoE が追加・変更された後は、ライセンスを有効にするためスイッチをリブートします。

2．転送が行われるようトポロジやスイッチの設定を確認します。

3．'copy support'コマンドを入力します。

4．障害の手がかりや切っ掛けを探すため、例えば'show logging raslog'などの参照コマンドを実行します。

5．様々なリソースの利用率をチェックします。

ａ．CPU の使用状況を知るために、'show process cpu'コマンドを入力します。

ｂ．メモリの利用状況を知るために、'show process me'コマンドを入力します。

ｃ．使用されている MAC アドレスの数を知るために、'show mac-address-table count'コマンドを入力します。

ｄ．ルートの数を知るために、'show fabric route topology'コマンドを入力します。

ｅ．VCS ファブリックノードの数を知るために、'show fabric all'コマンドを入力します。

ｆ．光モジュールの問題を調査するために、'show media'コマンドを入力します。

6．データパスファブリックの継続試験を実施します。

ａ．エンドステーションまたはデバイスから、エンドステーションまたはデバイスへの ping 実行

ｂ．もしパケットがエラー受信または破棄されるなら、'show interface'コマンド出力のカウンターをチェックする

ｃ．使用されている光モジュールが Brocade 製か確認する。'show media'コマンドを入力し Vender name フィールドに"Broacde"が表示されているか確認する。また、Tx Power フィールドと Rx Power フィールドがゼロではないことをチェックする。

ｄ．MAX アドレステーブルが MAC アドレスを学習しているか確認する

ｅ．もしスイッチがＶＣＳファブリッククラスターの一部なら、MAC アドレステーブルがクラスタ内の全てのスイッチにわたって正しく同期されているか確認する。

ｆ．LLDP が隣接スイッチを報告しているか確認する

ｇ．MAC アドレステーブルが他の VCS ファブリックスイッチから学習された MAC アドレスを通

知することを保証することにより Ethernet Name Server(ENS)の機能をチェックする

h. データパスファブリックの接続性を確認するため'l2traceroute'コマンドを使用する。このコマンドは、パケットがファブリック内のどこで破棄されたかを特定することを手助けします。コマンドは、幾つかの基本的なパラメータ入力と拡張パラメータを入力することが出来ます。

現在、サポートしている基本的なパラメータは下記です。
・動的に学習された MAC アドレスの Source Address (SA)と Destination Address (DA)
・VLAN
・Edge routing bridge ID

現在、サポートしている拡張パラメータは下記です。
・プロトコルタイプ(IP)
・ソースと宛先 IP アドレス
・IP プロトコルタイプ(TCP 推奨)
・ソースと宛先ポート番号
IP パラメータの目的は、特定の ECMP 接続を通る'traceroute'パケットを作るためです。

CAUTION
次に示す手順は、コンフィグレーションに影響があるので、注意して使用する必要があります。

7. ファブリック内の流れを追跡するため、許可 ACL を使ってカウンタの増分を観測します

30.3 トラブルシュートのホットスポットを理解する

このセクションは関連する背景説明と問題が報告される Network OS の機能に関連するベスト・プラクティス・ガイダンスを行います。このガイダンスに沿って、多くの可能性がある問題を回避することが出来るはずです。

30.3.1 ライセンス

ライセンスされた機能が働かない時、可能性の高い原因の一つとして、ライセンスが正しくインストールされていないことがあります。機能が正当にライセンスされて正しくインストールされるように 81 ページの『7 ライセンスの管理』に示すガイドラインと手順に従ってください。
ライセンスの回復手順は、330 ページの『30.4.7 ライセンスが正しくインストールされない』を参照下さい。

30.3.2 他社スイッチとの STP 接続性

・ Juniper や Cisco などの他社スイッチとの間でスパニングツリープロトコル(STP)を使用するため、共用スパニングツリーMAC アドレス(0100.0ccc.cccd)に BPDU を送信するためインタフェースを設定する必要があります。この設定がないと、RPVST/PVST のルートブリッジが VLAN1 を含む全ての VLAN を認識しません。

```
switch(conf-if-te-0/1)# spanning-tree bpdu-mac 0100.0ccc.cccd
```

INFORMATION
本設定は、工場出荷時のデフォルトコンフィグで有効になっています。

・ もし内蔵 DCBSW が tagged ポートを設定した VLAN が定義されていて、各 VLAN(PVST)上で Rapid Spanning Tree Protocol(RSTP)が有効ならば、VLAN に所属するポートに pvst-mode が定義されていなければ、tagged ポートで受信した BPDU は破棄されます。
次の例は、tagged ポートと VLAN 上で RSTP を有効化する設定例です。

```
vlan 2
tagged ethe 1/24 ethe 2/1 to 2/2
router-interface ve 2
rstp priority 100
```

もし条件が一致すれば、tag 付 BPDU がスイッチを通過するように設定され全てのポートは pvst-mode になるはずです。もし、pvst-mode が有効でない場合は、次の手順で有効化してください。

```
Brocade(config)# interface ethernet 2/1
Brocade(config-if-2/1)# pvst-mode
```

30.3.3 負荷分散配信

負荷分散に関する問題を理解するために、負荷分散アルゴリズムにより使用される条件の基本的な知識をもつ必要があります。表 30-1 は、負荷分散を提供する各機能の詳細を示しています。

表 30-1 負荷分散アルゴリズム

機能	アルゴリズム
ECMP IP	パスは次のパラメータから導出されたハッシュに基づいて選択されています： ・送信元 MAC アドレス ・宛先 MAC アドレス ・VID ・IP プロトコル ・送信元 IP アドレス ・宛先 IP アドレス ・レイヤ 4 送信元ポート ・レイヤ 4 宛先ポート 'fabric-ecm load-balance'および'fabric-ecmp load-balance-hash-swap'コマンドを使用してハッシュフィールドを設定できます。 関連の回復手順については、325 ページの 『30.4.4 期待通り ECMP が負荷分散しない』を参照してください。
LACP	フィールドがフレームで利用可能であるかに応じて、最大 7 つの基準に基づく適応可能な負荷分散を提供します。
Brocade trunk	メンバリンクの間で、均等パケット負荷分散（ラウンドロビン）を提供します。

30.3.4 routing bridge ID の静的割当

routing bridge ID の重複は、イーサファブリックにスイッチを組み込む際にエラーの一般的な原因とな

ります。イーサファブリックにスイッチを追加する前に、ユニークな routing bridge ID を割り当てなければなりません。もし、新しいスイッチが既存の VCS ファブリッククラスタに追加される場合は、クラスタ内の他のスイッチと同じ VCS ID を割り当てなければなりません。一旦スイッチが追加されると、principal routing bridge は新しいスイッチを含む制御プレーンでネゴシエーションを実行しファブリックを再構築します。データプレーンは影響を受けません。
routing bridge ID の重複から回復する手順はページの『"Routing bridge ID is duplicated"』に記載しています。

30.3.5 FSPF 経路変更

Fabric Shortest Path First (FSPF)アルゴリズムは新たな経路を選択し、一時的なトラフィックの中断を発生させます。これは、古い経路が最初途切れて新しい経路が作成されるので通常の振る舞いです。このような経路変更は、FSPF が新しい最短ルートを構築する時もしくは、現在の経路がダウンした際に発生します。

30.3.6 VCS Fabric モードと standalone モード

standalone モードと VCS Fabric モードでトラブルシュートの際注意すべき重要な違いが存在します。デフォルトで standalone モードはインタフェースが無効、VCS Fabric モードではインタフェースが有効となっています。デフォルトコンフィグレーションが適用された場合、この点を考慮してください。

INFORMATION
工場出荷時の設定では、standalone モードでインタフェースは有効になっています。ここでのデフォルトは、standalone モード/VCS Fabric モードを切替えた直後の状態となります。

インタフェースは、standalone モード/VCS Fabric モードでレイヤ２スイッチポートとして設定できます。
VCS Fabric モードと standalone モード間の切り替えや元のモードへの切替は、コンフィグレーションの消失やデフォルトコンフィグレーションを使った再起動となります。
port-profile ポートはレイヤ２ポートにのみ割当可能です。
管理ポートを介したアウトバンド管理は、デフォルトゲートウェイを設定されるようにします。

30.3.7 vLAG

vLAG の問題をトラブルシュートする前に、vLAG 機能の次の要点に気をつけてください。

- vLAG 上のマルチキャスト(BUM)トラフィック
- エッジポートの要件
- フェイルオーバー

(1) vLAG 上のマルチキャストトラフィック
フラッディングはいつも vLAG のプライマリリンクを通過します。トラフィックの帯域を設計する際この制限を考慮しなければなりません。このリンクは、'show port-channel'コマンドの出力結果であり、アスタリスク(*)で示されます。

```
switch# show port-channel 38
```

```
LACP Aggregator: Po 38
Aggregator type: Standard
Admin Key: 0038 -Oper Key 0038
Partner System ID -0x8000,01-e0-52-00-20-00
Partner Oper Key 0038
Member ports:
Link: Te 0/13 (0x180D0102) sync: 1
Link: Te 0/14 (0x180E0103) sync: 1 *
```

(2) vLAG に対するエッジポート要件

LACP はエッジポートに於いては、”Brocade”または”Standard type”の何れかのみと設定することが出来ます。もし、”Brocade”を選択した場合、リンクリセット(LR)プリミティブが正しく交換するために、エッジの接続先が Brocade Converged Network Adapter(CNA)か standalone モードの Brocade VDX スイッチか Brocade 8000 であるかを確認してください。

(3) フェイルオーバーと vLAG

高速なフェイルオーバーのために、‘vlag ignore-split’コマンドを使用することを推奨します。これにより１秒以下の切り替えを可能とします。このコマンドは Network OS 3.0 にアップグレードする時や Network OS 3.0 で新たな port-channel を追加すると、自動的に全ての port-channel に設定されます。この機能を使用する場合、vLAG メンバが互いに切り離してしまう「スプリット・ブレイン」問題を回避するために注意を払ってください。vLAG メンバ間を物理的に分離された複数の経路でスイッチ接続(ISL)することを推奨します。

次のトピックは「スプリット・ブレイン」問題とそれを軽減する方法について述べます。

(a) 「スプリット・ブレイン」を理解する

「スプリット・ブレイン」は、エンド・ホストやエッジスイッチが vLAG(LACP 使用)により２つの別々のクラスタに接続するケースで発生します。エンド・デバイスは、これらの２つのスイッチが LACP で同じシステム ID を広告するので一つのスイッチのように見えます。

レアケースですが、２つのクラスタスイッチ間の全ての ISL が切断されて、クラスタスイッチが LACP パートナーに同じシステム ID を広告し続けます。これにより、「ファブリックの分離」や「スプリット・ブレイン」状態が発生します。そして、エンド・ホストやエッジスイッチは、このセグメンテーションを検出しないことがあり、両 vLAG スイッチを一つのスイッチとして取り扱うことになります。

この状態は、パケットの複製や想定外のパケット喪失となります。

(b) スプリット・ブレイン状態での Network OS のトラフィック防止

デフォルトで、Network OS は「スプリット・ブレイン」問題から回復する機能を持っています。全てのクラスタスイッチ間の ISL がダウンした時、より低いルーティングブリッジ ID を持つスイッチが port-channel からセグメント化されたことをエッジスイッチパートナーに伝えるため

LACP を使います。それは、広告されるシステム ID を変更することにより行われます。エッジスイッチがメンバの一つから異なるシステム ID を学習する時、その port-channel からこのメンバを削除します。そして、より高いルーティングブリッジ ID をもつ一つの vLAG メンバスイッチとだけ動作し続けます。他の vLAG メンバスイッチは、以前リンクアップしていますが、もともとの port-channel(sync:0)からセグメント化されたままとなります。この機能で、「スプリット・ブレイン」に起因するパケットの複製やパケット破棄の可能性を回避します。

(c) メンバスイッチがリロードされた場合

より低いルーティングブリッジ ID をもったスイッチのリロードは何にも影響がありません。

より高いルーティングブリッジ ID を持ったスイッチがリロードされると、他の vLAG メンバは全ての ISL がダウンしたと認識します。これは、本当の「スプリット・ブレイン」ではありませんが、より低いルーティングブリッジ ID を持ったスイッチは区別することができず、変更されたシステム ID をパートナーに通知することになります。
パートナーエッジスイッチは２つのイベントと認識するでしょう。

- あるリンク変更でのシステム ID
- 他のインタフェースのダウン

このケースでは、LACP は再ネゴシエーションして port-channnel を再構築します。その間、port-channel はバタついて、一時的にトラフィックに影響を与えます。スイッチが起動しファブリックに再度参加する場合に同様の影響が発生します。

このように、もしより高いルーティングブリッジ ID を持ったスイッチが再起動すると、一時的にトラフィックを妨害することになる port-channel のバタつきが起こります。低いルーティングブリッジ ID を持ったスイッチがリロードする時には影響がないことに注意してください。

(d) スイッチリロード中のトラフィック影響の防止

Network OS の動作するスイッチは、論理 port-channel に対して設定できる特別な‘vlag ignore-split’オプションを持っており、ユーザに柔軟性を提供します。このオプションは両方の vLAG メンバポートに設定しなければなりません。

このオプションを設定することは、低いルーティングブリッジ ID を持ったスイッチのシステム ID の変更を防止することが出来ます。そして、両方のスイッチが同じシステム ID を広告し続けます。この動作は、スイッチの一つがリロードされてトラフィックが操作される時に、対向エッジスイッチの変更を検出することを防止します。

(e) ‘vlag ignore-split’オプションを使用する

‘vlag ignore-split’オプションを使用するために、全ての ISL が同時にダウンするような状況を回

避するために、ISL 周辺に冗長性をもたせる必要があります。全ての接続が同時にダウンする可能性を取り除くために、物理的に分離された複数経路の ISL を使用することを推奨します。

30.3.8 Principal ルーティングブリッジの可用性

もし新しい Principal ルーティングブリッジが動作中の VCS ファブリッククラスタに導入、もしくは、Principal ルーティングスイッチが失われることにより新しいスイッチが選出されることになると、ファブリックのコントロールプレーンは再構築され、データプレーンは混乱無くトラフィックの転送を継続します。VCS ファブリックでの Principal RBridge の初期の役割は、次の通りです。

- ルーティングブリッジ ID の配分
- 仮想管理 IP アドレスの所有
- 構成データベースの同期維持

30.3.9 Brocade トランク

Brocade トランクは、ISL 使用時に動作する唯一のアグリゲーション方法です。
Brocade ISL トランクは、対向スイッチとの間でラインリセット(LR)プリミティブを使って自動的に形成されます。
同一の隣接 Brocade スイッチに接続された全ての ISL ポートはトランクを形成しようとします。トランクの形成に成功するために、スイッチ上の全てのポートは、同じスピードに設定されなければなりません。トランクはデフォルトで有効です。
Brocade トランクは 1G リンクではサポートされません。
Brocade スイッチ間の Brocade トランクの利点を活用するため、少なくとも２つのメンバと複数の ECMP パスを持つことを推奨します。それはまた不慮の切断に備えて接続性を確保するため物理的に分離されたケーブルで経路を確保することも推奨します。

30.3.10 vLAG と NIC チーミング

NIC チーミングは、サーバとスイッチ間リンクのアグリゲーションを可能とします。NIC チーミングは、active/passive モデルか active/active モデルのいずれかです。いずれの場合も、スイッチに必要な設定については、NIC チーミング機能の使用条件に合わせる必要があります。『LAN 拡張機能設定手順書』を参照して、スイッチ側の設定を行ってください。

30.3.11 MTU の選択

通常、スイッチにはホストの最大 MTU+100 バイトを設定します。MTU の定義が時々ベンダの解釈により異なることがあるので、この方法が推奨されます。もし、スイッチの MTU が接続された MTU と同じであれば、パケットがドロップするかもしれません。

30.3.12 オーバーサブスクリプションの回避

ある輻輳条件の下、’ show qos rcv-queue interface’コマンドの出力にある“tail-drops”を意味する‘ packets dropped’が増加するかを観測してください。

```
switch# show qos rcv-queue interface tengigabitethernet 5/0/1
Interface TenGigabitEthernet TenGigabitEthernet 5/0/1
  In-use 0 bytes, Total buffer 144144 bytes
  0 packets dropped
           In-use         Max
  CoS      Bytes          Bytes
  -------------------------
  0           0           18018
  1           0           18018
  2           0           18018
  3           0           18018
  4           0           18018
  5           0           18018
  6           0           18018
  7           0           18018
```

この状況では、まずボトルネックを特定して輻輳状態を軽減するアクションを採らなければなりません。

(1) 輻輳のボトルネックを特定する
ボトルネックを特定するために、様々な箇所で'show interface'コマンドを入力します。そして、TX 及び RX の破棄が増加しているインタフェースを特定します。TX または RX の破棄に依存して、輻輳は下流のどこかで発生しているはずです。

(2) 輻輳の軽減
輻輳を軽減するために次のアクションを試してください。

- ボトルネックとなる帯域の増加
  - LAG や ECMP パスへの接続数の追加
  - 更に高速なインタフェースの使用
- ボトルネック箇所や隣接デバイスへのフロー制御設定
- QoS の設定
  - クリティカルトラフィックへの分類、マーキング、優先設定
  - スケジューリングの変更。SP または DWRR の効果を検討・比較してください。

フロー制御を有効化するには、サーバなどのエンドステーションからのトラフィックを受信するポートと接続しているエンドデバイス自身に、それぞれ設定してください。port-channel の場合の設定例を次に示します。

```
switch(conf-if-te-1/0/24)# interface port-channel 100
switch(config-Port-channel-100)# qos flowcontrol tx on rx on
```

一度フロー制御が有効化して、再度’show qos rcv-queue interface’コマンドを入力して、出力をチェックしてください。’packet drops’は見られなくなっているはずです。もし、’packet drops’が継続しているか受信レートが期待より低い場合は、更なる調査のため保守員またはサポート窓口に問合せ下さい。フロー制御は非対称に設定することを推奨します。任意の隣接する２つのデバイスに対して、一報のデバイスは Rx:ON で Tx:OFF、もう一方は Rx:OFF で Tx:ON です。
輻輳制御については、ページの"Congestion control and queuing"を参照してください。

30.3.13　　ACL の制限事項

もし、表 30-4 に示す ACL 使用時の制限事項を守っているなら、システム制限に遭遇することは殆どありません。ACL は迅速かつ正確にインスタンスかする必要があります。

表 30-2　 ACL の制限

機能	制限
標準または拡張 ACL 数は、各々のスイッチのために作成されますが、適用されません。	50
標準または拡張 ACL ごとのルール数	256
ACL が同時に適用される物理インタフェイス数	60（standalone モード） 48（VCS モード）
ACL が同時に適用される VLAN インタフェイス数	100
ACL カウンタ数	252
TCAM テーブルエントリ数	1000
スイッチ当たりの ACL ルール数	6000
適用された共存の標準および拡張 ACL 数	50

加えて、30,720 までの MAC アドレスをサポートしています。
これらの制限の組み合わせに近づいたり越えたりすると、ACL ルールのインスタンス化が遅延したり、プロセス例外が発生したり、MAC 学習問題のために ACL が失敗したりする可能性があります。
もし、ACL や VLAN の数が超過すると、ACL ルールとカウンターのインスタンス化において数分の遅延が発生します。L2SYS プロセスメッセージキューが一杯になるか、プロセス切り替えやスケジューリングが ACL のインスタンス化を遅延させるまで増加します。
‘show statistics access-list mac’コマンドの周期的なモニタリングにより、非ゼロの 252 以上の ACL ルールと正しくインスタンスかされハードウェアカウンタが割り当てられたルールに対する増加するフレームカウントが無いことを示します。
プロセス例外は、ACL の組合せが限界に近づくか超過した場合、時々L2YSD プロセスで発生します。一定の MAC 学習や破棄は、チップ内のテーブル限界が超過した場合に発生します。MAC アドレステーブルエントリ数が超過した場合、レイヤ２フレームスイッチングは失敗します。

30.4　トラブルシューティング手順

この章では、遭遇する可能性のある幾つかの問題の説明と、その問題の調査及び解決方法に関して提

案を行っています。もし、これらの手順で問題の解決に至らない場合、ページの"Getting technical help"に記載しているように、サポート窓口や保守員に問合せの準備をしてください。

30.4.1 AMPP が動作しない

Brocade Automatic Migration of Port Profiles (AMPP)を設定するのは複雑です。AMPP は standalone モードと VCS ファブリックモードの何れでも動作します。AMPP の設定に関する詳細は『14 AMPP の設定』を参照下さい。

AMPP を使用する場合に遭遇する問題は、ポートプロファイル自身の定義エラーによることが一般的です。そのエラーは、仮想マシン(VM)との関連付けやホストアダプタと AMPP の互換性問題などがあります。特に、AMPP の問題は、次の条件で発生します。

- ポートプロファイルの定義が対象スイッチ上に無い、または、switchport や VLAN の定義を含んでいない。321 ページの『30.4.1 (1) ポートプロファイルの定義の確認』を参照下さい。
- VM の MAC アドレスが MAC アドレステーブルにない。322 ページの『30.4.1 (2) VM の MAC アドレスの』を参照下さい。
- ポートプロファイルが有効化されない、または正しい MAC アドレスに関連付けされない。322 ページの『30.4.1 (3) ポートプロファイル状態の確認』を参照下さい。
- VM カーネルの MAC アドレスがそれぞれのスイッチのポートプロファイルと正しく関連付けされない。323 ページの『30.4.1 (4) VM カーネルの MAC アドレスの確認』を参照下さい。

- VM とその関連付けたホストが共通のストレージデバイスを共用しない。323 ページの『30.4.1 (5) 共用ストレージデバイスの確認』を参照下さい。
- ポートプロファイルが非プロファイル VLAN で学習される。323 ページの『30.4.1 (6) 学習済みプロファイル MAC アドレスの状態確認』を参照下さい。
- ポートプロファイルが同一インタフェースでコンフリクトしている。323 ページの『30.4.1 (7) ポートプロファイルの競合がないことを確認』を参照下さい。
- イーサネットネームサーバが正しく動作しない。324 ページの『30.4.1 (8) イーサネットネームサーバの確認』を参照下さい。
- ESX ホストがインストールされたネットワークアダプタやドライバと互換性が無い。324 ページの『30.4.1 (9) ESX ホストの確認』を参照下さい。

(1) ポートプロファイルの定義の確認

有効なポートプロファイルは、対象のスイッチ上に存在していなければなりません。そしてポートプロファイルは、基本的な switchport 設定と VLAN 設定が含まれている必要があります。

1．特権実行モードにおいて、対象スイッチ上にポートプロファイルが存在するか、また基本的な switchport 及び VLAN の定義が含まれているか確認するため、'show running-config port-profile' コマンドを入力します。

```
switch# show running-config port-profile
port-profile default
vlan-profile
switchport
switchport mode trunk
switchport trunk allowed vlan all
switchport trunk native-vlan 1
!
!
port-profile pp1
vlan-profile
!
!
port-profile pp2
vlan-profile
!
```

2．もしポートプロファイルの定義が存在してなかったり、必要な switchport や VLAN の定義を忘れている場合は、156 ページの『AMPP ポートプロファイルの構成』の記載に従ってポートプロファイルを作成してください。

(2) VM の MAC アドレスの確認

AMPP を正しく機能させるために、VM に対する MAC アドレスとその関連付けられたホストが、MAC アドレステーブルに登録されていなければなりません。

1．VM の MAC アドレスがスイッチの MAC アドレステーブルに登録されているか確認するため、’show mac-address-table’コマンドを入力します。

```
switch# show mac-address-table
VlanId Mac-address Type State Ports
1 0000.0010.0001 Static Inactive Te 4/0/3
1 0000.0010.0002 Static Inactive Te 4/0/3
Total MAC addresses : 2
```

2．もし、VM の MAC アドレスが存在していない場合は、更に調査するためサポート窓口か保守員に問い合わせて、情報を提供してください。

(3) ポートプロファイル状態の確認

AMPP を正しく機能させるには、ポートプロファイルは有効であり、正しい MAC アドレスに関連付けられている必要があります。

1．ポートプロファイルが有効で正しい MAC アドレスに関連付けられているかを確認するため、’show port-profile status’コマンドを入力します。

```
switch# show port-profile status
Port-Profile PPID Activated Associated MAC Interface
pp1 1 No None None
pp2 2 No None None
```

2．次に示すような設定ミスを修正します。

もし、ポートプロファイルが有効でない場合、有効化するために、’ port-profile [profile-name] activate’コマンドを入力します。

もし、ポートプロファイルが MAC アドレスに関連付けられてない場合は、関連付けするために’ port-profile [port-profile-name] static’コマンドを入力します。

```
switch(config)# port-profile PP3 static 0050.5600.10030
```

もし、ポートプロファイルが誤った MAC アドレスに関連付けられている場合、正しくない MAC アドレスとの関連付けを切るため、’ no port-profile port-profile-name static’コマンドを入力し、それから正しい MAC アドレスに関連付けてください。

```
switch(config)# no port-profile PP3 static 0050.5600.10020
switch(config)# port-profile PP3 static 0050.5600.10030
```

ポートプロファイルの有効化や MAC アドレスへの関連付けの詳細については、158 ページの『14.2.2 新しいポートプロファイルの構成』を参照してください。

(4) VM カーネルの MAC アドレスの確認

VM カーネルの MAC アドレスがそれぞれのスイッチ上にあるポートプロファイルに関連付けられているかを確認します。もし関連付けられていない場合、321 ページの『30.4.1 (1) ポートプロファイルの定義の確認』の記載に従って、関連付けてください。

(5) 共用ストレージデバイスの確認

VM とその関連するホストがストレージデバイスを共用しているか確認します。もし共用されて無い場合は、ストレージデバイスを共用するように VM とホストを再設定してください。

(6) 学習済みプロファイル MAC アドレスの状態確認

AMPP を正しく機能させるために、MAC アドレスは有効なソースであるプロフィアル VLAN から学習される必要があります。この手続きは、MAC アドレスが有効なソースから学習されているかどうかで決定されます。

1．学習済みのプロファイル MAC アドレスの状態をチェックするために、'show mac-address-table port-profile'コマンドを入力します。

```
switch# show mac-address-table port-profile
Legend: Untagged(U), Tagged (T), Not Forwardable(NF) and Conflict(C)
VlanId Mac-address Type State Port-Profile Ports
1 0050.5679.5351 Dynamic Active Profiled(U) Te 111/0/10
1 0050.567b.7030 Dynamic Active Profiled(U) Te 111/0/12
1 005a.8402.0000 Dynamic Active Profiled(T) Te 111/0/24
1 005a.8402.0001 Dynamic Active Profiled(NF) Te 111/0/24
1 005a.8402.0002 Dynamic Active Not Profiled Te 111/0/24
1 005a.8402.0003 Dynamic Active Not Profiled Te 111/0/24
1 005a.8402.0004 Dynamic Active Not Profiled Te 111/0/24
(output truncated)
Total MAC addresses : 17
```

"Not Profiled."と表示される MAC アドレスを確認、調査します。

(7) ポートプロファイルの競合がないことを確認

1．競合無しに複数のポートプロファイルがインタフェースに適用されているかを確認するために、'show port-profile name pp1_name name pp2_name validate'コマンドを入力します。

```
switch# show port-profile name pp1 name pp2 validate
Port-Profile Port-Profile Conflicts

pp1 pp2
vlan-profile vlan-profile No
qos-profile qos-profile No
security-profile security-profile No
```

2．もし競合しているなら、一方のポートプロファイルを再設定します。

共存ルールに関する情報は、153 ページ『14 AMPP の設定』を参照してください。

(8) イーサネットネームサーバの確認

AMPP はクラスタ内の各 VCS ファブリックスイッチが MAC アドレステーブルで同一に見えることが必要です。どのような違いがあっても、イーサネットネームサーバ(ENS)の問題を意味しています。詳細は、325 ページの『30.4.5 ENS の機能チェック』を参照してください。

(9) ESX ホストの確認

各 ESX ホストが適切なドライバとともに正しい Converged Network Adapter (CNA)がインストールされており、Cisco Nexus 1000V 仮想スイッチが使われていないかを確認します。(Cisco Nexus 1000V は、加工された特別なパケットを送信するので動作しません。)

30.4.2 パニックリブートの継続

もしスイッチがパニックリブートを繰り返しているなら、次の手順を実行してください。

1. オリジナルのバイナリを使ってスイッチを安定状態にするか、健全なイメージが格納された別のパーティションに切替えてください。
   a. ブート時に、' setenv OSLoadOptions 2'、' saveenv'、'reset'を実行してください。
   b. パニック前のリブート直後に、ログインしてみて' do chkconfig fabos off'を実行してください。

      これはスイッチを Linux OS のみで Network OS をロードしないシングルユーザモードでブートさせるものです。ファイルシステムに、例えば、'bootenv'を使ってパーティションを切替えるかオリジナルの健全なバイナリに置き換えるというような必要な変更を行ってください。

      シングルユーザモードでは、ネットワークにはアクセスできません。ですので、ネットワークにアクセスするには、'ifconfig eht0'コマンドを使ってください。更に、'init 3'コマンドで上記 a の手順実行後にブートさせます。そうでない場合は、' chkconfig fabos on; reboot'コマンドでリセットしてください。
2. もし、スイッチが５回のリブートの繰返しの後 halt した場合は、次のコマンドで DCMD データベースをクリアしてください。

```
rm -rf /etc/fabos/Dcmd/*.cfg; rm -rf /etc/fabos/Dcmd/WaveDatabase; rm -rf
/etc/fabos/Ccmd/*.cfg; rm -rf /etc/fabos/Ccmd/WaveDatabase; reboot
“/sbin/reboot -f
```

3. スイッチを正常状態に戻すために、健全なイメージをインストールしてください。

30.4.3 不意の CPU 利用率高騰

不意の CPU 利用率高騰は、普通、CPU サイクルを大量に消費するプロセスの結果です。その結果、telnet でのスイッチへのアクセスを妨げたり、ISL を動作させなくします。

もし、CPU 利用率高騰が疑われるなら、次の手順を実行してください。

1．特権実行モードで、どのプロセスが CPU を消費しているかを確認するため’ show process cpu’コマンドを実行してください。
2．対応するインタフェースを shutdown したり、CPU 消費の原因と疑われる設定を削除してください。

30.4.4 期待通り ECMP が負荷分散しない

Equal cost multipath (ECMP)ルーティングは、最適コストで複数経路を通るトラフィックを分散させることによりスループットを増大させます。もし、期待通りトラフィックが分散されていないと疑われる場合、次の手順を実行してください。

1．特権実行モードで、ECMP 経路が期待通りか確認するため、’ show fabric route topology’コマンドを入力してください。

```
switch# show fabric route topology


Total Path Count: 1


Src  Dst  Out  Out          Nbr  Nbr
RB-ID RB-ID Index Interface   Hops Cost Index Interface    BW  Trunk
--------------------------------------------------------------------------------
66   1    124   Fi 66/0/4   1    500   129   Fi 1/-1/-1    32G Yes
```

もし、出力結果がソースとデスティネーションスイッチ間の equal cost path が表示されたら、ECMP の負荷分散は期待通りです。

2.期待されるフロー数になっているかを確認するため､インタフェースの利用率をチェックします。
3．レイヤ2/3/4のフローがそれぞれの ECMP リンクにハッシュされているか調査するため’l2traceroute’コマンドを入力します。
ECMP 固有操作の妨害を避けるため、正しく機能する Brocade ルーティング方針は、一つの決定的な経路に沿って特定のフローを送信します。追加のフローは利用可能なコスト等価のルートを使います。この手順は、このハッシュ方針が正しく機能しているかを確認するものです。

‘l2traceroute’コマンドの使用方法詳細は、348 ページの『30.5.1 Layer 2 traceroute』を参照下さい。

30.4.5 ENS の機能チェック

イーサネットネームサーバ(ENS)は、MAC アドレステーブルの内容が同一 VCS ファブリッククラスタ内のスイッチ間で一致している時、正しく動作しています。ENS が正しく動作しているかを確認するため次のチェックを行ってください。

- ファブリックメンバの情報が期待通りかチェックする。326 ページの『30.4.5 (1) ファブリックの確認』を参照してください。
- MAC アドレスがポート間を移動してないか確認する。326 ページの『30.4.5 (2) ポート間の MAC アドレスの移動をチェック』を参照してください。
- エッジポートが外部ループを持っていないか確認する。326 ページの『30.4.5 (3) エッジポートの外部ループの確認』を参照してください。

(1) ファブリックの確認

‘show fabric all ‘コマンドを入力し、VCS ファブリッククラスタの全てのスイッチに関して情報が表示されるかを確認します。

```
switch# show fabric all


VCS Id: 1
Config Mode: Local-Only


Rbridge-id  WWN                   IP Address       Name
------------------------------------------------------------------------------
 1        50:00:51:E4:44:40:0E:04   0.0.0.0          "fcr_fd_1"
 2        50:00:51:E4:44:50:0F:09   0.0.0.0          "fcr_xd_2_128"
60        10:00:00:05:33:5F:EA:A4   10.24.81.65       "switch"
66        10:00:00:05:33:67:26:78   10.24.81.66      >"switch"
The Fabric has 4 Rbridge(s)
```

(2) ポート間の MAC アドレスの移動をチェック

ポートからポートへの MAC アドレスの移動は、同一のソースアドレスが複数のポートで検出される時発生します。この状態は、“MAC address flapping”として知られています。

MAC address flapping をチェックするため、’ show mac-address-table’コマンドを複数回入力し、出力をチェックします。

(3) エッジポートの外部ループの確認

物理的な外部ループをチェックします。

30.4.6 ISL が動作しない

VCS ファブリッククラスタ内の２つのスイッチ間の接続(ISL)の失敗には、様々な理由があります。

- ISL 設定が無効になっている。326 ページの『30.4.6 (1)　ISL ステータスの確認』を参照下さい。
- ISL がセグメントされている。326 ページの『30.4.6 (1)　ISL ステータスの確認』を参照下さい。
- VCS ファブリックモードが一方のスイッチで無効になっている。328 ページの『30.4.6 (2)　VCS ファブリック設定とルートブリッジ ID の確認』を参照下さい。
- 各スイッチで VCS ID が異なっている。328 ページの『30.4.6 (2)　VCS ファブリック設定とルートブリッジ ID の確認』を参照下さい。
- 隣接スイッチに LLDP が通知されてない。330 ページの『30.4.6 (3)　LLDP の確認』を参照下さい。
- CPU オーバーロードで keepalive パケット生成に失敗している。330 ページの『30.4.6 (4)　CPU 過負荷の確認』を参照下さい。

(1) ISL ステータスの確認

もし、どのポートも動作が怪しい場合、ISL ステータスをチェックします。

1．スイッチ上の異常なリンクの両端にて、特権実行モードで、ISL 接続の状態を見るため、’ show fabric isl’コマンドを入力します。

```
switch1# show fabric isl
Rbridge-id: 2 #ISLs: 2
Src Src Nbr Nbr
Index Interface Index Interface Nbr-WWN BW Trunk Nbr-Name

1 Te 2/0/1 1 Te 3/0/1 10:00:00:05:1E:CD:7A:7A 10G Yes "switch1"
2 Te 2/0/2 ? Te ?/?/? ??:??:??:??:??:??:??:?? (segmented -incompatible)
26 Te 2/0/26 56 Te 25/0/56 10:00:00:05:33:40:2F:C9 60G Yes "Edget12r31_25"
34 Te 2/0/34 58 Te 26/0/58 10:00:00:05:33:41:1E:B7 40G Yes "Edget12r32_26"

Ports on which the ISL link is broken appear with the text "(segmented -incompatible)."
Ports for which the ISL configuration is disabled do not appear in the output.
```

2．疑わしいポートの状態に関して、更に情報を採取するため’ show fabric islports’コマンドを入力します。

```
sw0# show fabric islports
Name:        sw0
Type:        107.4
State:       Online
Role:        Fabric Subordinate
VCS Id:      10
Config Mode:  Local-Only
Rbridge-id:   11
WWN:         10:00:00:05:33:6d:7f:77
FCF MAC:     00:05:33:6d:7f:77

 Index    Interface   State   Operational State
==========================================================================
  1      Te 11/0/1   Up     ISL 10:00:00:05:33:00:77:80 "sw0" (upstream)(Trunk
Primary)
  2      Te 11/0/2   Down
  3      Te 11/0/3   Down
  4      Te 11/0/4   Up     ISL (Trunk port, Primary is Te 11/0/1 )
  5      Te 11/0/5   Down
  6      Te 11/0/6   Down
  7      Te 11/0/7   Down
  8      Te 11/0/8   Down
  9      Te 11/0/9   Down
```

```
 10      Te 11/0/10  Down
 11      Te 11/0/11  Up     ISL 10:00:00:05:1e:00:50:00 "sw0" (Trunk Primary)
121      Fi 11/0/1   Up LS   ISL 50:00:53:37:b6:93:5e:02 "fcr_fd_160" (downstream)
(Trunk Primary)
122      Fi 11/0/2   Up LS   ISL (Trunk port, Primary is Fi 11/0/1 )
123      Fi 11/0/3   Down
124      Fi 11/0/4   Down
125      Fi 11/0/5   Down
126      Fi 11/0/6   Down
127      Fi 11/0/7   Down
```

３．もし、ポートの状態が”Down”なら、’no shutdown’コマンドでポートを有効化します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# no shutdown
```

４．もし、ポートの状態が”Up”だが、ISL がセグメントされている場合、セグメントされている理由のため”Operational State”を更なる手がかりとして調べる。
‘show fabric islports’コマンドとセグメントされた ISL の”Operational State"文字列の説明は、Network OS Command Reference を参照してください。

(2) VCS ファブリック設定とルートブリッジ ID の確認

ISL を正常に動作させるために、次の条件を守らなければなりません。

- 両スイッチで VCS ファブリックモードが有効であること
- 両スイッチで同じ VCS ID を使っていること
- 各スイッチでユニークなルーティング ID を使っていること

条件をチェックするため、次の手順を実行してください。

１．各スイッチで、’ show vcs’コマンドを入力する

２．出力によって、次の手順を実行する
もし、どちらかのスイッチで VCS ファブリックモードが有効でない場合、有効にするため’ vcs enable’コマンドを入力する。

```
switch1# show vcs
Config Mode : Local-Only
VCSID :1
Total Number of Nodes : 1
Rbridge-Id      WWN                             Management IP  Status HostName
-----------------------------------------------------------------------------
66             >10:00:00:05:33:67:26:78*       10.24.81.66    Online switch1


switch2# show vcs
```

```
state : Disabled


switch2# vcs vcsid 1 enable
```

もし、’ show vcs’コマンドの結果、互いの VCS ID が一致していない場合、設定を誤っているスイッチの VCS ID を修正するため’ vcs vcsid’コマンドを入力します。

```
switch1# show vcs
Config Mode : Local-Only
VCSID :1
Total Number of Nodes : 1
Rbridge-Id      WWN                             Management IP  Status HostName
-----------------------------------------------------------------------------
66              >10:00:00:05:33:67:26:78*       10.24.81.66    Online switch1


switch2# show vcs
Config Mode : Local-Only
VCSID :2
Total Number of Nodes : 1
Rbridge-Id      WWN                             Management IP  Status HostName
-----------------------------------------------------------------------------
66              >10:00:00:05:33:67:26:78*       10.24.81.77    Online switch1


switch2# vcs vcsid 1
```

もし、両スイッチとも同じルーティングブリッジ ID を持っているなら、ルーティングブリッジ ID をユニークな値に変更するため、’vcs rbridge-id’コマンドを入力する。

```
switch1# show vcs
Config Mode  : Local-Only
VCS ID    : 1
Total Number of Nodes      : 1
Rbridge-Id    WWN                   Management IP    Status  HostName
-----------------------------------------------------------------------------
66         >10:00:00:05:33:67:26:78* 10.24.81.66      Online  switch1


switch2# show vcs
Config Mode  : Local-Only
VCS ID    : 1
Total Number of Nodes      : 1
Rbridge-Id    WWN                   Management IP    Status  HostName
```

```
-----------------------------------------------------------------------------
66          >10:00:00:05:33:67:26:78* 10.24.81.77      Online  switch1

switch2# vcs rbridge-id 77
```

(3) LLDP の確認

ISL が正しく機能するとき、’ show lldp neighbors’コマンドは VCS ファブリッククラスタ内の各隣接スイッチの情報を表示します。

１．全ての隣接スイッチの LLDP 通知を確認するため’ show lldp neighbors’コマンドを入力します。

```
switch1# show lldp neighbors
Local Intf Dead Interval Remaining Life Remote Intf Chassis ID Tx Rx
Te 66/0/55 120 106 port1 0005.1e78.f004 20300 19914
Te 66/0/60 120 108 port0 0005.1e55.16c8 20300 19911
```

２．もし隣接スイッチが無ければ、更なる調査を行うか、サポート窓口か保守員に連絡してください。

(4) CPU 過負荷の確認

異常な CPU 高負荷は ISL の誤動作の原因となります。CPU 過負荷のトラブルシュートのために、324 ページの『30.4.3 不意の CPU 利用率高騰』の記載に従って、’ show process cpu’コマンドを使ってください。

30.4.7 ライセンスが正しくインストールされない

ライセンスされた機能が機能していないなら、大抵はその機能に対するライセンスが正しくインストールされていないからです。いずれかのライセンスがインストールされていないか、インストールされているが必ず必要なシステムリブートが実行されてないかのいずれかです。

もし、３つ目のスイッチを VCS ファブリッククラスタに追加できないなら、恐らく VCS Fabric license がインストールされていないでしょう。

もし、ライセンスが正しくインストールされていない疑いがあるなら、次の手順を実行してください。

１．特権実行モードで、現在どのライセンスがインストールされているかを確認するため、’ show license’コマンドを実行してください。

```
switch# show license
rbridge-id: 66
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
      VCS Fabric license
      Feature name:VCS_FABRIC
```

２．ライセンスが’ show license’コマンドで表示されなかった場合、インストールされていません。特権実行モードにて、ライセンスをインストールするために、’ license add lictstr’コマンドを入力してください。

```
switch# license add licstr "*B
slSETgzTgeVGUDeQR4WIfRx7mmXODdSwENoRGEnAmX3Ca3uHeZgXK0b,jzxyzfzKLrMsPN8ClSxvD
```

```
QRRT8VyuULyyKTO0ryU6qm4s1jjiSAeV,COoedzCx1v6ycQgnYMeSVp#"


License Added [*B
slSETgzTgeVGUDeQR4WIfRx7mmXODdSwENoRGEnAmX3Ca3uHeZgXK0b,jzxyzfzKLrMsPN8ClSxvD
QRRT8VyuULyyKTO0ryU6qm4s1jjiSAeV,COoedzCx1v6ycQgnYMeSVp#]
```

30.4.8 ハードウェアでのパケット破棄

この章では、全てのトラフィック、特定のトラフィック、特定のタイプのトラフィック、定常的、一時的にパケット破棄が発生したした時の問題のトラブルシュートについて説明します。パケット破棄は次に示す多くの理由で発生します。

- エンドデバイスでの高遅延。331 ページの『30.4.8 (1)　高遅延エンドデバイスによるパケット破棄』を参照下さい。
- データパスの障害。334 ページの『30.4.8 (2)　データパスの確認』を参照下さい。
- CRC エラー、パケットエラー、NIC との相互接続性エラーによるオプティカルライン上のノイズ。338 ページの『30.4.8 (3)　オプティカルラインのノイズをチェック』を参照下さい。

(1) 高遅延エンドデバイスによるパケット破棄

エンドデバイスが想定より応答に時間がかかることが原因で、ファブリック内のバッファオーバーランにより時々パケットが破棄されることがある。例えば、想定程早くデータを処理できないために、過負荷のディスクアレイがそのような遅延を発生さます。長時間データ受信を停止するデバイスは過度の遅延を発生させます。

これらの問題に対する究極のソリューションは、エンドデバイス自身を修正することです。しかし、スイッチとファブリックの設定に調整を加えることで問題を軽減することができます。

エンドデバイスでの遅延に起因する輻輳とパケット破棄を検出・緩和するために、次の手順を実行してください。

1．エンドデバイスが DCB に準拠していることを示す“DCBX TLVs”をチェックし、DCB ケイパビリティを広告しているかを確認するため、’ show lldp neighbors detail’コマンドを入力してください。

```
switch# show lldp neighbors detail
Neighbors for Interface Te 66/0/55


MANDATORY TLVs
===============
Local Interface: Te 66/0/55 (Local Interface MAC: 0005.3367.26d3)
Remote Interface: port1 (Remote Interface MAC: 0005.1e78.f004)
Dead Interval: 120 secs
Remaining Life : 104 secs
Chassis ID: 0005.1e78.f004
LLDP PDU Transmitted: 2412 Received: 2372
```

```
OPTIONAL TLVs
==============

DCBX TLVs
===========
Version : CEE
DCBX Ctrl OperVersion: 0 MaxVersion: 0 SeqNo: 1 AckNo: 4
DCBX ETS OperVersion: 0 MaxVersion: 0 Enabled: 1 Willing: 1 Error: 0
Enhanced Transmission Selection (ETS)
 Priority-Group ID Map:
  Priority : 0 1 2 3 4 5 6 7
  Group ID : 2 2 2 1 2 2 2 15
 Group ID Bandwidth Map:
  Group ID :  0  1  2  3  4  5  6  7
  Percentage:  0 40 60  0  0  0  0  0
  Number of Traffic Classes supported: 8
DCBX PFC OperVersion: 0 MaxVersion: 0 Enabled: 1 Willing: 1 Error: 0
Priority-based Flow Control (PFC)
   Enabled Priorities: 3
   Number of Traffic Class PFC supported: 8
FCoE App OperVersion: 0 MaxVersion: 0 Enabled: 1 Willing: 1 Error: 0
FCoE Application Protocol
   User Priorities: 3
```

2．Pauseフレームをチェックするため、’show qos flowcontrol interface’コマンドを入力します。

```
switch# show qos flowcontrol interface tengigabitethernet 66/0/55
Interface TenGigabitEthernet 66/0/55
 Mode PFC
 DCBX enabled for PFC negotiation
 TX 4926331124 frames
    TX    TX    RX     RX    Output Paused
CoS Admin  Oper   Admin   Oper   512    BitTimes
----------------------------------------
 0  Off    Off    Off    Off       0
 1  Off    Off    Off    Off       0
 2  Off    Off    Off    Off       0
 3  On     On     On     On        0
 4  Off    Off    Off    Off       0
```

```
 5  Off    Off    Off    Off       0
 6  Off    Off    Off    Off       0
 7  Off    Off    Off    Off       0
```

3．Cos 統計情報をチェックするため、’ show qos queue interface’コマンドを入力します。

```
switch# show qos queue interface tengigabitethernet 66/0/60
Interface TenGigabitEthernet 66/0/60
          RX      RX           TX        TX
 CoS     Packets   Bytes   TC    Packets     Bytes
 ---------------------------------- ----------------------------------
  0     1600    354184     0      0          0
  1        0         0     1    7962      636960
  2        0         0     2       0          0
  3     8508    544832     3      18       6048
  4        0         0     4       0          0
  5        0         0     5       0          0
  6        0         0     6       0          0
  7        0         0     7    2123      282360
 untag 2082 216528
```

4．破棄されたパケット、バッファ消費、およびリアルタイムのキュー統計を含む輻輳の指標をチェックするため、’ show qos rcv-queue interface’コマンドを入力します。

```
switch# show qos rcv-queue interface tengigabitethernet 66/0/55
Interface TenGigabitEthernet TenGigabitEthernet 66/0/55
 In-use 27216 bytes, Total buffer 144144 bytes
 0 packets dropped
        In-use    Max
 TC      Bytes   Bytes
-------------------------
  0       0      252
  1       0      252
  2       0      252
  3   27216      75284
  4       0      252
  5       0      252
  6       0     57456
  7       0      9576
```

５．QoS の設定をチェックするため、’ show qos interface’コマンドを入力します。

```
switch# show qos interface tengigabitethernet 66/0/55
Interface TenGigabitEthernet 66/0/55
 Provisioning mode cee
 Priority Tag disable
 CEE Map default
 FCoE CoS: 3
 FCoE Provisioned
 Default CoS 0
 Interface trust cos
        In-CoS:  0  1  2  3  4  5  6  7
  ------------------------------------------------
  Out-CoS/TrafficClass: 0/6 1/6 2/6 3/3 4/6 5/6 6/6 0/7
 Per-Traffic Class Tail Drop Threshold (bytes)
     TC:   0   1   2   3   4   5   6   7
  ------------------------------------------------------------------
  Threshold:  252  252  252 75284  252  252 57456  9576
 Flow control mode PFC
  CoS3 TX on, RX on
 Multicast Packet Expansion Rate Limit 3000000 pkt/s, max burst 4096 pkts
 Multicast Packet Expansion Tail Drop Threshold (packets)
  TrafficClass:  0  1  2  3  4  5  6  7
  ------------------------------------------------
   Threshold:  64  64  64  64  64  64  64  64
 Traffic Class Scheduler configured for 1 Strict Priority queues
  TrafficClass:  0  1  2  3  4  5  6  7
  ------------------------------------------
   DWRRWeight:  0  0  0 40  0  0 60 ---
 Multicast Packet Expansion Traffic Class Scheduler
  TrafficClass:  0  1  2  3  4  5  6  7
  ------------------------------------------------
   DWRRWeight:  12  13  12  13  12  13  12  13
```

６．QoS を再設定します。240 ページの『21 QoS の設定』を参照下さい。

(2) データパスの確認

この手順では、ファブリックの一貫性が破棄されたパケットの原因かどうかをチェックします。

１．エンドデバイスへのパスをテストするために’ping’コマンドを入力します。

```
switch# ping dest-address 10.24.81.2
PING 10.24.81.2 (10.24.81.2): 56 octets data
```

```
64 octets from 10.24.81.2: icmp_seq=0 ttl=128 time=9.4 ms
64 octets from 10.24.81.2: icmp_seq=1 ttl=128 time=0.3 ms
64 octets from 10.24.81.2: icmp_seq=2 ttl=128 time=0.3 ms
64 octets from 10.24.81.2: icmp_seq=3 ttl=128 time=0.3 ms
64 octets from 10.24.81.2: icmp_seq=4 ttl=128 time=0.3 ms


---10.24.81.2 ping statistics --5
packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/2.1/9.4 ms
```

2．パケットが到達したかエラーで破棄されたかを確認するために、‘show interface’コマンドを入力します。特に、次の例に示す受信統計情報のパケット数、バイト数やエラーパケットの数値が重要です。

```
switch# show interface tengigabitethernet 66/0/60
TenGigabitEthernet 66/0/60 is up, line protocol is up (connected)
Hardware is Ethernet, address is 0005.3367.26d8
  Current address is 0005.3367.26d8
Pluggable media present
Interface index (ifindex) is 283874428169
MTU 2500 bytes
LineSpeed Actual  : 10000 Mbit
LineSpeed Configured : Auto, Duplex: Full
Flowcontrol rx: off, tx: off
Last clearing of show interface counters: 22:07:59
Queueing strategy: fifo
Receive Statistics:
  15254 packets, 1395269 bytes
  Unicasts: 10641, Multicasts: 2637, Broadcasts: 1976
  64-byte pkts: 10874, Over 64-byte pkts: 3294, Over 127-byte pkts: 117
  Over 255-byte pkts: 969, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
  Over 1518-byte pkts(Jumbo): 0
  Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
  Errors: 0, Discards: 0
Transmit Statistics:
  12633 packets, 1155963 bytes
  Unicasts: 18, Multicasts: 12615, Broadcasts: 0
  Underruns: 0
  Errors: 0, Discards: 0
```

```
Rate info (interval 299 seconds):
  Input 0.000128 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 1d00h40m
```

3. 光モジュールが Brocade 製かをチェックするため’show media interface’コマンドを入力します。Vendor Name フィールドをチェックします。また、TX Power と RX Power フィールドがゼロでないことを確認します。

```
switch# show media interface tengigabitethernet 66/0/60
 Interface   TenGigabitEthernet 66/0/60
 Identifier   3 SFP
 Connector   7 LC
 Transceiver    0000000000000010 10_GB/s
 Name     id
 Encoding   6
 Baud Rate   103 (units 100 megabaud)
 Length 9u   0 (units km)
 Length 9u   0 (units 100 meters)
 Length 50u   8 (units 10 meters)
 Length 62.5u  3 (units 10 meters)
 Length Cu   0 (units 1 meter)
 Vendor Name  BROCADE
 Vendor OUI   00:05:1e
 Vendor PN   57-0000075-01
 Vendor Rev   A
 Wavelength   850 (units nm)
 Options    001a
 BR Max    0
 BR Min    0
 Serial No   AAA209282044472
 Date Code   090709
 Temperature  35 Centigrade
 Voltage    3356.4 (mVolts)
 Current    5.564 (mAmps)
 TX Power    568.9 (uWatts)
 RX Power    549.9 (uWatts)
```

4．MAC アドレステーブルが新しい値を学習しているかを確認するため、’show mac-address-table’ コマンドを入力します。新しい MAC アドレスはここに現れます。

```
switch# show mac-address-table
VlanId   Mac-address      Type    State    Ports
1002     0efc.0042.7300   FPMA    Active   Te 66/0/55
1002     0efc.0042.7302   FPMA    Active   Te 66/0/55
1002     0efc.0042.7800   FPMA    Active   Te 66/0/60
Total MAC addresses : 3
```

5．LLDP が全ての隣接スイッチを報告するか確認するために、’show lldp neighbors’コマンドを入力します。

```
switch# show lldp neighbors
Local Intf Dead Interval Remaining Life Remote Intf Chassis ID Tx
Rx
Te 66/0/55 120 101 port1 0005.1e78.f004 3000
2948
Te 66/0/60 120 117 port0 0005.1e55.16c8 2999
2945
```

もし、コマンド出力が全ての隣接スイッチを表示しない場合、サポート窓口か保守員に連絡してください。

6．イーサネットネームサーバの機能確認と、他の VCS ファブリックスイッチから学習済み MAC アドレスが存在するかを確認するため、’show mac-address-table’コマンドを入力します。
それらのスイッチがこの MAC アドレスを参照できるかを確認するため、ファブリック内の他のスイッチ上で、このコマンドを入力します。

```
switch# show mac-address-table
VlanId   Mac-address      Type    State    Ports
1002     0efc.0042.7300   FPMA    Active   Te 66/0/55
1002     0efc.0042.7302   FPMA    Active   Te 66/0/55
1002     0efc.0042.7800   FPMA    Active   Te 66/0/60
Total MAC addresses : 3
```

7．データパスのファブリック一貫性を検査するため、’l2traceroute’コマンドを入力します。
動的に学習されたソース MAC アドレスとデータパスに対するデスティネーション MAC アドレスを入力します。
拡張コマンドの中から、IP,SIP,DIP,TCP,Scr Port,Dest Port コマンドを使います。
Traceroute パケットが特定の ECMP リンクを通過するように IP コマンドパラメータを入力します。
‘l2traceroute’コマンドを使用する上での詳細は、348 ページの『30.5.1 Layer 2 traceroute』を参照下さい。

(3) オプティカルラインのノイズをチェック
オプティカルラインの過度のノイズは、CRC エラー、NIC 相互接続性エラーやその他状況により結果としてパケット破棄となります。

1．’show interface’コマンドを入力して、CRC エラーや TX 破棄をチェックします。次の例の Errors フィールドや Discards フィールドをチェックします。

```
switch# show interface tengigabitethernet 66/0/55
TenGigabitEthernet 66/0/55 is up, line protocol is up (connected)
Hardware is Ethernet, address is 0005.3367.26d3
 Current address is 0005.3367.26d3
Pluggable media present
Interface index (ifindex) is 283874100484
MTU 2500 bytes
LineSpeed Actual   : 10000 Mbit
LineSpeed Configured : Auto, Duplex: Full
Flowcontrol rx: off, tx: off
Last clearing of show interface counters: 21:51:35
Queueing strategy: fifo
Receive Statistics:
  15433457505 packets, 32164575799774 bytes
  Unicasts: 15433454934, Multicasts: 2571, Broadcasts: 0
  64-byte pkts: 11357, Over 64-byte pkts: 242664576, Over 127-byte pkts: 0
  Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
  Over 1518-byte pkts(Jumbo): 15190781568
  Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
  Errors: 0, Discards: 0
Transmit Statistics:
  21456965161 packets, 32549136821934 bytes
  Unicasts: 15313174675, Multicasts: 6143790486, Broadcasts: 0
  Underruns: 0
  Errors: 0, Discards: 0
Rate info (interval 299 seconds):
```

```
    Input 3345.136864 Mbits/sec, 200572 packets/sec, 33.45% of line-rate
    Output 3386.493904 Mbits/sec, 281345 packets/sec, 33.86% of line-rate
  Time since last interface status change: 1d00h24m
```

2．もし先の手順でエラーが報告されていれば、SFP トランシーバーやケーブルをチェックします。
   a．各スイッチ上で’ show media interface’コマンドを入力し、オプティックスが Brocade 製か確認するため Vender Name フィールドをチェックします。
   非 Brocade 製 SFP トランシーバは交換します。
   b．SFP トランシーバを交換してみます
   c．ケーブルを交換してみます。

30.4.9 Ping 失敗

もし、Ping が正常にスイッチを通らない場合、次の操作を試してください。

1．パケットの流れをトレースして、ARP か ICMP パケットが破棄されるかどうかをチェックします
2．インタフェースの統計情報を使って何れの方向が失敗するかトレースします。
3．パケットを破棄しているデバイスを探します。
4．デバイス上でどのエラーカウンタが増加するかを調査します。
5. MAC アドレスが正しいポート/port-channel で学習されるかどうかを判断するため MAC アドレステーブルをチェックします。

30.4.10 tail drops の原因となる QoS 設定

Tail-drop キューイングは輻輳制御の最も基本的な形です。全てのバッファーが尽きるまで、普通の動作は FIFO です。その後、新たなフレームが破棄されます。’ qos rcv-queue multicast threshold’コマンドを使って CoS 優先度の閾値を設定することにより、このような破棄の影響を低減することが出来ます。『21 QoS の設定』を参照下さい。

30.4.11 QoS は正しくパケットをマーキング・取り扱わない

QoS がパケットを正しくマーキングして取り扱うかをチェックするため、入出力ポートをミラーする Switched Port Analyzer (SPAN)機能を使います。『24 スイッチドポートアナライザ(SPAN)設定』を参照してください。

30.4.12 ルーティングブリッジ ID の重複

同じルーティングブリッジ ID を持つスイッチは、同一 VCS ファブリッククラスタ内に共存できません。存在するクラスタスイッチとして同じルーティングブリッジ ID を持つスイッチに対する試みは全て失敗します。２つのスイッチ間の ISL は、形成されませんし、セグメントされます。

1．新しいスイッチ上で、ルーティングブリッジ ID を決定するために、’ show vcs’コマンドを入力します。

```
switch2# show vcs
Config Mode : Local-Only
VCSID :1
```

```
Total Number of Nodes : 1
Rbridge-Id      WWN                             Management IP  Status HostName
-------------------------------------------------------------------------------
22             >10:00:00:05:33:13:B3:5A*    10.24.84.41    Online
```

2．動作している VCS ファブリッククラスタ内のどのスイッチ上でも、クラスタ内の全てのルーティングブリッジ ID を参照するため、'show vcs'コマンドを入力します。

```
switch1# show vcs
Config Mode : Local-Only
VCSID :1
Total Number of Nodes : 2
Rbridge-Id      WWN                             Management IP  Status HostName
-------------------------------------------------------------------------------
60              10:00:00:05:33:5F:EA:A4      10.24.81.65    Online switch1
66             >10:00:00:05:33:67:26:78*     10.24.81.66    Online switch 2
```

3．もし新しいスイッチがクラスタ内に存在するいずれかのスイッチと同じルーティングブリッジ ID を持っていれば、特権実行モードにて、ルーティングブリッジ ID をユニークな値に変更するため、' vcs rbridge-id'コマンドを入力します。

```
switch2# vcs rbridge-id 77
```

30.4.13　　SNMP MIB の不正値報告

もし、SNMP MIB が不正な値を報告した場合は、次の手順を実行してください。

1．サポートされた MIB ブラウザを使っているかを確認します。
2．問題は一貫して発生しているか確認します。
3．SNMP 設定が正しいか確認します。
4．もし、MIB ブラウザがサポートされたものであり、SNMP 設定が正しく、一貫して問題が発生しているならば、サポート窓口や保守員に連絡してください。

30.4.14　　SNMP trap 通知の失敗

もし SNMP trap 通知が失敗するなら、次の手順を実行してください。

1．正しい SNMP 設定が行われているか確認します。『8 SNMP 管理』を参照してください。
2．SNMP ホストがリーチャブルか確認します。
3．もし問題が依然として継続するなら、サポート窓口や保守員に連絡してください。

Workaround として、syslog メッセージに対して trap 設定をしてください。

30.4.15　　スイッチへの telnet 失敗

正しい IP アドレスと正しいログイン情報を想定しても、telnet を使ったスイッチへのアクセス失敗は次の理由のいずれかのためです。

- 管理ポートがダウンしている。341 ページの『30.4.15 (1)　管理ポートの状態を確認する』を参照

してください。

- 管理インタフェースへのアクセスが ACL で拒否されている。342 ページの『30.4.15 (2)　拒否 ACL の確認』を参照してください。
- スイッチ CPU が過負荷である。342 ページの『30.4.15 (3)　CPU 過負荷の確認』を参照してください。

(1) 管理ポートの状態を確認する

1．システムコンソール上で、管理ポートの状態をチェックするため、’ show system’コマンドを入力します。Management Port Status フィールドを確認します。

```
switch# show system
Stack MAC               : 00:05:33:67:26:78


 -- UNIT 0 --
Unit Name               : switch
Switch Status            : Online
Hardware Rev             : 107.4
TengigabitEthernet Port(s) : 60
Up Time                 : up 1 day, 2:52
Current Time             : 23:40:50 GMT
NOS Version              :
Jumbo Capable            : yes
Burned In MAC            : 00:05:33:67:26:78
Management IP            : 10.24.81.66
Management Port Status    : UP


 -- Power Supplies --
PS1 is faulty
PS2 is OK


 -- Fan Status --
Fan 1 is Ok
Fan 2 is Ok
Fan 3 is Ok
```

2．もし管理ポートのステータスが DOWN ならば、管理ポートを正しく設定するために、’interface management’コマンドを入力します。53 ページの『3.5 イーサネット管理インタフェースの構成』を参照してください。
3．問題が継続するようなら、サポート窓口や保守員に連絡してください。

(2) 拒否 ACL の確認
システムコンソール上で、’show running-config ip access-list’コマンドを入力して、ACL が管理ポートのアクセスを拒否していないかを判断するため、出力を確認してください。

(3) CPU 過負荷の確認
スイッチ CPU の過負荷は、telnet アクセスを阻害します。324 ページの『30.4.3 不意の CPU 利用率高騰』を参照してください。

30.4.16 Trunk メンバ未使用

もし、trunk メンバポートが使用されていないと疑われるなら、次の手順を実行してください。
1．どのインタフェースでトランキングが有効になっているかを判断するため、’show running-config interface’コマンドを入力します。

```
switch# show running-config interface
interface Management 66/0
 no ip address dhcp
 ip address 10.24.81.66/20
 ip gateway-address 10.24.80.1
 ipv6 address ""
 no ipv6 address autoconfig
!
interface TenGigabitEthernet 66/0/1
 fabric isl enable
 fabric trunk enable
 no shutdown
!
interface TenGigabitEthernet 66/0/2
 fabric isl enable
 fabric trunk enable
 no shutdown
!
interface TenGigabitEthernet 66/0/3
 fabric isl enable
 fabric trunk enable
 no shutdown
```

```
!
（出力省略）
```

2．ISL ポートとリンクの状態を検証します。

ａ．ISL がアップしているかどうか検証するため、’ show fabric isl’コマンドを入力します。

ｂ．各ポートの状態を検査するため、’ show fabric islports’コマンドを入力します。
詳細と修正のため操作は、326 ページの『30.4.6 (1)　ISL ステータスの確認』を参照してください。

3．それぞれのトランクリンクに対して、’ show interface’コマンドを入力し、トランクのインタフェースのトラフィックが均一に分配されているかをチェックするため、レート情報を精査します。

```
switch# show interface tengigabitethernet 66/0/12
TenGigabitEthernet 66/0/12 is up, line protocol is down (link protocol down)
Hardware is Ethernet, address is 0005.3367.26a8
  Current address is 0005.3367.26a8
Pluggable media not present
Interface index (ifindex) is 283871281409
MTU 2500 bytes
LineSpeed Actual   : Nil
LineSpeed Configured : Auto, Duplex: Full
Flowcontrol rx: off, tx: off
Last clearing of show interface counters: 1d00h42m
Queueing strategy: fifo
Receive Statistics:
  0 packets, 0 bytes
  Unicasts: 0, Multicasts: 0, Broadcasts: 0
  64-byte pkts: 0, Over 64-byte pkts: 0, Over 127-byte pkts: 0
  Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
  Over 1518-byte pkts(Jumbo): 0
  Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
  Errors: 0, Discards: 0
Transmit Statistics:
  0 packets, 0 bytes
  Unicasts: 0, Multicasts: 0, Broadcasts: 0
  Underruns: 0
  Errors: 0, Discards: 0
Rate info (interval 299 seconds):
  Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 1d03h16m
```

4. 他のトランクメンバはビジーであるのにトラフィックが発生していないトランクメンバが見られる場合、同じ’ show interface’コマンドの出力から、インタフェースの状態、設定、エラー統計情報などをチェックします。
もし、インタフェースが無効化されていたら、’no shutdown’コマンドで有効化します
もし、設定ミスがあるなら、ファブリックトランクの設定方法については、『9 ファブリック管理』を参照してください。
もし、エラー統計情報に極端なエラーが見られるならば、エラーによっては、SFP トランシーバやケーブルをチェックしてください。
ａ．’show media interface’コマンドを各スイッチ上で入力して、Brocade 製のモジュールかを確認するため Vender Name をチェックしてください。
非 Brocade 製 SFP トランシーバは交換してください。
ｂ．SFP トランシーバを交換してみます。
ｃ．ケーブルを交換してみます。

30.4.17　　アップデート失敗

ファームウェアのアップデート中に問題が発生したら、次の手順を実行します。
1．以前のファームウェアバージョンに戻します。
2．アップデートを再試行することが適切かどうかを確認するため、サポート窓口や保守員に連絡してください。

30.4.18　　VCS ファブリックが形成されない

VCS ファブリックがいくつかの理由で形成に失敗することがあります。
- 必要なライセンスが有効化されてない。344 ページの『30.4.18 (1)　VCS Fabric licenses の確認』を参照下さい。
- VCS ファブリック設定が正しくない。次の構成上の問題は VCS ファブリックの形成を阻害します。
  - VCS ファブリックモードが有効になってない。
  - 構成するスイッチの VCS ID が一致してない。
  - スイッチに接続している ISL ポートがアップしてない。

345 ページの『30.4.18 (2)　VCS ファブリック設定の確認』を参照してください。

(1) VCS Fabric licenses の確認

もし、VCS ファブリッククラスタが一つないしは二つのスイッチから構成されるならば、VCS Fabric license は必要ありません。VCS ファブリッククラスタに３台以上のスイッチが存在する場合、VCS Fabric license をインストールしなければなりません。

1. 必要な VCS Fabric license がインストールされているかどうかをチェックするため、’show license’コマンドを入力します。

```
switch# show license
rbridge-id: 66
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
      FCoE Base license
```

```
      Feature name:FCOE_BASE
```

2．’show license’コマンドの出力に VCS Fabric license が表示されない場合、ライセンスを有効化するため’ license add licstr’コマンドを入力します。

```
switch# license add licstr "*B
r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANFav5W:gWx3hH2:9RsMv3BHfeC
RFM2gj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#"

Adding license [*B
r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANFav5W:gWx3hH2:9RsMv3BHfeC
RFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#]
```

3．ライセンスが追加されたか確認するため、’ show license’コマンドを入力します。

NOTE

VCS Fabric license を有効化するため、スイッチをリブートする必要はありません。

```
switch# show license
Rbridge-Id: 66
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
      FCoE Base license
      Feature name:FCOE_BASE
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
      VCS Fabric license
      Feature name:VCS_FABRIC
```

ライセンス管理の更に詳細情報については、81 ページの『7 ライセンスの管理』を参照下さい。

(2) VCS ファブリック設定の確認

VCS ファブリック設定を確認するために、次の手順を実行してください。

1．VCS ファブリックモードが有効か、各スイッチの VCS ID が一致しているか、ルーティングブリッジ ID が異なっているかを確認するため、各スイッチ上で’ show vcs’コマンドを入力する。

2．ISL がアップしているかどうかを確認するため、’show fabric isl’コマンドを実行する。

3．各ﾎﾟｰﾄの状態を精査するため、’show fabric islports’コマンドを実行する。

詳細と修正のための操作については、326 ページの『30.4.6 ISL が動作しない』を参照下さい。

30.4.19 vLAG が形成されない

vLAG トランクが幾つかの理由で形成に失敗することがあります。

- VCS ファブリックスイッチ間のリンクが存在しない。346 ページの『30.4.19 (1) VCS ファブリックスイッチ間の接続確認』を参照下さい。
- LACPDU の異常な送受信による接続不良。346 ページの『30.4.19 (2) LACPDU を確認する』を参照下さい。
- VCS ファブリックスイッチ上で port-channel 番号の不一致。346 ページの『30.4.19 (3) vLAG 設定

の確認』を参照下さい。

- スイッチ間で異なる LACP モード(static/dynamic)。347 ページの『30.4.19 (4)　各スイッチの LACP モードの確認』を参照下さい。
- 1G port-channel 時の設定漏れ。347 ページの『30.4.19 (5)　1G port-channel の明示的なスピード設定』を参照下さい。

(1) VCS ファブリックスイッチ間の接続確認

スイッチ間の接続が様々な理由のため切断されていることがあります。

ポートが有効化されてない。

ISL トランクがセグメントされている。

VCS ファブリックが正しく形成されていない。

CPU 過負荷

問題の検出と修正に関する詳細は、326 ページの『30.4.6 ISL が動作しない』を参照下さい。

(2) LACPDU を確認する

LACPDU は vLAG の両端で送受信されなければなりません。この手順では、問題が発生したか、及び PDU のエラーかどうかをチェックする方法を示します。

1．両スイッチ上で、LACPDU を送受信しているか、エラーPDU は無いかを確認するため、'show lacp counter'コマンドを入力します。

```
switch# show lacp counter 10
% Traffic statistics
Port      LACPDUs         Marker          Pckt err
         Sent    Recv    Sent    Recv    Sent    Recv
% Aggregator  Po 10 1000000
Te0/1     65      0       0       0       0       0
Te0/2     64      0       0       0       0       0
Te0/3     64      0       0       0       0       0
Te0/4     0       0       0       0       0       0
```

このケースでは、LACPDU はスイッチにより送信されているが、受信されていません。

2．コマンド出力結果から LACPDU が正しく送受信されていない、または、パケットエラーを示している場合、サポート窓口か保守員に連絡下さい。

(3) vLAG 設定の確認

port-channel 番号は、全ての vLAG メンバスイッチに渡って一致しなければなりません。そうでなければ、vLAG は形成されません。

1．各 vLAG メンバスイッチ上で、特権実行モードにおいて、'show port-channel'コマンドを入力します。

```
switch# show port-channel summary
Static Aggregator: Po 15
Aggregator type: Standard
Member ports:
```

```
 Te 0/6
 Te 0/7
 Te 0/14
 Te 0/15
...
switch2# show port-channel summary
switch2#
```

2．Port-channel が両スイッチ上に表示されない場合、表示されないスイッチ上で、グローバルコンフィグレーションモードにて、port-channel を生成するために’ interface port-channel’コマンドを入力します。

```
switch2(config)# interface port-channel 15
```

詳細は、『17 リンクアグリゲーションの設定』を参照下さい。

(4) 各スイッチの LACP モードの確認

vLAG は vLAG の両端のスイッチ上で静的または動的に設定されなければなりません。詳細は、『17 リンクアグリゲーションの設定』を参照下さい。

(5) 1G port-channel の明示的なスピード設定

Network OS 3.0 では、1Gbps のポートスピードの vLAG は、ポートスピードをコンフィグで明示的に指定しなければ形成されません。デフォルトのポートスピードは、10Gbps です。1Gbps のポートスピードをもつ LAG 及び vLAG は、次のマイグレーション手順で形成されます。

1Gbps のポートスピードを設定するために、次の手順を実行してください。

1．インタフェースコンフィグレーションモードにて、port-channel を shutdown します。

```
switch(config-Port-channel-2)# shutdown
```

2．port-channel スピードを 1Gbps に設定します。

```
switch(config-Port-channel-2)# speed 1000
```

3．port-channel で、全てのメンバを再有効化します。

```
switch(config-Port-channel-2)# no shutdown
```

30.5　トラブルシューティングと診断ツール

この章では、Network OS 3.0 で使用できる様々なトラブルシューティングと診断ツールについての解説と、それらを使用する場合のガイドラインを示します。

また、310 ページの『30.2 問題解決情報の収集』を参照下さい。そこでは、Network OS の supportsave

についての情報を提供しています。

30.5.1 Layer 2 traceroute

TRILL OAM はファブリックパスの一貫性を検証するため、’ l2traceroute’コマンドを提供しています。‘l2traceroute’コマンドを拡張オプション付で使用すると、レイヤ２traceroute パケットが通過するレイヤ２パス上で細やかな制御が可能となります。

(1) レイヤ２ traceroute パケット

レイヤ２traceroute ツールを使用するために、リクエストフレームかレスポンスフレームかワイヤ上で観測できるレイヤ２traceroute パケットの構造を理解する必要があります。

図 30-1 は、通常のレイヤ２パケットがレイヤ２traceroute を適用しない状態でイーサネットファブリックを通過する時どのように見えるかを示しています。

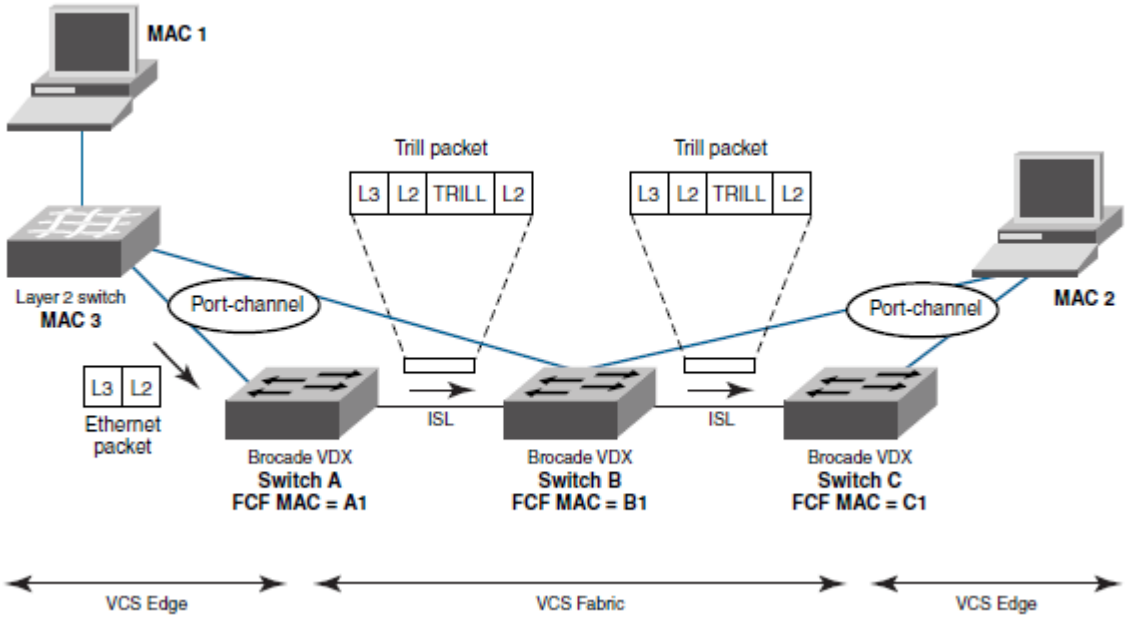

図 30-1 VCS ファブリックを通過する通常のレイヤ２パケット

図 30-1 では、イーサネットパケットが MAC1 から VCS ファブリックのエッジに到達しています。TRILL ヘッダの情報は、VCS ファブリックを通過する際に追加されます。TRILL 情報は VCS ファブリックを抜ける時に削除され、通常のイーサネットパケットが MAC2 に到着します。表 30-3 は、レイヤ２パケットヘッダの詳細を示しています。

表 30-3 VCS ファブリックを通過するレイヤ２パケットのヘッダ詳細

イーサネットパケット	TRILL パケットー最初のホップ	TRILL パケットー２番目のポップ
L2 DA = MAC 2 L2 SA = MAC 1	Outer L2 DA = B1 Outer L2 SA = A1 Outer 802.1q tag Outer etype = TRILL TRILL destination RBridge ID = C TRILL source RBridge ID = A TRILL flags Inner L2 DA = MAC 2 Inner L2 SA = MAC 1 Inner 802.1q tag Inner etype = 0x800	Outer L2 DA = C1 Outer L2 SA = B1 Outer 802.1q tag Outer etype = TRILL TRILL destination RBridge ID = C TRILL source RBridge ID = A TRILL flags Inner L2 DA = MAC 2 Inner L2 SA = MAC 1 Inner 802.1q tag Inner etype = 0x800

'l2traceroute'コマンドを使ってパケットを見るとき、それらが VCS ファブリックを通過する際パケットに付加された TRILL OAM ヘッダ情報が見られます。Switch A 上でトレースを開始すると、TRILL OAM は、隣接スイッチ、この場合は Switch B、とのパスの一貫性を最初に確認します。これは、図 30-2 に示すとおり、TRILL 属性の time-to-live (TTL)を'1'に設定したレイヤ２traceroute リクエストパケットを送信することで行われます。Switch B は next hop を読み出した到達可能情報と共にレスポンスを返します。

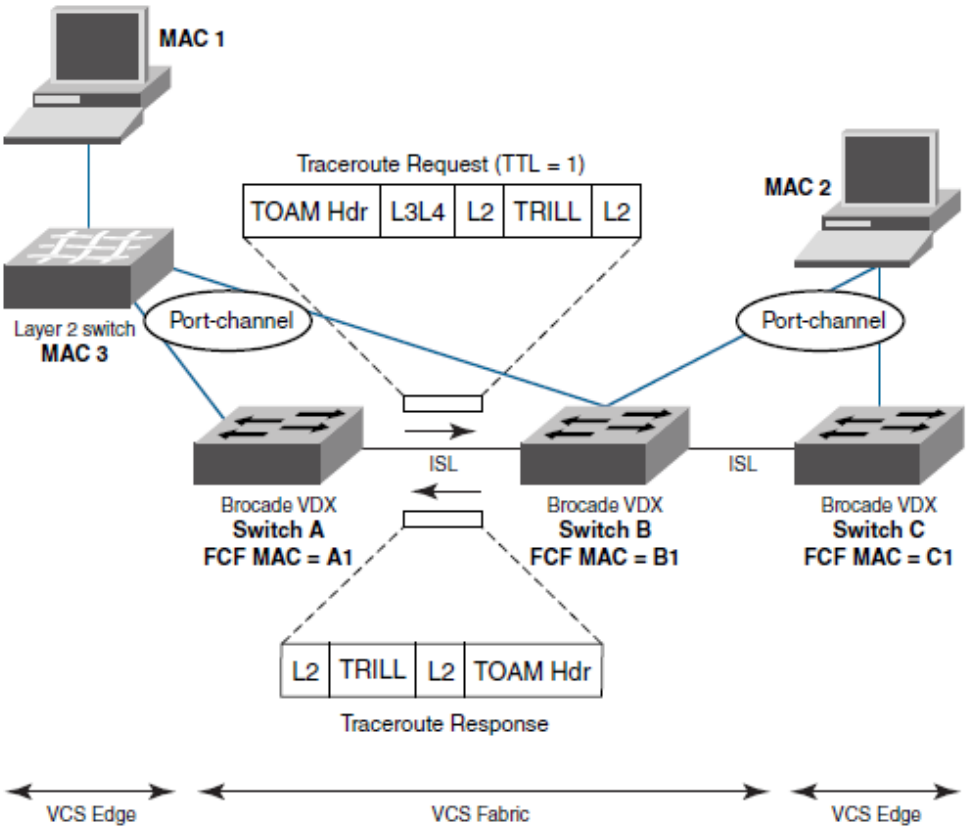

図 30-2 隣接スイッチとのパスー貫性の検証

表 30-4 は、リクエスト及びレスポンスのパケットヘッダ情報を示します。追加された TRILL OAM 情

報は、太字で示されます。

表 30-4 レイヤ２traceroute の第一ホップのパケットヘッダ詳細

traceroute 要求パケットのヘッダー	traceroute 応答パケットのヘッダー
Outer L2 DA = B1 Outer L2 SA = A1 Outer 802.1q tag Outer etype = TRILL TRILL destination RBridge ID = C TRILL source RBridge ID = A TRILL flags: TTL = 1 Inner L2 DA = MAC 2 Inner L2 SA = MAC 1 Inner 802.1q tag Inner etype = 0x800 TOAM Opcode = 5 (request)	Outer L2 DA = B1 Outer L2 SA = A1 Outer 802.1q tag Outer etype = TRILL TRILL destination RBridge ID = A TRILL source RBridge ID = B TRILL flags: TTL = MAX (63) Inner L2 DA = A1 Inner L2 SA = B1 Inner 802.1q tag Inner etype = TRILL OAM TOAM Opcode = 4 (reply) C reachable

隣接スイッチ(Switch B)と継続的にパケットが交換されることと Switch C への到達性を確立することは、レイヤ２traceroute 機能が TTL を'2'に設定することで別のリクエストを作り出します。
Switch B は、TTL カウントを減じて Switch C にパケットを転送します。そして、Swith A にレスポンスを返します。図 30-3 を参照してください。

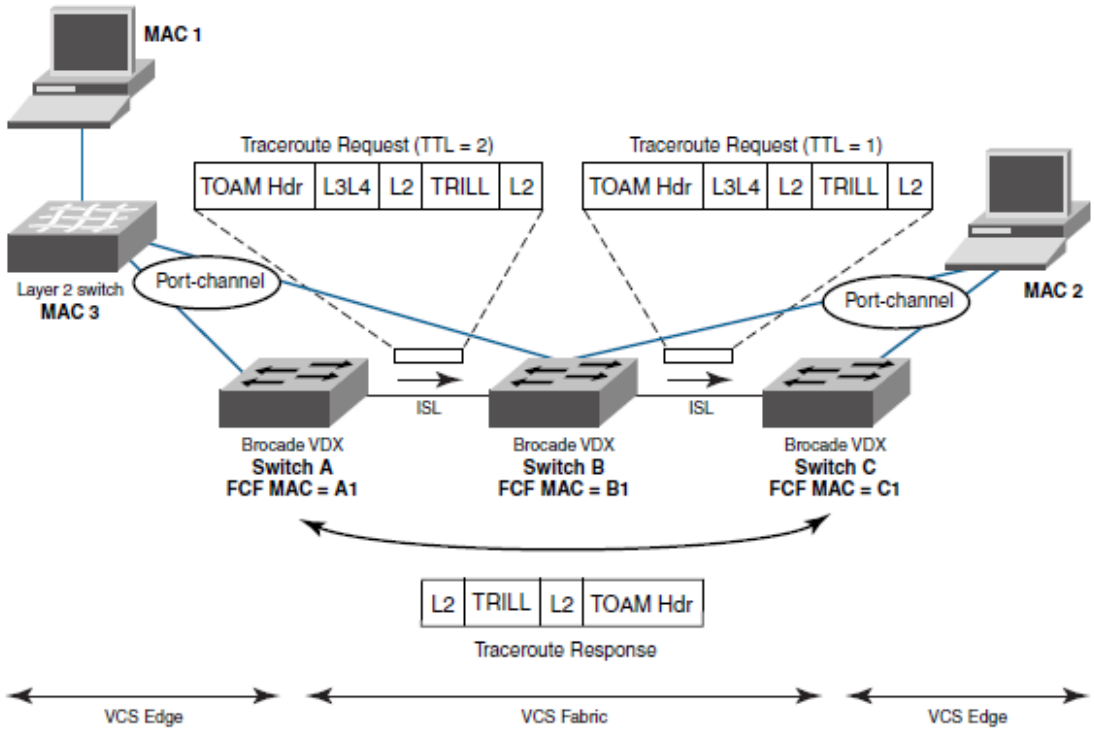

図 30-3 第２ホップへのパス一貫性の検証

表 30-5 は、リクエストとレスポンスのパケットヘッダ情報を示します。レイヤ２traceroute 機能固有

の情報は、太字で示されます。

表 30-5 レイヤ２traceroute の第２ホップへのパケットヘッダ詳細

Traceroute 要求－最初のホップ (TTL = 2)	Traceroute 要求－２番目のホップ (TTL = 1)	Traceroute 応答
Outer L2 DA = B1 Outer L2 SA = A1 Outer 802.1q tag Outer etype = TRILL TRILL destination RBridge ID = C TRILL source RBridge ID = A TRILL flags: TTL = 2 Inner L2 DA = MAC 2 Inner L2 SA = MAC 1 Inner 802.1q tag Inner etype = 0x800 TOAM Opcode = 5 (request)	Outer L2 DA = C1 Outer L2 SA = B1 Outer 802.1q tag Outer etype = TRILL TRILL destination RBridge ID = C TRILL source RBridge ID = A TRILL flags: TTL = 1 Inner L2 DA = MAC 2 Inner L2 SA = MAC 1 Inner 802.1q tag Inner etype = 0x800 TOAM Opcode = 5 (request)	Outer L2 DA = B1->A1 Outer L2 SA = C1->B1 Outer 802.1q tag Outer etype = TRILL TRILL destination RBridge ID = A TRILL source RBridge ID = C TRILL flags: TTL = MAX (63) Inner L2 DA = A1 Inner L2 SA = B1 Inner 802.1q tag Inner etype = TRILL OAM TOAM Opcode = 4 (reply)

(2) l2traceroute コマンドを使ったトレース情報

次の例では、’ l2traceroute’コマンドがポート 3/0/1(ソース MAC: 0050.5685.0003)とポート 2/0/9(ソース MAC: 0024.3878.3720)の間のパスを検証しています。

１．ネットワーク上の全ての MAC アドレスを表示するため、’show mac-address-table’コマンドを入力します。

```
switch# show mac-address-table
VlanId  Mac-address    Type   State   Ports
100   0024.3878.e720  Dynamic Active  Po 11
100   0050.5685.0001  Dynamic Active  Po 1
101   0000.0000.0003  Dynamic Active  Po 1
101   0024.3878.e720  Dynamic Active  Po 11
101   0050.5685.0003  Dynamic Active  Po 1
Total MAC addresses  : 5
```

出力結果から、ソースとデスティネーション MAC アドレスを選択します。

・Source MAC: 0050.5685.0003

・Destination MAC: 0024.3878.e720

２．’l2traceroute’コマンドを入力します

```
switch2# l2traceroute
Source mac address          : 0050.5685.0003
Destination mac address      : 0024.3878.e720
Vlan [1-3962]              : 101
Edge rbridge-id [1-239]      : 3
Extended commands [Y/N]?     : y
```

```
Protocol Type [IP]          : IP
Source IP address           : 101.101.101.10
Destination IP address       : 101.101.101.101
IP Protocol Type [TCP/UDP]    : TCP
Source port number [0-65535]  : 3000
Dest port number [0-65535]    : 22
Rbridge  Ingress               Egress                Rtt(usec)
--------------------------------------------------------------------------------
3       Te 3/0/1(std-lag, Po 1)  Te 3/0/20(isl) 0
2       Te 2/0/20(isl)          Te 2/0/9(std-lag, Po 11)  34041
```

以下の点をご承知おきください。

・MAC アドレスは MAC address-table に存在しなければならない(dynamic or static)
・' l2traceroute'コマンドは VCS ファブリックモードでのみ使用可能
・パス選択に影響する'IP'パラメータを使用してください

30.5.2 show コマンド

表 30-6 は、トラブルシュートでしばしば使用される'show'コマンドをリストしています。全ての'show'コマンドの詳細については、『Network OS Command Reference』を参照して下さい。

表 30-6 トラブルシュートに使われる show コマンド

コマンドグループ	コマンド	特定のフィールドまたは目的
システムコマンド	show system	
	show license	
	show running-config	
	show startup-config	
	show logging raslog	
	show version	
	show chassis	
	show environment	
	show vlan brief	
	show mac-address-table	
	show process cpu	
	show process memory	
	show firmwaredownloadstatus	
インタフェースコマンド	show interface	
	show media	
	show ip int brief	
	show qos flowcontrol interface	ポーズフレームをチェックします。
	show qos queue interface	CoS 統計情報をチェックします。
	show qos rcv-queue interface	パケットドロップ、バッファ消費、リアルタイムのキュー統計をチェックします。

	show qos int	インタフェース上でのQoS設定をチェックします。
診断コマンド	show diags status	
	show diags post results detailed	
	show diag burninerrshow	
	show diag burninstatus	
機能コマンド	show port-channel detail	
	show lacp counter	
	show port-profile status	
	show lldp neighbors detail	
	show lldp statistics	
	show qos interface all	
VCSファブリックコマンド	show vcs	
	show fabric trunk all	
	show fabric all	
	show fabric isl	
	show fabric islports	
	show fabric route linkinfo	
	show fabric route multicast	
	show fabric route neighbor-state	
	show fabric route pathinfo	
	show fabric route topology	
	show name-server detail	

30.5.3 Debugコマンド

デバッグ機能に関連した次の操作を実行することが出来ます。

- デバッグ機能を有効にするため、'debug'コマンドを使います。

```
debug feature required-keywords
```

- デバッグ機能が有効かどうかを確認するため、'show debug'コマンドを使います。

```
show debug feature
```

- デバッグ機能を無効化するため、'no debug'コマンドを使います。

```
no debug feature required-keywords
```

リアルタイムでバッギングはCPUに負担を掛けますので、運用環境でのリアルタイムでデバッグする際は注意を払ってください。まず、テスト機でデバッグ出力をチェックして、結果が許容できるならば実運用環境で更にデータ収集するためデバッグ機能を有効化してください。加えて、CPU 負荷を軽減するために、「詳細」や「全て」といった包括的なオプションより、デバッグ機能の範囲を限定する特定イベントや「要約」のようなオプションを使用することを推奨します。

デバッグ機能の操作は、主にLACPやLLDPのようなコントロールプレーンをデバッグするために使います。例えば、コンソールでLLDPパケットの受信を確認するために、次のコマンドを使用します。

```
switch# debug lldp packets all rx
```

スイッチがtelnetでアクセスされているなら、ターミナルモニタを有効化します。次の例は、最もよく使われる'debug'コマンドの例です。

・`debug lldp packets interface [rx | tx | both]`

・`debug lacp pdu [rx | tx]`

・debug spanning-tree bpdu [rx | tx] – Standaloneモードのみ

・debug dot1x packet – Standaloneモードのみ

30.5.4 SPANポート及びトラフィックミラーリング

あるインスタンスにおいて、特定ポートのトラフィックパターンを理解するためにリンクを通過するパケットを調査する必要があるかもしれません。このような状況では、アナライザを接続したミラーポートに特定のイーサネットポートのトラフィックをコピーするため、Switched Port Analyzer (SPAN)を設定することが出来ます。アナライザによりキャプチャされたパケットを分析することが可能になります。

```
switch(config)# monitor session 1
switch(conf-mon-sess-1)# source tengigabitethernet 1/0/10 destination
tengigabitethernet 1/0/15 direction both

switch# show monitor 1
Session :1
Description :Test SPAN Session
State :Enabled
Source interface : 1/0/10 (Up)
Destination interface : 1/0/15 (Up)
Direction :Both
```

デスティネーションポートを、ISL,レイヤ２，レイヤ３，QoS, ACL, 802.1x, LAG メンバ, LLDP, port-profileポートにすることは出来ません。ソースポートをISLポートにすることはできません。VCSファブリックモードでは、エッジポートだけがミラーリング可能です。

30.5.5 ハードウェア診断

次の診断タイプ現状あります。

- Power-on self-test (POST)
- オフライン診断

オンライン診断機能は現状ありません。

(1) POST診断

POSTはブート時に実行され、結果は格納されます。格納された結果を参照するために、’show diag post results’コマンドを使います。

POSTを有効にするために、’diag post [rbridge-id] [rbridge-id] enable’コマンドを使います。

(2) オフライン診断

オフライン診断は、個々のハードウェアコンポーネント全体をチェックし、検出したことをレポート

する破壊的テストです。テストを実行する前に、モジュールを無効化('chassis disable')する必要があります。決して、運用中に実施しないで下さい。
一通りのオフライン診断を実行するために、' diag systemverification'コマンドを入力します。このコマンドは、完了するまでに 2 時間かかります。また、ハードウェアの様々な部分をチェックするオフラインコマンドの一部を実行することも出来ます。表 30-7 は、サポートしているオフラインコマンド全てをリストしています。

表 30-7 オフライン診断コマンド

オフライン診断コマンド	目的
diag burninerrclear	バーンインプロセス中に不揮発性ストレージに保存されているエラーをクリアします。
diag clearerror	診断障害状態をクリアします。
diag portledtest	ポート LED 上の各種アクションモードを実行し、機能を検証します。
diag portloopbacktest	スイッチ上で様々な ASIC 間のフレームを送信し、ASIC の機能を検証します。
diag setcycle	システム検証テストに必要なすべてのパラメータを設定します。
diag systemverification	様々なハードウェア診断テストを組み合わせて実行します。
diag turboramtest	ASIC チップのターボスタティック RAM（SRAM）テストを実行します。

表 30-8 は、オフライン診断の出力を確認する'show'コマンドをリストしています。

表 30-8 オフライン診断 show コマンド

オフライン診断表示コマンド	目的
show diag burninerrshow	バーンイン時に不揮発性ストレージに格納されたエラーを表示します。
show diag burninstatus	診断バーンインステータスを表示します。
show diag setcycle	システム検証で使用されている現在の値を表示します。
show diag status	現在、実行している診断テストを表示します。

表 30-7 と表 30-8 にリストされたコマンドの詳細は、『Network OS Command Reference』を参照下さい。

30.5.6 'show fabric route pathinfo 'コマンドによる経路情報の参照

'show fabric route pathinfo'コマンドは、ローカルスイッチ上のソースポートインデックスから、VCS ファブリッククラスタや、異なる VCS ファブリッククラスタや、接続された Fabric OS の backbone fabric や、エッジファブリックにある別のスイッチ上のデスティネーションポートインデックスまでの経路を情報を表示します。この経路情報は、全てのファブリック内のスイッチを含むこれらのポート間を通過するデータストリームのフルパス情報を示しています。
経路及び統計情報は、現在のルーティングテーブル情報とリアルタイムに継続的に集計される統計情報に基づき、パスに沿った全てのスイッチによって提供されます。各スイッチは、1 hop を表します。
'show fabric route pathinfo'コマンドをリモートファブリックに跨り使用するためには、リモートスイ

ッチの VCS ID(または Fabric ID)とルーティングブリッジ ID(ドメイン ID)の両方を指定しなければなりません。リモートファブリックにまたがってパス情報を入手する時、デスティネーションスイッチはルーティングブリッジ ID またはドメイン ID により特定されます。名称や WWN によりスイッチを特定することは、受け付けられません。
‘show fabric route pathinfo’コマンドの詳細は、『Network OS Command Reference』を参照してください。

31 TACACS+ Accounting の例外

31.1 コマンドアカウンティングの制限

TACACS+コマンドアカウンティングは、次の制限事項があります。

- TACACS+コマンドアカウンティングは、ベースコマンド名をログに記録します。例えば、実行されたコマンドが'secpolicy defined-policy SCC_POLICY'の場合、'secpolicy'コマンドのみが TACACS++サーバに記録されます。
- 'no radius-sever'コマンドは、'radius-server'コマンドとして記録されます。
- いくつかのコマンドは考慮されません。サポートされていない運用コマンドのリストについては、表 31-1 を参照してください。サポートされていないコンフィギュレーションコマンドのリストについては、表 31-2 を参照してください。

表 31-1 特権実行モードでサポートされていないコマンド

コマンド名	コマンド説明
cipherset	LDAP と SSH のために FIPS 準拠の安全な暗号を設定します。
clear	指定されたパラメータをクリアします。
clear arp	Address Resolution Protocol（ARP）の設定データをクリアします。
clear counters	スイッチからの統計情報をクリアします。
clear dot1x	IEEE 802.1X ポートベースのアクセス制御の設定データをクリアします。
clear ip	インターネットプロトコル（IP）の設定データをクリアします。
clear lacp	Link Aggregation Control Protocol（LACP）の設定データをクリアします。
clear lldp	Link Layer Discovery Protocol（LLDP）の設定データをクリアします。
clear mac-address-table	MAC アドレステーブルをクリアします。
clear mcagt	MCAGT エージェントをクリアします。
clear policy-map-counters	ポリシーマップのカウンタをクリアします。
clear sflow	sFlow の設定データをクリアします。
clear spanning-tree	Spanning Tree Protocol（STP）の設定データをクリアします。
clear vrrp	Virtual Router Redundancy Protocol（VRRP）の設定データをクリアします。
configure	コンフィグレーションアクセスモードに移行します。
copy	データをコピーします。
debug	デバッグオプションを設定します。
delete	指定されたファイルを削除します。
dir	ディレクトリリストを表示します。
dot1x	IEEE 802.1X ポートベースのアクセス制御オプションを実行します。
exit	トップレベルに出て必要に応じてコマンドを実行します。
fips	FIPS 関連の操作を実行します。
help	ヘルプ情報を提供します。
history	履歴ログのサイズを設定します。
logout	現在のログインセッションを終了します。
mac-rebalance	ポートチャネル上の MAC をリバランスします。
ping	ping コマンドを実行します。
quit	現在のセッションを終了します。

表 33-1 特権実行モードでサポートされていないコマンド（続き）

コマンド名	コマンド説明
rename	ファイル名をリネームします。
reload	システムを再起動します。
resequence	リストを再オーダーします。
send	一つの端末または、すべてのユーザにメッセージを送信します。
terminal	ターミナルプロパティを設定します。
show arp	Address Resolution Protocol（ARP）設定を表示します。
show bpdu-drop	Bridge Protocol Data Unit（BPDU）ガード設定を表示します。
show cee maps	CEE マップを表示します。
shor cipherset	LDAP および SSH のための暗号を表示します。
show cli	CLI セッションパラメータを表示します。
show clock	日付・時刻設定を表示します。
show debug arp	ARP パケットのデバッグ情報を表示します。
show diag	診断情報を表示します。
show dot1x	IEEE 802.1X ポートベースアクセス制御の設定データを表示します。
show edge-loop-detection globals	システム全体のエッジループ検出ステータス情報を表示します。
show file	ファイルの内容を表示します。
show history	コマンド履歴を表示します。
show interface	インタフェースステータスと設定を表示します。
show ip	Internet Protocol（IP）を表示します。
show lacp counter	Link Aggregation Control Protocol（LACP）カウンタを表示します。
show lldp	Link Layer Discovery Protocol（LLDP）設定データを表示します。
show monitor	インタフェースステータスと設定を表示します。
show netconf-state	NTECONF 統計を表示します。
show ntp	活動中の NTP サーバを表示します。
show parser dump	パーサーダンプを表示します。
show policy-map	設定されたレート制限ポリシーマップを表示します。
show port	ポートパラメータを表示します。
show port-channel	ポートチャネル設定を表示します。
show port-profile	ポートプロファイルの設定を表示します。
show qos	Quality of Service（QoS）設定を表示します。
show running-config	実行コンフィギュレーションを表示します。
show sflow	sFlow 設定を表示します。
show spanning-tree	スパニングツリー設定を表示します。
show ssm	スイッチサービスサブシステムを表示します。
show startup- db	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 storm-control	ストーム制御の設定を表示します。
show statistics	アカウンティング情報を表示します。
show system	ランタイムシステム情報を表示します。
show rmon	Remote Monitoring Protocol（RMON）の設定を表示します。
show vcs	VCS 情報を表示します。
show vlan	VLAN 設定を表示します。
show mac-address-table	MAC アドレステーブルを表示します。
show startup-config	スタートアップ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 zoning	ゾーニング情報を表示します。
Traceroute	traceroute コマンドを実行します。

表 31-2 グローバルコンフィグレーションモードでサポートされていないコマンド

コマンド名	コマンド説明
abort	現在のコンフィギュレーションセッションを中止します。
diag	診断コマンドを管理します。
do	グローバルコンフィギュレーションモードで運用コマンドを実行します。
end	現在のコンフィギュレーションセッションを終了します。
exit	現在のモードから退出します。
help	ヘルプ情報を提供します。
Pwv	現在のモードパスを表示します。
Service	パスワード暗号化サービスを実行します。
Top	トップレベルに出て、オプションでコマンドを実行します。
no vlan	VLAN コマンドを無効にします。

32 サポートされているタイムゾーンと地域

Network Time Protocol（NTP）によってサポートされているタイムゾーンと地域を次の表に示します。

- アフリカ（Africa）－360 ページの表 32-1 に示します。
- アメリカ（America）－361 ページの表 32-2 に示します。
- 南極大陸（Antarctica）－362 ページの表 32-3 に示します。
- 北極（Arctic）－362 ページの表 32-4 に示します。
- アジア（Asia）－362 ページの表 32-5 に示します。
- 大西洋（Atlantic）－363 ページの表 32-6 に示します。
- オーストラリア（Australia）－363 ページの表 32-7 に示します。
- ヨーロッパ（Europe）－363 ページの表 32-8 に示します。
- インド（Indian）－364 ページの表 32-9 に示します。
- 太平洋（Pacific）－364 ページの表 32-10 に示します。

32.1 アフリカ（Africa）

表 32-1 アフリカの地域/都市タイムゾーン

Africa/Ouagadougou	Africa/Conakry	Africa/Sao_Tome
Africa/Bujumbura	Africa/Malabo	Africa/Mbabane
Africa/Porto-Novo	Africa/Bissau	Africa/Ndjamena
Africa/Gaborone	Africa/Nairobi	Africa/Lome
Africa/Kinshasa	Africa/Monrovia	Africa/Tunis
Africa/Lubumbashi	Africa/Maseru	Africa/Dar_es_Salaam
Africa/Bangui	Africa/Tripoli	Africa/Kampala
Africa/Brazzaville	Africa/Casablanca	Africa/Johannesburg
Africa/Abidjan	Africa/Bamako	Africa/Lusaka
Africa/Douala	Africa/Nouakchott	Africa/Harare
Africa/Djibouti	Africa/Blantyre	
Africa/Algiers	Africa/Maputo	
Africa/Cairo	Africa/Windhoek	
Africa/El_Aaiun	Africa/Niamey	
Africa/Asmara	Africa/Lagos	
Africa/Ceuta	Africa/Kigali	
Africa/Addis_Ababa	Africa/Khartoum	
Africa/Libreville	Africa/Freetown	
Africa/Accra	Africa/Dakar	
Africa/Banjul	Africa/Mogadishu	

32.2　アメリカ（America）

表 32-2　アメリカの地域/都市タイムゾーン

America/Antigua	America/Guatemala	America/Edmonton
America/Anguilla	America/Guyana	America/Cambridge_Bay
America/Curacao	America/Tegucigalpa	America/Yellowknife
America/Argentina/Buenos_Aires	America/Port-au-Prince	America/Inuvik
America/Argentina/Cordoba	America/Guadeloupe	America/Dawson_Creek
America/Argentina/San_Luis	America/Jamaica	America/Vancouver
America/Argentina/Jujuy	America/St_Kitts	America/Whitehorse
America/Argentina/Tucuman	America/Cayman	America/Thunder_Bay
America/Argentina/Catamarca	America/St_Lucia	America/Iqaluit
America/Argentina/La_Rioja	America/Marigot	America/Pangnirtung
America/Argentina/San_Juan	America/Adak	America/Resolute
America/Argentina/Mendoza	America/Martinique	America/Rankin_Inlet
America/Argentina/Rio_Gallegos	America/Montserrat	America/Winnipeg
America/Argentina/Ushuaia	America/Mexico_City	America/Rainy_River
America/Aruba	America/Cancun	America/Regina
America/Barbados	America/Merida	America/Montevideo
America/St_Barthelemy	America/Monterrey	America/St_Vincent
America/La_Paz	America/Mazatlan	America/Caracas
America/Noronha	America/Chihuahua	America/Tortola
America/Belem	America/Hermosillo	America/St_Thomas
America/Fortaleza	America/Tijuana	America/New_York
America/Recife	America/Managua	America/Detroit
America/Araguaina	America/Panama	America/Kentucky/Monticello
America/Maceio	America/Lima	America/Indiana/Indianapolis
America/Bahia	America/Miquelon	America/Indiana/Vincennes
America/Sao_Paulo	America/Puerto_Rico	America/Indiana/Knox
America/Campo_Grande	America/Asuncion	America/Indiana/Winamac
America/Cuiaba	America/Paramaribo	America/Indiana/Marengo
America/Santarem	America/El_Salvador	America/Indiana/Vevay
America/Porto_Velho	America/Grand_Turk	America/Chicago
America/Boa_Vista	America/Swift_Current	America/Indiana/Tell_City
America/Manaus	America/Dawson	America/Indiana/Petersburg
America/Eirunepe	America/Santiago	America/Menominee
America/Rio_Branco	America/Bogota	America/North_Dakota/Center
America/Nassau	America/Costa_Rica	America/North_Dakota/New_Salem
America/Belize	America/Havana	America/Denver
America/St_Johns	America/Dominica	America/Boise
America/Halifax	America/Santo_Domingo	America/Shiprock
America/Glace_Bay	America/Guayaquil	America/Phoenix
America/Moncton	America/Grenada	America/Los_Angeles
America/Goose_Bay	America/Cayenne	America/Anchorage
America/Blanc-Sablon	America/Godthab	America/Juneau
America/Montreal	America/Danmarkshavn	America/Yakutat
America/Toronto	America/Scoresbysund	America/Nome
America/Nipigon	America/Thule	America/Port_of_Spain

32.3　南極大陸（Antarctica）

表 32-3　南極大陸の地域/都市タイムゾーン

Antarctica/McMurdo	Antarctica/Mawson	Antarctica/Vostok
Antarctica/South_Pole	Antarctica/Davis	Antarctica/DumontDUrville
Antarctica/Rothera	Antarctica/Casey	Antarctica/Syowa

32.4　北極（Arctic）

表 32-4　北極の地域/都市タイムゾーン

Arctic/Longyearbyen

32.5　アジア（Asia）

表 32-5　アジアの地域/都市タイムゾーン

Asia/Dubai	Asia/Tokyo	Asia/Gaza
Asia/Kabul	Asia/Bishkek	Asia/Qatar
Asia/Yerevan	Asia/Phnom_Penh	Asia/Yekaterinburg
Asia/Baku	Asia/Pyongyang	Asia/Omsk
Asia/Dhaka	Asia/Seoul	Asia/Novosibirsk
Asia/Bahrain	Asia/Kuwait	Asia/Krasnoyarsk
Asia/Brunei	Asia/Almaty	Asia/Irkutsk
Asia/Thimphu	Asia/Qyzylorda	Asia/Yakutsk
Asia/Shanghai	Asia/Aqtobe	Asia/Vladivostok
Asia/Harbin	Asia/Aqtau	Asia/Sakhalin
Asia/Chongqing	Asia/Oral	Asia/Magadan
Asia/Urumqi	Asia/Vientiane	Asia/Kamchatka
Asia/Kashgar	Asia/Beirut	Asia/Anadyr
Asia/Nicosia	Asia/Colombo	Asia/Riyadh
Asia/Tbilisi	Asia/Rangoon	Asia/Singapore
Asia/Hong_Kong	Asia/Ulaanbaatar	Asia/Damascus
Asia/Jakarta	Asia/Hovd	Asia/Bangkok
Asia/Pontianak	Asia/Choibalsan	Asia/Dushanbe
Asia/Makassar	Asia/Macau	Asia/Dili
Asia/Jayapura	Asia/Kuala_Lumpur	Asia/Ashgabat
Asia/Jerusalem	Asia/Kuching	Asia/Taipei
Asia/Kolkata	Asia/Katmandu	Asia/Samarkand
Asia/Baghdad	Asia/Muscat	Asia/Tashkent
Asia/Tehran	Asia/Manila	Asia/Ho_Chi_Minh
Asia/Amman	Asia/Karachi	Asia/Aden

32.6　大西洋（Atlantic）

表 32-6　大西洋の地域/都市タイムゾーン

Atlantic/Bermuda	Atlantic/Faroe	Atlantic/Azores
Atlantic/Cape_Verde	Atlantic/South_Georgia	Atlantic/St_Helena
Atlantic/Canary	Atlantic/Reykjavik	
Atlantic/Stanley	Atlantic/Madeira	

32.7　オーストラリア（Australia）

表 32-7　オーストラリアの地域/都市タイムゾーン

Australia/Lord_Howe	Australia/Sydney	Australia/Darwin
Australia/Hobart	Australia/Brisbane	Australia/Perth
Australia/Currie	Australia/Lindeman	Australia/Eucla
Australia/Melbourne	Australia/Adelaide	

32.8　ヨーロッパ（Europe）

表 32-8　ヨーロッパの地域/都市タイムゾーン

Europe/Andorra	Europe/Gibraltar	Europe/Warsaw
Europe/Tirane	Europe/Athens	Europe/Lisbon
Europe/Vienna	Europe/Zagreb	Europe/Bucharest
Europe/Mariehamn	Europe/Budapest	Europe/Belgrade
Europe/Sarajevo	Europe/Dublin	Europe/Kaliningrad
Europe/Brussels	Europe/Isle_of_Man	Europe/Moscow
Europe/Sofia	Europe/Rome	Europe/Volgograd
Europe/Minsk	Europe/Jersey	Europe/Samara
Europe/Zurich	Europe/Vaduz	Europe/Stockholm
Europe/Prague	Europe/Vilnius	Europe/Ljubljana
Europe/Berlin	Europe/Luxembourg	Europe/Bratislava
Europe/Copenhagen	Europe/Riga	Europe/San_Marino
Europe/Tallinn	Europe/Monaco	Europe/Istanbul
Europe/Madrid	Europe/Chisinau	Europe/Kiev
Europe/Helsinki	Europe/Podgorica	Europe/Uzhgorod
Europe/Paris	Europe/Skopje	Europe/Zaporozhye
Europe/London	Europe/Malta	Europe/Simferopol
Europe/Guernsey	Europe/Amsterdam	Europe/Vatican
Europe/Oslo		

32.9 インド（Indian）

表 32-9 インドの地域/都市タイムゾーン

Indian/Cocos	Indian/Antananarivo	Indian/Mahe
Indian/Christmas	Indian/Mauritius	Indian/Kerguelen
Indian/Chagos	Indian/Maldives	Indian/Mayotte
Indian/Comoro	Indian/Reunion	

32.10 太平洋（Pacific）

表 32-10 太平洋の地域/都市タイムゾーン

Pacific/Pago_Pago	Pacific/Kwajalein	Pacific/Palau
Pacific/Rarotonga	Pacific/Saipan	Pacific/Guadalcanal
Pacific/Easter	Pacific/Noumea	Pacific/Fakaofo
Pacific/Galapagos	Pacific/Norfolk	Pacific/Tongatapu
Pacific/Fiji	Pacific/Nauru	Pacific/Funafuti
Pacific/Truk	Pacific/Niue	Pacific/Johnston
Pacific/Ponape	Pacific/Auckland	Pacific/Midway
Pacific/Kosrae	Pacific/Chatham	Pacific/Wake
Pacific/Guam	Pacific/Tahiti	Pacific/Honolulu
Pacific/Tarawa	Pacific/Marquesas	Pacific/Efate
Pacific/Enderbury	Pacific/Gambier	Pacific/Wallis
Pacific/Kiritimati	Pacific/Port_Moresby	Pacific/Apia
Pacific/Majuro	Pacific/Pitcairn	