BladeSymphony 10Gb DCB スイッチ

Network OS 管理者ガイド

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 2.0 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　　５月　（第４版）

■著作権

目　次

図一覧

表一覧

1 Network OS と VCS™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
  virtual cluster switching を含む Brocade VCS™テクノロジ、ファブリックベースのレイヤ２イーサネットテクノロジは、自動プロビジョニング及び自己修復機能を備えた次世代仮想化データセンタでのネットワーク管理を簡略化します。
  概要は 18 ページの『1.2　VCS』を参照下さい。VCS テクノロジの詳細は、94 ページの『11 ファブリック管理』を参照下さい。
- 高い回復力
  VCS ベースの分散コンピューティングサービスは、実績のあるリンクステートルーティングを使ってネットワークの回復力を改善します。
- ネットワーク利用率の改善
  Transparent Interconnection of Lots of Links (TRILL)-based Layer 2 ルーティングサービスは、ネットワークにコストと等価なマルチパスを提供し、結果、ネットワークの利用率を改善します。
  TRILL に関する追加情報は、94 ページの『11.1　TRILL』を参照下さい。
- 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設定を行い、ポートプロファイルの転送を行い、Virtual Machine (VM)の可動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、101 ページの『12 AMPP の設定』を参照下さい。

Network OS では、全ての機能が単一の業界標準のコマンドラインインタフェース(CLI)で設定できます。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 VCS 用語

次の言葉がこのドキュメントでは使われます。

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互いに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)	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。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る。ISL は単一リンクもしくは Brocade 独自のハードベースのトランクとなる。
RBridge	イーサ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、イーサネット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、97 ページの『11.3 VCS ファブリックの構成』を参照下さい。
VCS ID	イーサネット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。イーサネットファブリックの全てのスイッチは、同じ VCS ID を持たなければならない。
WWN World Wide Name	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 VCS テクノロジ イントロダクション

Brocade VCS 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。VCS 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を可能とします。

VCS テクノロジは次のコンセプトに基づいています。

- イーサネットファブリック
- 分散インテリジェンス
- ロジカルシャーシ

２つ以上の VCS モードの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、互い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。VCS 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規模を容易に拡大できます。

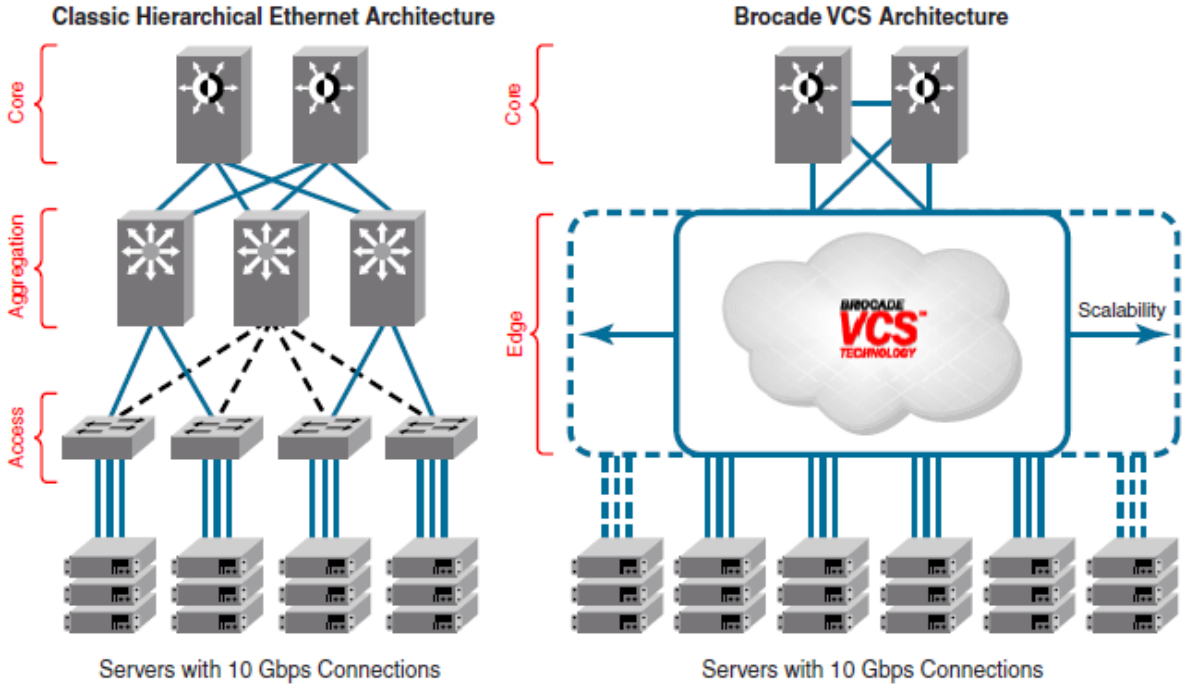

図 1-1 従来のイーサネットと VCS アーキテクチャの比較

1.2.1　イーサネットファブリック

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。

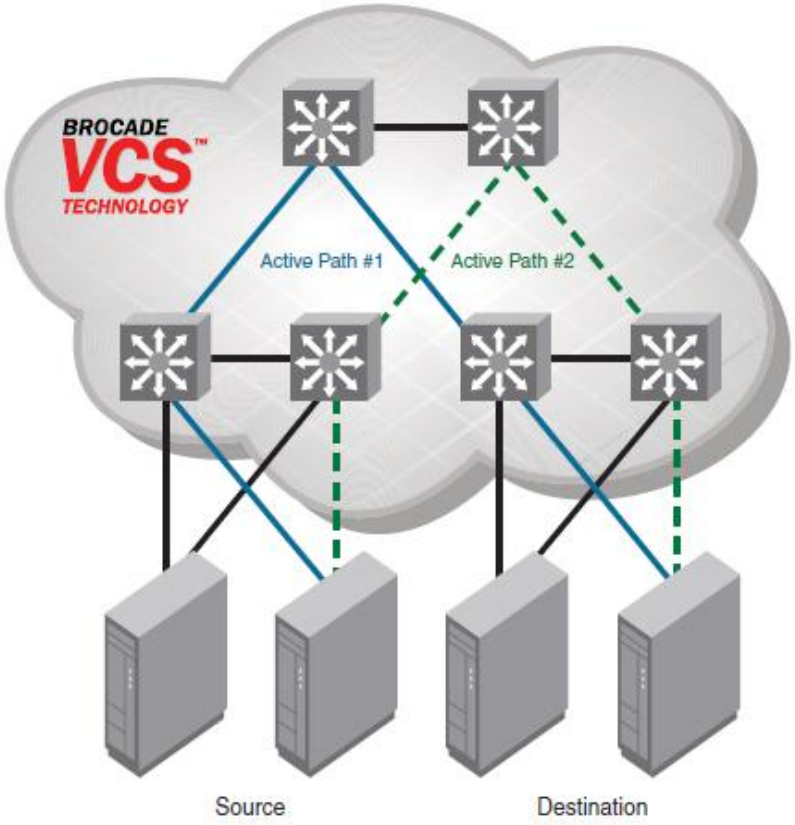

図 1-2 レイヤ2マルチパスを持ったイーサネットファブリック

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。
- 接続されるファブリックのメンバーやデバイスは、常にお互いを認識しています。
- ファブリック内の全てのパスが利用可能です。トラフィックは、常にコストに見合ったパス間に分散されます。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。
- トラフィックは最も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、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スイッチされます。

1.2.2　分散インテリジェンス

VCS テクノロジを使うと、全ての意味のある情報は、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スイッチの各メンバーに自動的に分散されます。例えば、サーバが最初にファブリックに接続すると、ファブリック内の全てのスイッチはそのサーバについて学習します。このように、ファブリックに必要となる手動の再設定を行うことなく、ファブリックスイッチが追加されたり削除されたりして、物理または仮想サーバが再配置されます。

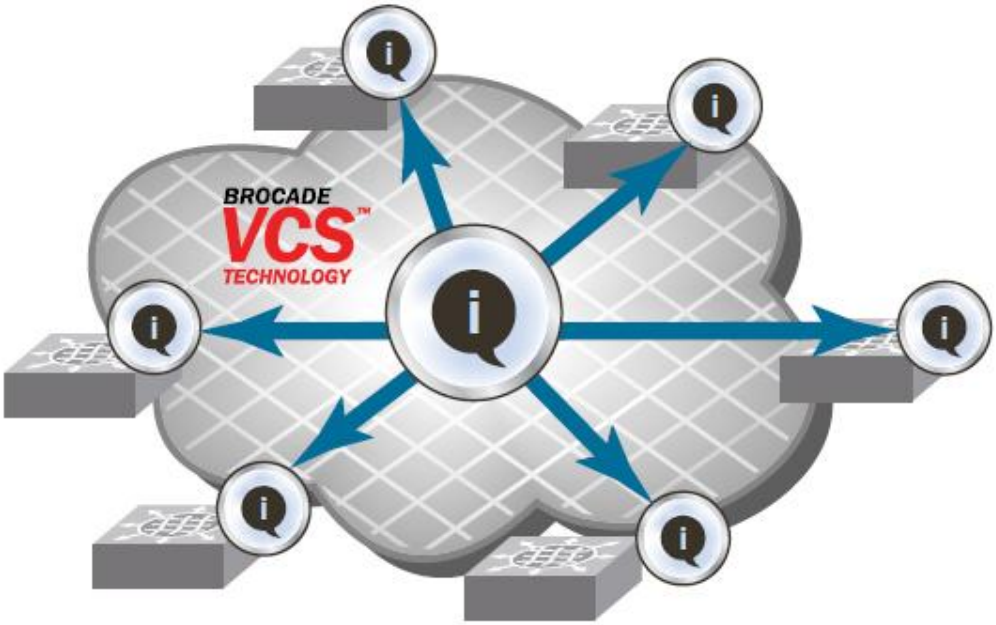

図 1-3 イーサファブリック内の分散インテリジェンス

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、Virtual Machines (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にあるかの様に管理されます。外部のネットワークに対して、ファブリックは他のスイッチと全く異なって見えます。図 1-4 は、２つのシャーシをもつ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。

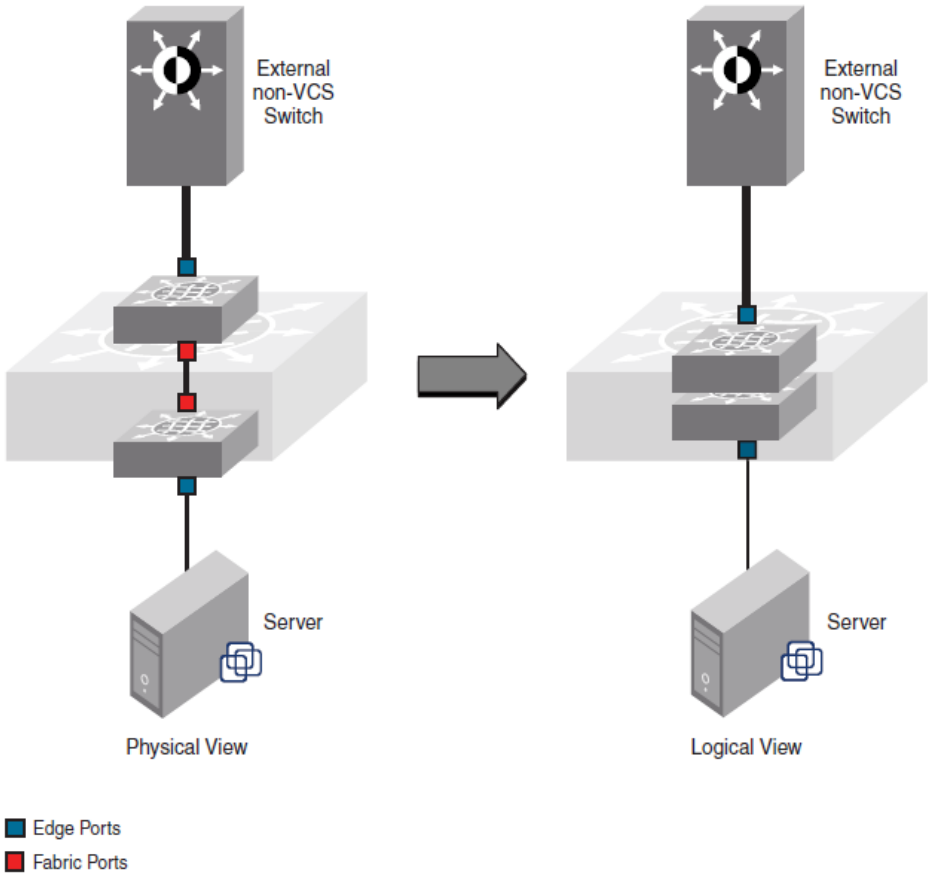

図 1-4 イーサファブリック内のロジカルシャーシ

ファブリック内の各物理スイッチは、シャーシ内のブレード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、最小のユーザ設定でイーサネットファブリックを形成することを補助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、94 ページの『11.2　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、97 ページの『11.3　VCS ファブリックの構成』を参照下さい。

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 の変更に関する情報は、97 ページの『11.3　VCS ファブリックの構成』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。ポートが同じポートグループに所属している時だけトランクが形成されます。これらのトランクを形成するために、ユーザ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、98 ページの『11.5　ファブリック ISL の設定』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決定します。もし競合していると、Principal RBridge は参加した RBridge は分離されたままとなります。
RBridge ID の設定に関する情報は、97 ページの『11.3　VCS ファブリックの構成』を参照下さい。

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、デフォルトの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 管理モードとなります。Network OS 管理モードから CLI コマンドを使って情報を得るには、ページ 25 の『2.1.5 Network OS CLI command modes』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。
(1) 特権モードでの 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、66 ページの『9.1 ロール管理』を参照下さい。

2.1.3 デフォルトのロール

デフォルトのロールの属性は、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ることです。全てのコマンド(CLI)は管理者ロールに関連付けられたユーザが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。
- ユーザのロールは、特権実行モードではほとんど show コマンドに限定されているという制限された権限をとなります。ユーザアカウントは、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か Telnet セッションの何れも同じで、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 V2.0.1 は 32 セッションまでサポートしています。

2.1.5　Network OS CLI command modes

図 2-1 に Network OS CLI コマンドモード階層を示します。

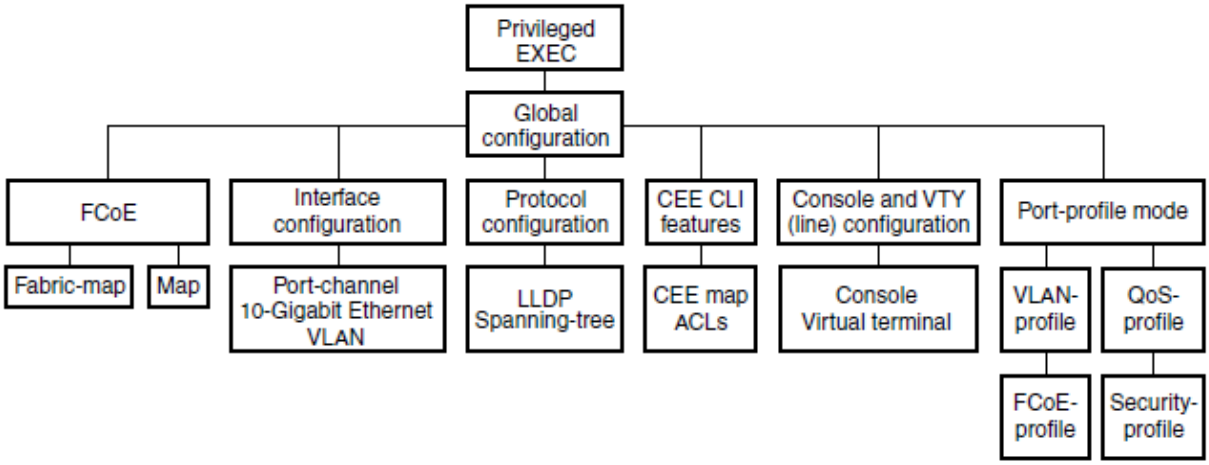

図 2-1 Network OS CLI コマンドモード階層

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。
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実行 • 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実行 • 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
Feature configuration	Standard ACL: switch(conf-macl-std)# Extended ACL: switch(conf-macl-ext)#	グローバルコンフィグレーションモードから次のコマンド実行 • mac access-list standard • mac access-list extended	ACL の表示設定。

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。本装置では、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、クエスチョンマーク('?')に続いてキーワード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 コマンド出力フィルタ(output modifiers)

Network OS CLI は表 2-3 に示すコマンド出力フィルタが使用できます。コマンドに、これらのフィルタを付加するためにパイプ文字('|')を使用してください。

表 2-3 Network OS CLI コマンド出力フィルタ

出力フィルタ	説　明
Begin	指定された表現で始まるコマンド出力を表示します。
count	コマンド出力の行数を表示します。
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。
include	指定された表現を含むコマンド出力を表示します。
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。
Until	指定した表現の行に到達するまでコマンド出力を表示します。

3 スイッチ管理の基本

3.1 スイッチに接続する

本装置に接続するには、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、33 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、33 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 アドレスやスイッチ ID、ブリッジ ID、ホスト名称やシャーシ名称で識別されま

す。'switch-attributes'コマンドでホスト名称やシャーシ名称をカスタマイズできます。

- ホスト名称は３０文字までです。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。ホスト名称は、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称を割り当てるなら、システムログはシャーシ名称でスイッチを識別できます。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．'switch-attributes'コマンドに続いて switch ID を入力します。
3．'host-name'オペランドに続き、ホスト名を入力します。
4．'copy running-config file startup-config'コマンドを使って、変更を格納します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# switch-attributes 2
switch(config-switch-attributes-2)# host-name lab1_vdx0023
switch(config-switch-attributes-2)# exit
switch(config)# do copy running-config startup-config
switch(config)# do show running-config switch-attributes 2
switch-attributes 2
  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．'switch-attributes'コマンドに続いて switch ID を入力します。
3．'chassis-name'オペランドに続いて、シャーシ名を入力します。
4．'copy running-config file startup-config'コマンドを使って、変更を格納します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# switch-attributes 2
switch(config-switch-attributes-2)# chassis-name lab1_vdx0023
switch(config)# do copy running-config startup-config
switch(config)# do show running-config switch-attributes 2
switch-attributes 2
```

```
chassis-name lab1_vdx0023
host-name lab1_vdx0023
```

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 command'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。
'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。

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。

3.5 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ポートです。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

もーつの IP アドレスを設定します。また、IPv4 フォーマットでの静的アドレス設定や自動的に IPv4 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。IPv6 アドレスに対しては、Network OS v2.0.1 では静的アドレスやステートレス自動設定の両方をサポートしています。
静的 IPv4 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 IPv4 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設定されて無い場合は、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、35 ページの『3.5.2　DHCP を使った IPv4 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、'configure terminal'コマンドを入力します。
4．DHCP 機能を無効化するために、'no 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．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、'gateway-address'コマンドを実行します。

NOTE
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)# ip gateway-address 10.24.80.1
```

3.5.2　DHCP を使った IPv4 アドレスの設定

デフォルトでは、DHCP は無効です。’ip address dhcp'コマンドを使ってサービスを有効化しなければなりません。Netowork 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。' no ip address dhcp'コマンドを使って DHCP を無効化してください。

NOTE
DHCP が有効になると、静的な IPv4 アドレス設定は削除されます。

3.5.3 IPv6 イーサネットアドレスの設定

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．' interface Management switchID/0'コマンドを入力します。
3．' ipv6 address IPv6_addresss/prefix_length 'コマンドを入力します。

```
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
```

3.5.4 ステートレス IPv6 の自動設定

IPv6 プロトコルは各ネットワークインタフェースに複数の IP アドレスを割り当てることが出来ます。各インタフェースは、ほとんどのケースでローカルアドレスが設定されます。しかし、このアドレスは同一サブネットのホストにしかアクセスできません。更に広域にアクセス可能にするため、一般的にはインタフェースには少なくとも一つのグローバルな IPv6 アドレスが割り当てられます。IPv6 自動設定は、更に多くの IPv6 アドレスを割り当てることが可能で、その数はローカルネットワークに接続されているルータの数や、それらルータが広告しているプレフィックスの数に依存しています。
IPv6 自動設定が有効な場合、本装置はステートレス IPv6 自動設定状態となります。また、IPv6 自動設定が無効な場合、本装置は IPv6 自動設定が有効だった間に得られた IPv6 アドレスの利用を中止します。またこの有効/無効の状態により、各管理エンティティに対するローカルアドレスの利用を有効もしくは無効となります。なぜならば、これらのローカルアドレスはルーター検索のために必要とされるからです。
自動設定の有効・無効状態は、生成されるどの静的 IPv6 アドレスにも影響しません。ステートレス IPv6 自動設定と静的 IPv6 アドレスは共存することができます。

3.5.5 IPv6 自動設定機能の設定

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．IPv6 自動設定を有効にするか無効にするかにより、いずれかの設定を行います。

- 対象プラットフォームの全ての管理ポートに対する IPv6 自動設定を有効にするために、'ipv6 address autoconfig'コマンドを使います。
- 対象プラットフォームの全ての管理ポートに対する IPv6 自動設定を無効にするために、'no ipv6 address autoconfig'コマンドを使います。

3.5.6　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 running-config 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 running-config interface Management 1/0
interface Management 1/0
 no ip address dhcp
 ip address 10.24.85.81/20
 ip gateway-address 10.24.80.1
 ipv6 address fd00:60:69bc:832:e61f:13ff:fe67:4b94/64
 no ipv6 address autoconfig
```

3.5.7　管理インタフェースの速度の設定

デフォルトでは、インタフェースの速度は自動設定となっています。これは、負荷やその他の要素により動的に最適化されることを意味しています。このデフォルト値は、10Mbps/全二重もしくは 100Mbps/全二重の固定速度に変更することが可能です。

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．switchID/0 を引数として'interface management'コマンドを入力します。
3．オプションを表示するために、'?'マークと共に’speed'コマンドを入力します。
4．パラメータを選択肢、再度’speed'コマンドを入力します。
5．新しい設定を表示するために、' show running-config interface management 'コマンドを入力します。
6．'copy running-config startup-config'コマンドを使って、変更を格納します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# interface Management 1/0
switch(config-Management-1/0)# speed ?
switch(config-Management-1/0)# speed 100
switch(config-Management-1/0)#exit
switch(config)# do show running-config interface Management 1/0
interface Management 1/0
 no ip address dhcp
 ip address 10.24.85.81/20
 ip gateway-address 10.24.80.1
 ipv6 address ""
 no ipv6 address autoconfig
 speed 100
!
switch(config)# do copy running-config startup-config
switch(config)# do show interface Management 1/0
ip address 10.20.49.112/20
ip gateway-address 10.20.48.1
ipv6 ipv6_address [  ]
ipv6 ipv6_gateways [ fe80::21b:edff:fe0b:2400 ]
LineSpeed Actual "100 Mbit, Duplex: Full"
LineSpeed Configured "100 Mbit, Duplex: Full"
```

3.6 インバンド管理インタフェースの設定

インバンド管理は、パネルのイーサネットポートでレイヤ３での管理端末との通信を可能とするものです。この目的は、アウトバンドの管理インタフェースが使えないような場合に、ファームウェアのダウンロード、トラブルシューティングやスイッチ設定のような管理タスクのためです。管理端末は、SSH、SCP または Telnet を使って接続することができます。インバンド管理は次に示すインタフェースで利用可能です。

- VLAN
- 物理ポート
- 論理ポート(Port channel インタフェース)

インバンド管理を実現するために、IP 通信とサブネットを理解しなければなりません。インバンド管理用に設定されたフロントパネルのポートは、内部のプロセッサと外部ポートを経由して管理端末と通信できるよう IP 転送機能を持ったルータとして動作します。管理端末の IP アドレスとイーサネットポートの IP アドレスは、図 3-1 に示すように同一サブネットになければなりません。

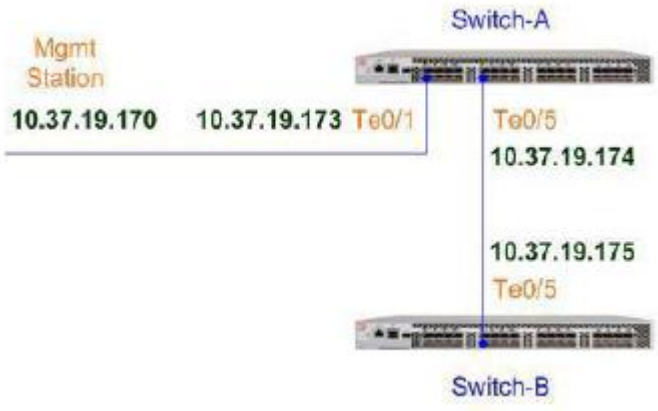

図 3-1 インバンド管理時の接続例

図 3-1 に示す構成では、次の操作が可能です。

- 管理端末から Switch-A に SSH または Telnet での接続
- Switch-A から Switch-B に SSH または Telnet での接続
- 管理端末から Switch-A へ secure copy(SCP)を使ってのファイル転送
- Switch-A から Switch-B へ secure copy(SCP)を使ってのファイル転送

3.6.1 インバンド管理インタフェースの設定

1. シリアルコンソールか管理インタフェース経由でスイッチに接続します。
2. '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。
3. 'interface'コマンドに続いて、設置したいインタフェースタイプを指定します。
4. 'ip address <IPv4_address>/<prefix_length>'コマンドを使ってインタフェースに IPv4 アドレスを設定します。
5. 'ip mtu'コマンドを使って、バイト単位で MTU サイズを指定します。
6. 'arp-ageing-timeout'コマンドで、インタフェースの ARP タイムアウト時間を設定します。
7. 未使用の ARP エントリーを削除するため、'no-refresh'オプションを指定して、'clear-arp-cache'コマンドで ARP キャッシュをクリアします。
8. 'ip proxy-arp'コマンドで、インタフェース毎の Proxy ARP を設定します。
9. 'show ip interface'コマンドで、設定を表示します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# interface Vlan 2
switch(config-Vlan-2)# ip address 1.1.1.1/24
switch(config-Vlan-2)# ip mtu 1200
switch(config-Vlan-2)# arp-ageing-timeout 300
switch(config-Vlan-2)# clear-arp-cache no-refresh
switch(config-Vlan-2)# ip proxy-arp
switch(config-Vlan-2)# exit

switch# show ip interface Vlan 2
Vlan 2 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 unreachablesare always sent
ICMP mask replies are never sent
IP fast switching is enabled
```

3.7 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。

3.7.1 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。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、『Netowrk 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
```

3.7.2 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 を採取する前に、最初にグローバルコンフィグ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、障害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。

3.8 syslog サーバの設定

syslog デーモン(syslogd)は、システムメッセージロギングのための IP ベースのサービスです。
syslog デーモンは UNIX と Linux OS の一部です。
システムイベントとエラーメッセージをリモートサーバのログファイルに転送することが出来ます。サーバは、UNIX、Linux または標準的な syslogd 機能をサポートした OS でなければなりません。
syslog メッセージの転送を設定する際には、IPv4 形式でサーバの IP アドレスを設定します。

3.8.1 syslog サーバの追加

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．'logging syslog-server'コマンドを使ってとサーバの IP アドレスを指定します。
3．サーバを追加する場合は、別のサーバ IP アドレスを使ってコマンドを繰り返します。
4．'do show running-config logging syslog-server'コマンドを使って、設定を確認します。

```
switch#configure terminal
Entering configuration mode terminal
switch(config)# logging syslog-server 192.168.163.233
switch(config)# logging syslog-server 192.168.163.234
switch(config)# logging syslog-server 192.168.163.235
switch(config)# logging syslog-server 192.168.163.236
switch(config)# do show running-config logging syslog-server
logging syslog-server 192.168.163.233
logging syslog-server 192.168.163.234
logging syslog-server 192.168.163.235
logging syslog-server 192.168.163.236
```

NOTE
'logging syslog-server'コマンドは、IPv4 アドレスのみサポートしています。サーバは最大４つまで指定できます。

3.8.2 syslog サーバの削除

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．'no logging syslog-server'コマンドを使って、サーバの IP アドレスを指定します。
3．'do show running-config logging syslog-server'コマンドを使って設定を確認します。

```
switch#configure terminal
Entering configuration mode terminal
switch(config)# no logging syslog-server 192.168.163.236
switch(config)# do show running-config logging syslog-server
logging syslog-server 192.168.163.233
logging syslog-server 192.168.163.234
logging syslog-server 192.168.163.235
```

3.9 RASlog コンソールの設定

RASlog メッセージは、重要度を設定することによってフィルタされたシステムイベントを記録します。各メッセージは、タイムスタンプ、メッセージＩＤ、シーケンス番号、重要レベル、シャーシ名とメッセージで構成されます。RASlog コンソールは、重要度でメッセージをフィルタしたり、スイッチ上のメッセージを表示したり、全てのメッセージをクリアすることができます。更に詳細な情報は、『Network OS Message Reference』を参照下さい。

3.9.1 RASlog 情報の表示

RASlog メッセージを表示するために、'show logging raslog'コマンドを使用します。次に例を示します。

```
switch# show logging raslog
NOS: v2.0.0

2000/03/11-20:12:03, [NSM-2006], 13187,, INFO, AMPP_SK_112, Port-profile aa1
removed successfully on TenGigabitEthernet 2/0/17

2000/03/11-20:12:24, [NSM-2004], 13188,, INFO, AMPP_SK_112, Port-profile aa1
application succeeded on TenGigabitEthernet 2/0/17

2000/03/11-20:15:56, [HIL-1404], 13189,, WARNING, Brocade8000, 1 fan FRUs
missing. Install fan FRUs immediately.

2000/03/11-20:19:33, [NSM-2006], 13190,, INFO, AMPP_SK_112, Port-profile aa1
removed successfully on TenGigabitEthernet 2/0/14

2000/03/11-20:26:02, [HIL-1404], 13191,, WARNING, Brocade8000, 1 fan FRUs
missing. Install fan FRUs immediately.

2000/03/11-20:26:03, [NSM-2004], 13192,, INFO, AMPP_SK_112, Port-profile aa1
application succeeded on TenGigabitEthernet 2/0/14

2000/03/11-20:31:33, [NSM-2006], 13193,, INFO, AMPP_SK_112, Port-profile aa1
removed successfully on TenGigabitEthernet 2/0/14
(output truncated)
```

3.9.2 RASlog 重要度フィルタの設定

RASlog メッセージをフィルタするために、INFO(デフォルト)、WARNIG、ERROR、CRITICAL のうちから重要度の一つを選択します。キーワードは大文字で指定します。設定された重要度は、レポートする閾値を決めます。設定された重要度以上の全てのメッセージが表示されます。

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．'logging switchid switchID raslog console'を使って、重要度を指定します。
3．'copy running-config startup-config'コマンドを使って、変更をセーブします。

```
switch#configure terminal
Entering configuration mode terminal
switch(config)# logging switchid 2 raslog console WARNING
switch(config)# do copy running-config startup-config
switch# show logging raslog
NOS: v2.0.0
2000/03/11-20:15:56, [HIL-1404], 13189,, WARNING, Brocade8000, 1 fan FRUs
missing. Install fan FRUs immediately.

2000/03/11-20:26:02, [HIL-1404], 13191,, WARNING, Brocade8000, 1 fan FRUs
missing. Install fan FRUs immediately.

(output truncated)
```

3.9.3 RASlog の消去

'clear logging raslog'コマンドを使ってスイッチ上の全ての RASlog メッセージを消去します。

4 レイヤ２イーサネットの概要

4.1 レイヤ２転送

レイヤ２イーサネットフレームは、ポート間で転送されます。802.1Q により、指定された VLAN に到着フレームに tag 付けできるようになります。そして、802.3ac により外部デバイスから tag 付 VLAN を受信可能となります。
Network OS は、レイヤ２スイッチ間のブリッジプロトコルである次の 802.1D を使います。そして、ループフリーなネットワーク環境を維持します。

- Spanning Tree Protocol (STP)
- Rapid Spanning Tree Protocol (RSTP)
- Multiple Spanning Tree Protocol (MSTP)
- Per-VLAN Spanning Tree (PVST+)
- Rapid Per-VLAN Spanning Tree (RPVST+)

これらのプロトコルの設定に関する詳細については、122 ページの『14 スパニングツリーの設定』を参照下さい。

スイッチハードウェアは、次に示すようにイーサネットフレームを制御します。

- 宛先 MAC アドレスが検索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く同一 VLAN に所属する全てのポートにフラッディングされます。
- 宛先 MAC アドレスが検索テーブルに登録されている場合、フレームは正しい出力ポートにだけスイッチされます。
- 宛先 MAC アドレスがテーブルに登録されている場合、出力ポートと入力ポートが同じ場合、フレームは破棄されます。
- もしイーサネットフレームチェックシーケンス(FCS)が正しくない場合、スイッチは cut-through モードで動作するため、イーサネットフレームフォーマットが正しいものは、不正な FCS のまま送出されます。
- もしイーサネットフレームが短すぎる場合、フレームは破棄されエラーカウンタがアップします。
- もしイーサネットフレームが長すぎる場合、フレームは切り取られてエラーカウンタがアップします。切り取られたフレームは、不正な FCS がついて送出されます。
- ブロードキャストフレームは入力ポートを除き同一 VLAN に属する全てのポートにフラッディングされます。
- 検索テーブルにある MAC アドレスエントリがタイムアウトした場合、それらは削除されます。このれにより、フレーム転送はユニキャストからフラッディングに変わります。
- 検索テーブルに存在する MAC アドレスは、接続されたデバイスが切り離された場合、破棄されます。デバイスの接続が変更されると、新しいポートからの入力フレームによって、検索

テーブルの古いエントリが破棄されて、新しいエントリが検索テーブルに登録されます。フレームは新しいポートへのユニキャストのままです。

- 検索テーブルが一杯になると、新しいエントリがエージングやタイムアウトに近い最も古い MAC アドレスエントリと置き換わります。通信に使われている MAC アドレスは、タイムアウトしません。

NOTE
新しいエントリは、32K エントリの検索テーブルの 90%になると古いエントリが置き換わります。

4.2 VLAN tagging

レイヤ２スイッチは、入力フレームに常に tag 付けします。もし、入力フレームが untagged の場合は、ポート設定に従って tag が付加されます。ポートは untagged トラフィックを単一 VLAN か複数 VLAN かに分類します。もし入力フレームに既に tag 付けされている場合、ポートは、設定されている VLAN 許容ルールに従って、フレームを転送か破棄します。
次は VLAN tagging の３つの例です。

- もし、ポートが入力フレームに対して単一 VLAN ID を tag 付けするように設定されていれば、untagged の入力フレームはその VLAN ID で tag 付けされます。
- もし、ポートが入力フレームに対して複数 VLAN ID を tag 付けするように設定されていれば、untagged の入力フレームはポート設定に基づいた正しい VLAN ID に tag 付けされます。
- もしポートが外部からの tag 付けフレームを受け付けるように設定されている場合は、VLAN ID で tag 付けされたフレームは変更なく通過させます。

NOTE
VLAN のコンフィグレーションの詳細については、111 ページの『13 VLAN の設定』を参照下さい。

4.3 入力フレームの分類

スイッチはハードウェアレベルで次の条件に基づき、入力レームの分類を行います。

- Port number
- Protocol
- MAC address

分類されたフレームは VLAN ID か 802.1p イーサネットプライオリティで分類されます。802.1p イーサネットプライオリティ tag はレイヤ２ Class of Service(CoS)で使われます。802.1p イーサネットプライオリティは、VLAN のフレームに、VLAN でのトラフィックを優先付けするレイヤ２ CoS 値を tag 付けします。スイッチはまたハードウェアレベルで、外部デバイスで tag 付けされ

たフレームを受け付けます。
フレームの分類は次の通りです。

- 物理ポート番号による VLAN ID とレイヤ２ CoS 値 － このオプションでは、入力フレームを分類するために、物理ポートに設定済みの VLAN ID とレイヤ２ CoS 値に設定します。
- LAG 仮想ポート番号による VLAN ID とレイヤ２ CoS 値 － このオプションでは、入力フレームを分類するために、リンクアグリゲーショングループ(LAG)の仮想ポートに設定済みの VLAN ID とレイヤ２ CoS 値に設定します。
- レイヤ２ CoS 変換 － このオプションでは、QoS 変換機能を有効化することによりレイヤ２ CoS 値設定を変更します。
- レイヤ２ CoS トラスト － このオプションでは、QoS トラスト機能を有効化することにより入力フレームのレイヤ２ CoS 値を受付けるよう設定します。

QoS の設定の詳細については、154 ページの『19 QoS の設定』を参照下さい。

4.4 輻輳制御とキューイング

本装置はハードウェアレベルで幾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。出力キューの輻輳制御として、最大リンク利用率を維持するために選択的・予測的にフレームを破棄するため Random Early Detection(RED)が使われます。入力フレームのレイヤ２ CoS 設定やポート、もしくは VLAN に設定に基づきレイヤ２ CoS フィールドを書き換えることにより入力フレームを優先キューに分類します。

本装置では、出力ポートにフレームをキューイングする際、２つのスケジューリングアルゴリズムを組み合わせることができます。絶対優先とも言われる優先キューイングと不足荷重ラウンドロビン(DWRR: Deficit Weighted Round Robin)キューイングです。
キューイング機能は次の通りです。

- RED － RED はリンク利用率を高めます。複数の TCP トラフィックストリーム入力が同一の出力ポートにスイッチされ、幾つかのトラフィックストリームは小さいフレームを、その他は大きなフレームを送信している場合、リンク利用率は 100%にはなりません。RED が有効になっていると、リンク利用率がほぼ 100%になります。
- 分類 － ユーザプライオリティの設定です。
  - 受信フレームは入力ポートに設定されたユーザプライオリティが tag 付けされています。tag は出力ポートでフレームをチェックすると見ることが出来ます。デフォルトでは、全てのフレームは優先度 0 に tag 付けされます。
  - 外部で tag 付けされたレイヤ２ふれーむ － ポートが外部で tag 付けされたレイヤ２フレームを受付けるように設定された場合、ユーザプライオリティは受信したフレームのレイヤ２ CoS 値に設定されます。
- キューイング
  - 入力キュー － 入力キューは次の方法でトラフィックフローを最適化します。ポートは幾つかの優先値で tag 付けされたトラフィックを受信し、異なる優先度設定をもったトラフ

ィックは別の出力ポートにスイッチされます。幾つかの出力ポートは既に輻輳しており、一方別のポートは輻輳していません。入力キューにおいては、輻輳していないポートへのトラフィックストリームのレートは高いままに維持されます。

- 出力キュー ― 出力キューは次に示す方法でトラフィックフローを最適化します。幾つかのポートは、異なる優先度設定を持った受信トラフィックを転送しています。全てのポートからのトラフィックは同一出力ポートにスイッチされます。もし、受信ポートが異なるトラフィックレートを持っていれば、幾つかの出力優先グループは輻輳し、一方では輻輳が発生していないままです。出力キューにおいては、輻輳していないトラフィックストリームのレートは高いままに維持されます。
- マルチキャストレートリミット ―マルチキャストレートリミットの典型的な例は、幾つかのポートが幾つかの優先度に tag 付けされた複数の受信トラフィックを転送するところです。異なる優先度を持ったトラフィックは異なる出力ポートへスイッチされます。マルチキャストレートリミットは、出力ポートのトータルのマルチキャストレートが指定されたリミットより小さくなるようにセットします。
- マルチキャスト入力キューイング ―マルチキャスト入力キューイングの典型的な例は、幾つかのポートで幾つかの優先度で tag 付けされた複数の受信トラフィックを転送しているところです。異なる優先度を持ったトラフィックは異なる出力ポートへスイッチされます。幾つかの出力ポートは既に輻輳しており、一方別のポートは輻輳していません。輻輳していないポートへのトラフィックストリームのレートは高いままに維持されます。全ての出力ポートは全ての入力ポートからのマルチキャストフレームを転送します。これは、閾値に対して、マルチキャストトラフィック分配を可能とします。
- マルチキャスト出力キューイング ― マルチキャスト出力キューイングの典型的な例は、幾つかのポートでマルチキャスト受信トラフィックを転送しているところです。各ポートは、異なる優先度が設定されています。全てのポートからのトラフィックは同一出力ポートにスイッチされます。もし受信ポートが異なるトラフィックレートならば、幾つかの出力プライオリティグループでは輻輳し、一方その他は輻輳していません。輻輳していないトラフィックストリームのレートは、高いままです。出力ポートは全ての入力ポートからのマルチキャストフレームを転送するはずです。

- スケジューリング ― スケジューリングポリシーの典型的な例は(絶対優先 0 と絶対優先 1 のモデルを使った場合)、ポート 0 から 7 でトラフィックを受信していて、それぞれのポートが一様な優先レベルを持っている場合です。全てのトラフィックは同一出力ポートにスイッチされます。絶対優先 0 のモードでは、全てのポートは DWRR スケジューリングで、全てのポートの秒当たりのフレーム数(FPS)は DWRR 設定に対応します。絶対優先 1 のモードでは、優先度 7 のトラフィックが絶対優先を使います。優先度 7 は高い FPS を実現します。同じ優先度を持った入力ポートからのフレームは、出力ポートに対してラウンドロビンでスケジュールされます。スケジューリングポリシーが設定されると、DWRR スケジューリングで使用される各プライオリティグループは、PG_Percentage パラメータで設定されるトータル帯域の割合を使うよう設定されます。

QoS の設定の詳細については、154 ページの『19 QoS の設定』を参照下さい。

4.5 アクセス制御(Access control)

Access Control Lists (ACLs)はレイヤ２スイッチでのセキュリティのために使われます。標準的な ACL は入力ポートで送信元アドレスを検査します。拡張 ACL は送信元と宛先とプロトコルによるフィルタリングが可能です。ACL はポートもしくは VLAN 単位に適用できます。
ACL の機能は、次の通りです。

- 物理ポートに設定される標準イーサネット ACL は、送信元 MAC アドレスに基づきフレームを許可か拒否するために使われます。デフォルトは全てのフレームが許可されています。
- 物理ポートに設定される拡張イーサネット ACL は、送信元 MAC アドレス、宛先 MAC アドレス、イーサタイプに基づき、フレームを許可か拒否するために使われます。デフォルトは全てのフレームが許可されています。
- LAG 仮想ポートに設定されている標準イーサネット ACL は、送信元 MAC アドレスに基づきフレームを許可か拒否するために使われます。デフォルトは全てのフレームが許可されています。LAG ACL は LAG に含まれる全てのポートに適応されます。
- LAG 仮想ポートに設定されている拡張イーサネット ACL は、送信元 MAC アドレス、宛先 MAC アドレス、イーサタイプに基づき、フレームを許可か拒否するために使われます。デフォルトは全てのフレームが許可されています。LAG ACL は LAG に含まれる全てのポートに適用されます。
- VLAN に設定される標準イーサネット ACL は、送信元 MAC アドレスに基づきフレームを許可か拒否するために使われます。デフォルトは全てのフレームが許可されています。VLAN ACL は VLAN に対する Switch Vertical Interface (SVI)に適用される。
- VLAN に設定される拡張イーサネット ACL は、送信元 MAC アドレス、宛先 MAC アドレス、イーサタイプに基づき、フレームを許可か拒否するために使われます。デフォルトは全てのフレームが許可されています。VLAN ACL は VLAN に対する Switch Vertical Interface (SVI)に適用される。

ACL の設定についての詳細は、168 ページの『18 アクセスコントロールリスト(ACL)の設定』を参照下さい。

4.6 トランキング

NOTE
イーサネットネットワークでの”トランキング”という言葉は、単一リンクまたはポートの限界を超えてリンクスピードを増やすため、更により高いアベイラビリティのため冗長性を増加させるために複数のネットワークリンク(port)使うことを示します。

802.3ad Link Aggregation Control Protocol (LACP)は、全ての個別リンクを組み合わせた帯域幅でトランクを作り出すために複数のリンクを結合するために使われます。LACP の設定の詳細については、122 ページの『15 リンクアグリゲーションの設定』を参照下さい。

NOTE
本装置では最大 24 の LAG インタフェースをサポートしています。

4.7 フロー制御

802.3x イーサネットポーズはリンクの送信端での速度で以下によるフレームドロップを回避するために使われます。スイッチもしくはホストのポートが受信可能となってない場合、多くの場合は輻輳による、送信を一時停止するため送信元にポーズフレームを送信します。輻輳が解消した場合、送信を一時停止するための送信元への要求を中止し、フレームドロップすること無しに通信を再開します。
イーサネットポーズが有効な場合、ポーズフレームは送信元に送信されます。
イーサネットポーズの設定に関する詳細な情報は、154 ページの『19 QoS の設定』を参照下さい。

5 Network Time Protocol の設定

5.1 時計設定

'ntp server'コマンドは、IPv4/IPv6 に対応しています。複数の NTP サーバを登録することができ、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、到達可能なサーバが無い場合は、スイッチローカルの時計を使用します。

NOTE
スイッチの時計は、起動時にマネジメントモジュールより設定されます。

ネットワーク時間との同期は、全てのスイッチで使われる外部の標準的なタイムサーバが使われる時にのみ保証されます。

5.1.1 外部ソースへのローカル時間の同期

'ntpserver'コマンドは NTP サーバの IP アドレスをリストに追加するために使用します。

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. 'ntp server'コマンドを入力します。

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

5.1.2 NTP サーバの削除

'no ntp server'コマンドを使って、サーバのリストから、NTP サーバの IP アドレスを削除します。

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. 'no ntp server'コマンドを入力します。

```
switch(config)# no ntp server 192.168.10.1
```

5.1.3 NTP サーバ IP アドレスの表示

'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。)
switch ID が指定されていない場合は、ローカルのスイッチに対して実行されます。
'show ntp status'コマンドを入力します。

```
switch# show ntp status [switchid id | all]
```

5.2 タイムゾーンの設定

スイッチの操作は日付や時刻設定には依存しません。しかし、正確な時刻設定は正しいログ情報や追跡に必要となります。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)となっています。
- 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。

5.2.1 時計の設定

次の手順でスイッチの日付と時刻が設定できます。NTP サーバがアクティブな場合、自動的に時計がアップデートされます。本装置の時計は、1970 年 1 月 1 日から 2038 年 1 月 19 日まで有効です。
'clock set CCYY-MM-DDTHH:MM:SS'コマンドを入力します。CCYY-MM-DDTHH:MM:SS は、年-月-日 T 時:分:秒の書式で指定します。

```
switch# clock set 2010-03-17T12:15:00
```

5.2.2 タイムゾーン設定

次の手順でタイムゾーンの設定を行います。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、一度設定するだけです。
'clock timezone region [/country|/state/] city'コマンドを入力します。

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

5.2.3 タイムゾーン設定の削除

次の手順でタイムゾーン設定を削除することが出来ます。
'no timezone'コマンドを入力します。

```
switch# no clock timezone
```

5.2.4 現在の時刻とタイムゾーンの表示

次の手順で、ローカル時刻、日付、タイムゾーンが表示されます。switch ID を指定しない場合は、ローカル時刻を表示します。all は未サポートです。
'show clock'コマンドを入力します。

```
switch# show clock [switchid id | all]
```

6 構成情報の管理

6.1 スイッチ構成情報の概要

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書きのとおりです。

- running configuration を startup configuration ファイルへの格納(55 ページの『6.4　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(56 ページの『6.5　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(56 ページの『6.6　コンフィグレーションの回復』参照)

6.2 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。

6.2.1 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には、'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
```

6.2.2 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には、'delete file'コマンドを使用します。

```
switch#delete myconfig
```

6.2.3 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、'rename <file> <destination file>'コマンドを使用します。

```
switch#rename myconfig myconfig_20101010
```

6.2.4 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、'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-table 2 2 2 1 2 2 2 2
!
interface Vlan 1
shutdown
!
port-profile default
vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
!
protocol lldp
!
end
!
```

6.3 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 6-1 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 6-1 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	Network OS のファームウェアパッケージの一部です。default configuration は、スイッチの初期状態が格納されており、初期状態に戻す際に使用します。
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。

スイッチを起動する初回に、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 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。

6.3.1 default configuration

Default configuration ファイルは、Network OS ファームウェアパッケージの一部で、初期状態のコンフィグレーションファイルです。スイッチを初期状態に戻す場合に本ファイルをリストアします。default configuration は削除、名称変更、コンフィグレーションの変更は出来ません。

(1) default configuration の表示

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

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

6.3.2 startup configuration

startup configuration は不揮発情報で、システムがリブートする時に適用されます。
running configuration に対してコンフィグレーションを変更し、'copy'コマンドで startup configuration に変更を格納した場合は、running configuration は startup configuration となります。

(1) startup configuration の表示

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

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

6.3.3 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、'show running-config'コマンドを使用してください。

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

6.4 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。

6.4.1 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。

'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
```

6.4.2 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．'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
```

6.4.3　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。

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

6.5 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。

- 全てのスイッチの 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。
- 回復時はバックアップコピーからの変わりに、一つのスイッチからコンフィグレーションをコピーするのは避ける。

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

'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
```

6.6 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。

- 56 ページ記載の『6.6.1　以前の startup configuration の回復』
- 57 ページ記載の『6.6.2　default configuration の回復』

6.6.1　以前の startup configuration の回復

running configuration の変更に startup configuration を上書きすることで、コンフィグレーションの変更を元に戻す場合の方法です。

1．アーカイブされた startup configuration ファイルを FTP サーバからコピーする。
2．スイッチをリブートします。

```
switch# copy
ftp://admin:******@122.34.98.133/archive/startup-config_vdx24-08_
20101010 startup-config
switch# reload
```

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。

6.6.2 default configuration の回復

この回復手順は、工場出荷時の状態に回復する場合に使用します。初期値を格納したファイルはスイッチ上に存在し、'copy'コマンドで簡単に回復することが出来ます。
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 falsh://defaultconfig.novcs startup-config
This operation will modify your startup configuration. Do you want
to continue?
[Y/N]: y
```

ATTENTION
工場出荷設定では、全てのスイッチの機能が無効化されています。スイッチを使用するためには、必要な全ての設定を再度行う必要があります。

6.7 VCS モードでの構成情報管理

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
スイッチは、構成ファイルを共有できるよう同じモデル、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。

6.7.1　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．　55 ページの『6.4.1　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(56 ページの『6.5.1　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、56 ページの『6.6 コンフィグレーションの回復』を参照下さい。

7 ファームウェアのインストールと管理

7.1 アップグレードをはじめる前に

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。59 ページの『7.1.1　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。56 ページの『6.5　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。

7.1.1　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

7.2 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、デフォルトモードで'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、アップブレードの評価を行いたい場合は、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、60 ページの『7.3　ファームウェアアップグレードの検証』を参照下さい。

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 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: 10.38.33.131
File Name: nos_2.0.0
Protocol (ftp, scp): ftp
User: admin
Password:******
Do Auto-Commit after Reboot [Y]:y
Reboot system after download [Y]:y

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]: y
Server IP: 10.38.33.131, Protocol IPv4
Checking system settings for firmware download...
System settings check passed.

You are running 'firmware download' with auto-reboot and auto-commit enabled.
After the firmware is downloaded the system will reboot and commit firmware
automatically.
2010/09/23-14:31:44, [SULB-1001], 64858, WARNING, VDX6720-24, Firmwaredownload
command has started.
2010/09/23-14:31:44, [SULB-1036], 64859, INFO, VDX6720-24, The current
Version: NOS v2.0.0.0_bld16
dir                 ##################################################
ldconfig            ##################################################
glibc               ##################################################
[output truncated]
```

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。

7.3 ファームウェアアップグレードの検証

新しい(または古い)バージョンを簡易に検証した後に以前のバージョンに回復することが出来ま

す。ファームウェアの回復を可能とするため、nocommit オプションで'firmware download'コマンドを実行します。これは、'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。ファームウェアのアップグレードの検証は、現状のファームウェアを置換えることなく以前のファームウェアバージョンに回復できることを可能としています。

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。

7.3.1 ファームウェアのダウンロード

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 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"n"を入力します。

```
switch#firmware download interactive
Server Name or IP Address: 10.38.33.131
File Name: nos2.0.0
Protocol (ftp, scp): ftp
User: admin
Password:******
Do Auto-Commit after Reboot [Y]:n
Reboot system after download [Y]:y

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]: y
Server IP: 10.38.33.131, Protocol IPv4
Checking system settings for firmware download...
System settings check passed.

You are running 'firmware download' with auto-commit disabled. After the
system is rebooted, please run 'firmware commit' or 'firmware restore'
manually.
2010/09/23-14:31:44, [SULB-1001], 64858, WARNING, VDX6720-24, Firmwaredownload
command has started.
2010/09/23-14:31:44, [SULB-1036], 64859, INFO, VDX6720-24, The current
Version: NOS v2.0.0.0_bld16
dir                ##################################################
ldconfig           ##################################################
glibc              ##################################################
[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'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、62 ページの『7.3.3　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 62 ページの『7.3.2　ファームウェアアップグレードの承認』に進んでください。

7.3.2　ファームウェアアップグレードの承認

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。承認が完了するまで数分かかります。

1．'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。

7.3.3　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。
ファームウェアの承認は、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５分間待ちます。

3．'show version'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。

8 ライセンスの管理

Brocade Network Operationg 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 8-1 に各機能に必要なライセンスの一覧を示します。

表 8-1 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１０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。

8.1 ライセンスの管理

8.1.1 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、'show license id'コマンドを入力します。

```
switch# show license id
SwitchId LicenseId
========================================
2 10:00:00:05:1E:00:4C:80
```

8.1.2 ライセンスキーの保管

ライセンスアップグレードの指示は、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。

8.1.3 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、ある機能は、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。ライセンスタイプによって、スイッチのリブートを促されます。コマンド出力に沿って適切な作業を行ってください。

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:fUjANFav5W:gWx3
hH2:9RsMv3BHfeCRFM2gj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t
#"
Adding license [*B
r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANFav5W:gWx3
hH2:9RsMv3BHfeCRFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,7
3t#]
switch# show license
SwitchId: 2
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
     VCS Fabric license
     Feature name:VCS
```

8.1.4 ライセンスの削除

ライセンスを削除する場合、ある機能はスイッチのリブートが必要となります。

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、スイッチをリブートを促されます。
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。

---

9 セキュリティ

9.1 ロール管理

ロールは、スイッチのユーザアカウントのアクセス権限を定義したものです。ユーザは、一つのロールに関連付けられています。ロールにどのように権限を割り当てるかは 70 ページの『ロールベースアクセス制御』を参照してください。

9.1.1 デフォルトロール

デフォルトロールの属性は、修正できません。しかし、デフォルトロールは、非デフォルトのユーザアカウントに割り当てることができます。次に示すロールはデフォルトロールです。

- 管理者ロールは最も高い権限を持っています。全てのコマンド(CLI)は管理者ロールに割り当てられたユーザが使用することが出来ます。
- ユーザのロールは、特権実行モードではほとんど show コマンドに限定されているという制限された権限をとなります。ユーザアカウントは、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。'exit'コマンドと'no'コマンドもユーザロールで利用可能です。

9.1.2 ロールの属性

ロールは２つの属性を持っています。ロールの名前と説明です。

- Name ― ロール名称は唯一省略できない属性です。ロール名称は、文字で始まる 4～32 文字で無ければなりません。数字、アルファベットとアンダースコア(_)が使用可能です。名前は、登録済みユーザのものと同じものは使えません。
- Description ― ロールのディスクリプションは、オプションです。ディスクリプションは、64 文字までで、句読点、シングルクォート(')、ダブルクォート(")、エクスクラメーションマーク(!)、コロン(:)、セミコロン(;)を除く表示可能な ASCII 文字が使用可能です。ロールディスクリプションを設定する時、ダブルクォーテーションでテキストを囲む必要があります。ダブルクォーテーションはテキストにスペースを含む場合にのみ必要です。

9.1.3 ロールの追加と変更

ロールの最大数は 64 です。

ロールへの権限の割り当て方については、70 ページの『9.3　ロールベースアクセス制御』を参照下さい。

1．'configure terminal'コマンドを入力します。

2．'role name'コマンドを入力します。

ロール名称"NetworkSecurityAdmin"の追加と変更例

```
switch(config)# role name NetworkSecurityAdmin desc "Manages
```

```
security CLIs”
switch(config-name-NetworkSecurityAdmin)#
```

9.1.4 ロールの削除

1．'configure terminal'コマンドを入力します。

2．'no role name'コマンドを入力します。

ロール名称" VLANAdmin"の削除例

```
switch(config)# no role name VLANAdmin
```

9.1.5 ロールの表示

'show running-config role'コマンドを入力します。

```
switch# show running-config role
role name VLANAdmin desc “Manage security CLIs”
role name NetworkAdmin desc “Manages Network CLIs”
role name ClusterAdmin desc “Manages Cluster CLIs”
```

9.2 ユーザ管理

認可された特権レベルが他のユーザを作成、変更、削除することを決定するための役割をユーザに割り当てなければなりません。

9.2.1 ユーザ属性

全てのユーザは、次の属性を持っています。

- Name ― ユーザの名前です。ユーザ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。登録済みロールで使われているものは使用できません。
- Password ― ユーザのパスワードです。
- Encryption level ― パスワード入力が、プレーンテキストか暗号化を示します。0 がテキスト、7 が暗号化となります。プレーンテキスト(0)がデフォルトです。
- Role ― ユーザに関連付けられたロールです。
- Desc ― ユーザの説明です。ディスクリプションフィールドは 64 文字以内で、シングルクォート(')、ダブルクォート(")、エクスクラメーションマーク(!)、コロン(:)、セミコロン(;)を除く表示可能な ASCII 文字が使用できます。もしテキスト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。
- Enabled ― ユーザが有効か無効かを設定します。無効ユーザはログインできません。デフォルトは有効です。

工場出荷設定の一部としてスイッチのデフォルトユーザは"admin"と"user"です。"admin"と"user"

のみがログイン可能で、パスワードを除いて、他の属性は変更できません。

NOTE
名前、パスワード、ロール属性は省略できません。

9.2.2 ユーザの追加

ユーザの登録数は最大 64 です。

NOTE
'username'と'no username'コマンドはグローバルコンフィグレーションモードコマンドで、
'unlock username'コマンドは特権実行コマンドです。

1．'configure terminal'コマンドを入力します。
2．'username'コマンドを入力します。

```
switch(config)# username brcdUser role user password
“BwrsDbB+tABWGWpINOVKoQ==¥” encryption-level 7 desc “Brocade User”
enable true
```

NOTE
'enable'が “false”なら、ユーザはログインできません。

9.2.3 ユーザの変更

全てのアクティブログインセッションは、ユーザのパスワードかロールが変更されると、終了します。

NOTE
'username'と'no username'コマンドはグローバルコンフィグレーションモードコマンドで、
'unlock username'コマンドは特権実行コマンドです。

追加と変更操作の書式は、似ています。違いは、必須なパラメータかどうかです。システムは内部でコンフィグレーションに登録済みかどうかをチェックすることで、追加か変更かを識別します。

1．'configure terminal'コマンドを入力します。
2．'username'コマンドを入力します。
ユーザの変更例(例では、desc のデフォルト値を設定)

```
switch(config)# username testUser enabled false
switch(config-username-testUser)# desc "add op test user"
switch(config)# no username testUser desc
```

NOTE
ログイン中のユーザに対して、'username'コマンドの no 形式を使用することで、セッションを終了させます。

9.2.4 ユーザの削除

ユーザアカウントが無効になると、ユーザの全てのアクティブログインセッションは終了します。

NOTE
'username'と'no username'コマンドはグローバルコンフィグレーションモードコマンドで、'unlock username'コマンドは特権実行コマンドです。

1．'configure terminal'コマンドを入力します。
2．'no username'コマンドを入力します。

```
switch(config)# no username testUser
```

9.2.5 ユーザの表示

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

```
switch# show running-config username userBrocade
username userBrocade
 desc " User to monitor"
password $1$no$password-hidden
 role     user
 enabled  true
```

9.2.6 ユーザ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、システムはアカウントをロックします。

NOTE
'username'と'no username'コマンドはグローバルコンフィグレーションモードコマンドで、'unlock username'コマンドは特権実行コマンドです。'show users'コマンドで、現在スイッチにログインしているアカウントとロックされているアカウントを確認することが出来ます。

ロックされているユーザアカウントを解除するために'unlock username'コマンドを使います。

１．'unlock username'コマンドを入力します。

```
switch# unlock username testUser
Result: Unlocking the user account is successful
```

9.3 ロールベースアクセス制御

ロールベースアクセス制御(RBAC)は、許可メカニズムとして使われる。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ルールに関連付けられます。ユーザアカウントは、いずれかのロールに関連付ける必要があり、全てのユーザアカウントは一つのロールにだけ関連付けることが出来ます。権限は、ユーザアカウントに直接に割り当てることはできません。関連するロールを通してのみ設定することが出来ます。

RBAC はロールに対してリソースへのアクセス権を指定する機能です。ユーザがコマンドを実行する時、ユーザのロールに基づき、コマンドが使用可能かを判別します。
デフォルトロールは、どのユーザからも変更できない事前定義のルールを持っています。管理者ロールは全てのコマンドを実行する権限があります。一方、ユーザロールは全ての'show'コマンドと'show running-config'コマンドを実行する権限があります。新しいロールが定義されると、デフォルトではユーザロールの権限を持ちます。

NOTE
新しいスイッチでは、管理者ユーザアカウントだけがユーザとロール管理を実行する権限を持っています。管理者ユーザは、どんなロールも作成可能で、ユーザとロール管理を行うためのロールを定義することが出来ます。

9.3.1 ルール管理

コマンドの実行許可は、順に並んだルールの集合として定義されます。ルールは次に示す CIL コマンドの書式の属性を持ちます。

- Index — ルールの識別子。１から 1024 までの範囲が有効です。このフィールドは省略できません。
- Role — ルールを定義するロールの名称。このフィールドは省略できません。
- Operation — 操作タイプの定義。read-only と read-write の２つの値を持ちます。このフィールドはオプションです。デフォルトは、read-write。
- Action — accept と reject の２つの値を持ちます。このフィールドはオプションです。デフォルトは、accept です。
- Command — アクセスを拒否するコマンド。コマンドは、スペースで区切ります。RBAC は次の例に示すように copy、clear、interface、protocol コマンドをサポートします。

```
rule 70 action accept operation read-write role NetworkAdmin command
copy running-config
```

```
rule 71 action accept operation read-write role NetworkAdmin command
interface management
rule 72 action accept operation read-write role NetworkAdmin command
interface fcoe
```

ルールは、次のサンプルに示されるように'interface tengigabitethernet'の個別インスタンスに対して作られます。

```
rule 60 action accept operation read-write role NetworkAdmin command
interface tengigabitethernet 0/4
```

'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。

```
rule 75 action reject operation read-write role NetworkAdmin command
no-operation
```

(1)コンフィグコマンドに対するルール

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る。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にとっては、'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)により変更することが出来ます。ユーザはどのコンフィグコマンドでも実行できるように'configure'コマンドに対して read-write 権限を持っています。

次のルールはコンフィグレーションコマンドに適用されています。

- もし、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。
- もし、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。
- もし、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。

(2)運用コマンドに対するルール

指定された operational コマンドにしてルールは作成される。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るが、実行することは出来ない。show コマンドは全てのユーザが使用可能である。

次のルールが運用コマンドに適用されています。

もし、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はコマンドを実行できます。

- もし、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。

- もし、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はコマンドへアクセスも実行もできません。

(3)interface 関連コマンドのルール

ルールは、10G Ether のインタフェースに関連したコンフィグレーションコマンドの特定のインスタンスに対して作成されます。ユーザは、'show running-donfig interface te'コマンドを使って、全ての interface インスタンスのコンフィグレーションデータにアクセスすることが出来ます。
次のルールが interface 関連コマンドに適用されます。

ロール			ユーザ権限
operation	ルール		
	action	対象	
read-write	accept	interface の特定インスタンス	属性の変更のみ
read-only	accept	interface の特定インスタンス	データの読み出しのみ show running-config 全ロールのデフォルトルール
read-write	reject	interface の特定インスタンス	実行/読み出し不可
read-write	reject	Tengigabitethernet	データの消去/参照不可

clear / show を実行するには、少なくとも read-only の許可権限が必要です。

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

```
rule 30 role NetworkAdmin action reject command interface
tengigabitethernet
```

上記のルールで、ユーザは次のコマンドを使用することが出来ません。

- clear arp-cache tengigabitethernet 1/0/1 no-refresh
- clear counters interface tengigabitethernet 1/0/1
- clear dot1x statistics interface tengigabitethernet 1/0/1
- clear fcoe login interface tengigabitethernet 1/0/1
- clear ip igmp groups interface tengigabitethernet 1/0/1
- clear lldp neighbors interface tengigabitethernet 1/0/1
- clear lldp statistics interface tengigabitethernet 1/0/1
- clear mac-address-table dynamic interface tengigabitethernet 1/0/1
- clear spanning-tree counter interface tengigabitethernet 1/0/1
- clear spanning-tree detected-protocols interface tengigabitethernet 1/0/1
- show arp tengigabitethernet 1/0/1
- show dot1x diagnostics interface tengigabitethernet 1/0/1

- show dot1x session-info interface tengigabitethernet 1/0/1
- show dot1x statistics interface tengigabitethernet 1/0/1
- show ip igmp groups interface tengigabitethernet 1/0/1
- show lldp interface tengigabitethernet 1/0/1
- show lldp neighbors interface tengigabitethernet 1/0/1
- show lldp statistics interface tengigabitethernet 1/0/1
- show mac access-group interface tengigabitethernet 1/0/1
- show mac-address-table count dynamic interface tengigabitethernet 1/0/1
- show mac-address-table count interface tengigabitethernet 1/0/1
- show mac-address-table dynamic interface tengigabitethernet 1/0/1
- show mac-address-table interface tengigabitethernet 1/0/1
- show mac-address-table linecard interface tengigabitethernet 1/0/1
- show mac-address-table static interface tengigabitethernet 1/0/1
- show media interface tengigabitethernet 1/0/1
- show port port-channel tengigabitethernet 1/0/1
- show port-profile interface tengigabitethernet 1/0/1
- show qos flowcontrol interface tengigabitethernet 1/0/1
- show qos interface tengigabitethernet 1/0/1
- show qos queue interface tengigabitethernet 1/0/1
- show qos rcv-queue interface tengigabitethernet 1/0/1
- show qos rcv-queue multicast tengigabitethernet 1/0/1
- show sflow interface tengigabitethernet 1/0/1
- show spanning-tree interface tengigabitethernet 1/0/1
- show spanning-tree mst detail interface tengigabitethernet 1/0/1
- show spanning-tree mst interface tengigabitethernet 1/0/1
- show statistics access-list interface tengigabitethernet 1/0/1

interface のサブモードにある dot1x オプションは、dot1x コマンドとインタフェースのロールが read-write で accept 権限の場合のみ設定可能です。下記は例です。

```
rule 16 action accept operation read-write role cfgadmin command interface
tengigabitethernet

rule 17 action accept operation read-write role cfgadmin command dot1x

switch(config)# interface TenGigabitEthernet 1/0/1
switch(conf-if-te-1/0/1)# ?

Possible completions:
  cee                 Apply default CEE map 'default'
  channel-group       LACP channel commands
  description         Interface specific description
  do                  Run an operational-mode command
  dot1x               IEEE 802.1X Port-Based Access Control
  exit                Exit from current mode
  fabric              Fabric Protocol
  fcoeport            Configure the port to be an FCOE port
  help                Provide help information
  ip                  The Internet Protocol (IP).
  lacp                LACP commands
  lldp                The Link Layer Discovery Protocol(LLDP).
  mac                 Configure MAC parameters
  mtu                 Set mtu value to interface
  no                  Negate a command or set its defaults
  port-profile-port   Set the interface to AMPP profile mode
  pwd                 Display current mode path
  qos                 Quality of Service (QoS)
  rmon                Remote Monitoring Protocol (RMON)
  sflow               SFlow
  shutdown            Shutdown the selected interface
  speed               Set speed informational parameter
  switchport          Set the switching characteristics of the Layer2 interface
  top                 Exit to top level and optionally run command
  vepa                Enable vepa to support U-turn of the traffic on the
selected
                      interface
  vlan                Vlan commands
```

interface tengigabitethernet のサブモードで'no vlan'と'no spanning-tree'を実行するためには、ユーザは vlan と protocol spanning-tree コマンドに read-write と accept の権限が必要です。デフォルトでは、ユーザロール含む全てのロールが、全ての interface に対して read-only と accept 権限を持ちます。

9.3.2 デフォルトロール

デフォルトロールはどのユーザからも変更できない事前定義のルールセットです。
管理者ロールは全てのコマンドを実行する権限を持っています。初期の管理目的のあるコマンドは、管理者ロールでのみ利用できます。
次のコマンドはユーザロールで利用可能です。

- show
- show running-config

NOTE
新しく作成されたロールは、デフォルトでユーザロールの全ての権限を持っています。

9.3.3 ルールの処理

ユーザがコマンドを実行する時、ルールはインデックスに合致するものを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。もし、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。もし、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 で accept 権限の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
```

次の例では、ルール 9 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 reject role
NetworkAdmin command aaa
```

9.3.4 ルールの追加

ルールの最大数は 512 です。

1．'configure terminal'コマンドを入力します。

2．'rule'コマンドを入力します。

NOTE
ロールとコマンドフィールドは省略できません。actionとoperationフィールドはオプションです。

```
switch(config)# rule 150 action accept operation read-write role
NetworkAdmin command config
switch(config)# rule 155 action accept operation read-write role
NetworkAdmin command username
```

ルール作成後、NetworkSecurityAdminUser アカウントはスイッチにログインして、'username'コマンドに続いて指定されるユーザアカウントの生成や変更が可能となります。

```
switch login: NetworkSecurityAdminUser
Password:
Welcome to the ConfD CLI
NetworkSecurityAdminUser connected from 127.0.0.1 using console on
switch
switch# config
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 testpassword
```

9.3.5 ルールの変更

1．'rule'コマンドを入力します。

```
switch(config)# rule 155 command role
```

NOTE
rule index を除く全てのフィールドはオプションです。

ルール 155 を変更した後は、NetworkSecurityAdminUser アカウントは、スイッチにログインして'role'コマンドは実行できますが、'username'コマンドは実行できません。

```
switch login: NetworkSecurityAdminUser
Password:
Welcome to the ConfD CLI
NetworkSecurityAdminUser connected from 127.x.x.x using console on
```

```
switch
switch# config
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
```

9.3.6 ルールの削除

1．'configure terminal'コマンドを実行します。

2．'no rule'コマンドを実行します。

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

ルール 155 を削除した後は、NetworkSecurityAdminUser アカウントは'role'コマンドにアクセスできません。

9.3.7 ルールの表示

'show running-config rule'コマンドを入力します。

```
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
rule 40 action accept operation read-write role FCOEAdmin
rule 40 command "interface fcoe"
switch# show running-config rule 32
rule 32 action accept operation read-write role NetworkSecurityAdmin
rule 32 command username
```

9.3.8 ネットワークセキュリティ管理のためのロール管理

1．ネットワークセキュリティ管理用ロールを作成します。

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

2．ネットワークセキュリティ管理用アカウントを新たに作成したロールに関連付けます。

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

3．ネットワークセキュリティ管理用ルールを作成します。

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

NetworkSecurityAdmin ロールに関連付けられた NetworkSecurityAdminuser アカウントは、ユーザ管理、ロール管理、ルール管理の操作が可能となります。

9.4 RADIUS

RADIUS は主に認証(authentication)、認可(authorization)、アカウンティング(accounting)の AAA サービスを管理するために使用されます。RADIUS が使用できるアクセス方法は、シリアルポート、telnet 及び SSH です。

9.4.1 認証とアカウント

認証のためにスイッチが一連の RADIUS サーバと共に構成されると、スイッチは RADIUS サーバに暗黙的にアカウントデータを送信します。RADIUS ユーザのログイン成功・失敗のみが記録される唯一のイベントです。

NOTE
もし RADIUS サーバがアカウンティング機能をサポートサポートするよう構成されていない場合、スイッチから送信されるアカウンティングイベントは廃棄されるでしょう。

9.4.2 認可

RADIUS ユーザのアクセス制御は、スイッチの RBAC による制御されます。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 ユーザは正しく認証された後、もし RADIUS サーバにい割り当てられたロールがスイッチに存在しない場合、ユーザにはユーザロールが割り当てられます。

9.4.3 パスワードの変更

スイッチ上のローカルなユーザ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もたらしません。すなわち、RADIUS ユーザ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。

9.4.4 RADIUS サーバのパラメータ

次に示すパラメータは、スイッチ上で定義できる RADIUS サーバに関する情報です。スイッチ上で CLI コマンドを使って AAA サービスのために RADIUS サーバを最大５つの設定できます。

- host - IP アドレス。IPv4 または IPv6 が指定可能。
- auth port - 認証のために RADIUS サーバと接続する UDP ポート。１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-MSCHAP が指定可能。デフォルトは CHAP。IPv6 では PEAP-MSCHAP 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。
- 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。デフォルトは５秒。
- retrasmit - 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
もし key 属性を設定しない場合、認証セッションは暗号化されません。key の値は RADIUS 構成ファイルに設定されている値と一致しなければなりません。槽でなければ、サーバとスイッチ間の通信は失敗します。

9.4.5　RADIUS サーバの追加

ドメイン名やホスト名で RADIUS サーバを追加する前に、スイッチに domain name server (DNS) を設定しなければなりません。DNS が無ければ、RADIUS サーバの名前解決が失敗して、追加することが出来ません。

1．'configure terminal'コマンドを入力します。
2．'radius-server'コマンドを入力します。

```
switch(config)# radius-server host ?
Possible completions:
  <hostname: IP Address or Hostname of this RADIUS server>
switch(config)# radius-server host

switch(config)# radius-server host 10.24.65.6 ?
Possible completions:
  auth-port     UDP Port for Authentication (default=1812)
  protocol      Authentication protocol to be used (default=CHAP)
  key           Secret shared with this server (default='sharedsecret')
  retransmit    Number of retries for this server connection (default=5)
  timeout       Wait time for this server to respond (default=5 sec)

switch(config)# radius-server host 10.24.65.6
switch(config)# radius-server host 10.24.65.6 protocol chap ?
Possible completions:
  auth-port     UDP Port for Authentication (default=1812)
  key           Secret shared with this server (default='sharedsecret')
  retransmit    Number of retries for this server connection (default=5)
  timeout       Wait time for this server to respond (default=5 sec)
  <cr>
switch(config)# radius-server host 10.24.65.6 protocol chap retransmit ?
Possible completions:
  <0-100> [5]
switch(config)# radius-server host 10.24.65.6 protocol chap retransmit 100
switch(config-radius-server-10.24.65.6)#

switch(config)# radius-server host 10.38.37.180 protocol pap key
"new#virgo*secret timeout 10
switch(config-host-10.38.37.180)#
```

9.4.6　RADIUS サーバの変更

引数無しで'radius-server host'コマンドを使うことで、パラメータのデフォルト値を設定できます。RADIUS サーバのホスト名称または IP アドレスとキー文字列を変更するために、'radius-server host'コマンドを使います。

1．'configure terminal'コマンドを入力します。
2．'radius-server host'コマンドを入力します。

```
switch(config)# radius-server host ?
Possible completions:
<hostname: IP Address or Hostname of this RADIUS server> 10.xx.xx.xxx
10.xx.xx.x
switch(config)# radius-server host 10.xx.xx.xxx
switch(config-host-10.xx.xx.xxx)# key ?
```

```
Possible completions:
<string>[new#virgo*secret]
switch(config-host-10.xx.xx.xxx)# key “changedsec”
switch(config-host-10.xx.xx.xxx)# no timeout
```

9.4.7 RADIUS サーバの表示

NOTE
デフォルト値は表示されません。

1．'show running-configuration radius-server'コマンドを入力します。

```
switch# show running-configuration radius-server host ?
Possible completions:
  10.xx.xx.xxx IP Address or Hostname of this RADIUS server
  10.xx.xx.x IP Address or Hostname of this RADIUS server

switch# show running-config radius-server host 10.xx.xx.x
radius-server host 10.xx.xx.x
 key           new#vcs*secret
 retransmit 100
 timeout     3

switch#

switch# show running-config radius-server host 10.xx.xx.xxx
radius-server host 10.xx.xx.xxx
protocol   pap
key          changedsec
timeout    3
```

9.4.8 RADIUS サーバの削除

1．'configure terminal'コマンドを入力します。
2．'radius-server'コマンドを入力します。

```
switch(config)# no radius-server 10.xx.xx.x
switch(config)# exit
switch# show running-config radius-server host
radius-server host 10.xx.xx.xxx
 auth-port  1812
 protocol   chap
 key        changedsec
 retransmit 5
 timeout    3
```

9.5 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。

NOTE
ユーザプロファイルで RADIUS は認証と認可を結合したとしても、TACACS+は２つのサービスを分離します。

TACACS+に基づく認証機能を設定した場合、シリアルポート、telnet 及び SSH が利用できます。これらのアクセス方法では、ユーザがスイッチに接続するためにスイッチの IP アドレスもしくは名称を知っている必要があります。スイッチは管理用 IP アドレスのみを使用します。VCS の仮想アドレスは、TACACS+サーバの認証には使われません。
認証プロトコルは、ユーザ認証のために Password Authentication Protocol (PAP) と Challenge Handshake Authentication Protocol (CHAP)をサポートしています。
TACACS+サーバは、認証にのみ使用されます。ロールは TACACS+サーバ及びスイッチローカルに定義されたユーザに割り当てられます。もし認証後にスイッチが TACACS+サーバからユーザロールを取得できなかった場合、またはスイッチ上に定義されたどのロールにも一致しない場合、デフォルトのユーザロールが適用されます。それ以降は、TACACS+サーバから引き出されたロールかデフォルトロールが RBAC として使われます。

9.5.1 TACACS+サーバのパラメータ

次に示すパラメータは、スイッチ上で定義できる TACACS+サーバに関連する情報です。CLI コマンドを使って、認証サービスのためにスイッチ上に最大５つの TACACS+サーバを設定できます。

- host - TACACS+サーバの IP アドレス(IPv4)。
- port - 認証のために TACACS+サーバと接続する TCP ポート。デフォルトは４９。
- protocol - 使用する認証プロトコル。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。
- 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。デフォルトは５秒。
- retries - TACACS+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
key 属性が設定されていない場合、認証セッションは暗号化されません。key の値は TACACS+構

成ファイルに定義された値と一致しなければなりません。そうでなければ、サーバとスイッチの通信は失敗します。

9.5.2 TACACS+サーバの追加

1．'configure terminal'コマンドを入力します。

2．'takacs-server'コマンドを入力します。

```
switch(config)# tacacs-server host ?
Possible completions:
  <hostname: IP Address or Hostname of this TACACS+ server>
switch(config)# tacacs-server host 10.24.65.6 ?
Possible completions:
  port    TCP Port for Authentication (default=49)
  protocolAuthentication protocol to be used (default=CHAP)
  retriesNumber of retries for this server connection (default=5)
  timeoutWait time for this server to respond (default=5)
  <cr>
switch(config)# tacacs-server host 10.24.65.6
switch(config)# tacacs-server host 10.24.65.6 protocol chap ?
Possible completions:
  port    TCP Port for Authentication (default=49)
  retriesNumber of retries for this server connection (default=5)
  timeoutWait time for this server to respond (default=5)

switch(config)# tacacs-server host 10.24.65.6 protocol chap
switch(config)# tacacs-server host 10.24.65.6 protocol chap retries ?
Possible completions:
  <0-100>
switch(config)# tacacs-server host 10.24.65.6 protocol chap retries 100
switch(config-tacacs-server-10.24.65.6)#
switch(config)# tacacs-server host 10.38.37.180 protocol chap key
"new#virgo*secret
```

9.5.3 TACACS+サーバの変更

TACACS+サーバホスト名または IP アドレスとキー文字列を変更するためには、'tacacs-server host'コマンドを使用します。

1．'configure terminal'コマンドを入力します。

2．'tacacs-server host'コマンドを入力します。

```
switch(config)# tacacs-server host ?
Possible completions:
  <hostname: IP Address or Hostname of this TACACS+ server>
  10.xx.xx.xxx
  10.xx.xx.x
switch(config)# tacacs-server host 10.xx.xx.xxx
switch(config-host-10.xx.xx.xxx)# key ?
Possible completions:
  <string>[##tac*Plus&secret]
switch(config-host-10.xx.xx.xxx)# key "changedsec"
```

9.5.4 TACACS+サーバの表示

NOTE
デフォルト値は表示されません。

1．'show running-configuration tacacs-server host'コマンドを入力します。

```
switch# show running-config tacacs-server host ?
Possible completions:
  10.xx.xx.xxx IP Address or Hostname of this TACACS+ server
  10.xx.xx.x IP Address or Hostname of this TACACS+ server

switch# show running-config tacacs-server host 10.xx.xx.x
tacacs-server host 10.xx.xx.x
 key         new#virgo*secret
 retries     100
!
switch#

switch# show running-config tacacs-server host 10.xx.xx.xxx
tacacs-server host 10.xx.xx.xxx
key         changedsec
```

9.5.5 TACACS+サーバの削除

'no tacacs-server host'コマンドを入力します。

NOTE
引数無しで'tacacs-server host'コマンドを使用するとパラメータのデフォルト値を設定します。

```
switch(config)# no tacacs-server host 10.xx.xx.x
switch(config)# exit
switch# show running-config tacacs-server host
Possible completions:
  10.xx.xx.xxx IP Address of this TACACS+ server
  <cr>
switch# show running-config tacacs-server host 10.xx.xx.xxx
tacacs-server host 10.xx.xx.xxx
key        changedsec
!
switch# config
switch(config)# no tacacs-server host 10.xx.xx.xxx key
switch(config)# exit
switch# show running-config tacacs-server host 10.xx.xx.xxx
tacacs-server host 10.xx.xx.xxx
!
switch# config
switch(config)# tacacs-server host 10.xx.xx.xxx key ?
<string> [sharedsecret]
```

9.6 ログイン認証

認証モードは、ユーザ認証(ログインプロセス)として使われる認証ソースの順番として定義されます。プライマリとセカンダリの認証に２つのソースをサポートしています。認証におけるセカンダリソースは、プライマリソースの交代時に使われ、オプションとなります。ソースは３種類が可能です。

- ローカル(デフォルトソース)
- RADIUS
- TACACS+

NOTE
認証モードをセットできますが、新しいモードや存在するモードを削除することは出来ません。

認証・承認・アカウンティング(AAA)モードが変更された時、適切なメッセージが全てのログインユーザとアクティブなログインセッションに向けてブロードキャストされます。もし、プリマリソースが外部の AAA タイプ(RADIUS か TACACS+)に設定され、セカンダリソースが未設定ならば、次のイベントが発生します。

- Telnet 及び SSH のログインに対しては、設定された AAA サーバ(プライマリソース)の応答が無いか、AAA サーバのログイン拒否のいずれかの場合、ログイン認証が失敗します。
- シリアルポート接続のログインに対しては、フェイルオーバーが発生したり同一ユーザの証明書がローカルソース経由のログインに使われるなど、いかなる理由に対してもユーザのログインは失敗します。このフェイルオーバーは明確ではありません。
- もし、プライマリソースが外部 AAA タイプに設定されていて、セカンダリソースがローカル

ソースに設定されている場合、設定されたサーバが応答しないか、ログインが拒否されたいずれかの理由で、プライマリソースのログインが失敗すると、フェイルオーバーが発生して、セカンダリサーバにより再度認証されます。

9.6.1 一致する条件

もし一つ目のソースがデフォルトで指定されたなら、二番目のソース指定しないで下さい。二番目のソースはログイン認証モードをデフォルトにするよう知らせます。
ローカルを除く認証ソースと関連するサーバタイプの構成は互いに独立しています。それゆえ、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ーつの設定されたサーバが存在するべきです。
もし、ソースがサーバタイプであると設定された場合は、リストに唯一存在するサーバであれば削除することは出来ません。例えば、TACACS サーバにエントリが無ければ、認証モードは'tacacs+'にも'tacacs+local'にも設定できません。同様に、認証モードが radius か radius local の場合は、RADIUS サーバはリスト上の唯一のサーバであれば削除することは出来ません。

9.6.2 認証の限界

認証モードを tacacs+ local から tacacs+へ、または、radius local から radius へ変更することは出来ません。代替方法は、AAA を削除して正しい値をセットすることです。

1．'no aaa authentication login'コマンドを入力します。
2．'aaa authentication login tacacs+'コマンドか'aaa authentication login radius'

9.6.3 認証モードの設定

'aaa authentication login'コマンドを入力します。

```
switch(config)# aaa authentication login ?
Possible completions:
   default local radius tacacs+
switch(config)# aaa authentication login tacacs+ ?
Possible completions:
   local
switch(config)# aaa authentication login tacacs+ local
```

9.6.4 認証モードの表示

'show running-config aaa'コマンドの表示

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

9.6.5　認証モードのデフォルト設定への復帰

'no aaa authentication login'コマンドを実行します。

```
switch(config)# no aaa authentication login
switch(config)# exit
switch# show running-config aaa
aaa authentication login local
```

9.7 パスワード

パスワード強度のポリシーは新しいパスワードが満足しなければならないルールセットを実施します。パスワード強度のポリシーは、新しいパスワードが定義された時だけ実施され、全てのローカルユーザアカウントに実施されます。そして以下の文字制限のセットで構成されます。

- Lowercase ― 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 値以下で無ければなりません。デフォルトは 0 で、小文字の制約はありません。
- Uppercase ― 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 値以下で無ければなりません。デフォルトは 0 で、大文字の制約はありません
- Digits ― パスワードに使われなければならない数字の最小値を指定します。最大値は MinLength 値以下で無ければなりません。デフォルトは 0 で、数字の制約はありません。
- Punctuation ― 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。
- MinLenght ― 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 値以下で無ければなりません。

パスワードが上記属性の一つ以上を満足しない場合、エラーとして報告されるのは属性の一つだけです。

9.7.1　パスワードアカウントのロックアウト

アカウントロックアウトポリシーは、ログインが設定された回数以上失敗した時に、ユーザアカウントを無効化することです。この仕組みは、アカウントをロック解除する明確な管理操作が採られるまで、またはロックされたアカウントが一定期間経過後自動的にロック解除されるまで、ロック状態を維持するよう設定されます。管理者は、いつでもロックされたアカウントを解除することが出来ます。

ログイン失敗のカウンタはユーザ毎に設けられます。全てのユーザアカウントのカウンタは、アカウントロックアウトポリシーが無効になったとき、ゼロにリセットされます。個別のアカウントのカウンタは、ログインが成功した時にゼロにリセットされます。

最大リトライとロックアウトの閾値は、CLI コマンドで設定可能です。

- 最大リトライ(ロックアウト閾値)は、アカウントがロックされる前のログイン中にユーザが誤ったパスワードを指定した回数を指定します。失敗したログインの回数は、前回ログインに成功した時からカウントします。
- ロックアウト閾値は、0 から 16 の値で設定できます。パラメータを 0 に設定するとロックアウト機構は無効となります。デフォルトは 0 です。

アカウントロックアウトポリシーは、'admin'以外の全てのユーザアカウントに適用されます。ユーザアカウントがロックされた場合は、69 ページの『9.2.6　ユーザアカウントのロック解除』を使ってロック解除できます。

9.7.2　外部サーバでのパスワード相互作用

パスワードポリシーは、ローカルスイッチ認証にのみ適用されます。RADIUS や TACACS+のような外部の AAA サーバは、独立したパスワード実施機構を提供します。スイッチが RADIUS や TACACS+認証を使うよう設定されていても、パスワード管理コマンドは、ローカルパスワードデータベースでのみ動作します。ソ設定されている場合は、RADIUS または TACACS+認証はログインにのみ適用されます。

RADIUS または TACC+認証が有効な場合、管理者はユーザとパスワード管理機能をローカルパスワードデータベース上で実行します。

9.7.3　パスワード属性の設定

1．'configure terminal'コマンドを実行します。

2．'password-attributes'コマンドを実行します。

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

9.7.4　デフォルトパスワード属性

パスワード属性コマンドに'no'をつけることで、個々の属性にデフォルト値をセットできます。

1．'configure terminal'コマンドを入力します。

2．'no password-attributes'コマンドを入力します。

```
switch(config)# no password-attributes min-length
switch(config)# password-attributes max-retry 4
switch(config)# no password-attributes
```

9.7.5　パスワード属性の表示

NOTE
デフォルト値の属性は表示されません。

1．'configure terminal'コマンドを入力します。
2．'show running-config password-attributes'コマンドを入力します。

```
switch(config)# password-attributes ?
Possible completions:
  character-restriction   Set restriction on various types of character
  max-retry           Maximum number of login retires before which the user
account is locked.
  min-length              Minimum length of the password.
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
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
switch(config)# no password-attributes
switch(config)# exit
switch# show running-config password-attributes
% No entries found.
switch#
```

10 SNMP 管理

10.1 SNMP コミュニティ

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。もし、新しいコミュニティを作る場合は、スペースを確保するために、６つのデフォルトコミュニティの一つを削除しなければなりません。

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"

10.1.1 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、れ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 32 文字以内で指定します。
- ro もしくは rw は、コミュニティが read-only (ro) か read-write (rw)かを指定します。

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。

10.1.2　　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'を入力します。以下は例です。

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

10.1.3　　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。

10.1.4　　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、次のコマンドを入力します。

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

10.2　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。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。

- • <community:WORD> MIB オブジェクトの問い合わせに使われるコミュニティ
- • ConvergedNetwork—read-only
- • OrigEquipMfr—read-write
- • Secret C0de—read-write
- • common—read-only
- • private—read-write
- • public—read-only

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つのうち一つを削除する必要があります。

10.2.1 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 server host ipv4_host community string [version {1|2c}] [udp-port port]'コマンドを入力します。

ipv4_host は、ホストの IP アドレスを指定します。IPv4 のみサポートしています。

community-string は、コミュニティ名を指定します。

version は、SNMPv1 か SNMPv2c を選択します。これらのパラメータは、コミュニティ名を含みます。デフォルトは、1 (SNMPv1)です。

udp-port は、SNMP トラップを受信する UDP ポートを指定します。デフォルトは 162 です。指定可能な値は、0 から 65535 です。

次の例は、read-only ユーザとして、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
```

10.2.2 SNMP サーバの連絡先の設定

SNM サーバの連絡先情報を設定するために、この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。もし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"
```

10.2.3 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ために、このコマンドを使用します。デフォルト値は、"End User Premise"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 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"
```

10.2.4 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、ロケーションなどの SNMP 設定情報を表示するために、このコマンドを使います。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、特権ユーザ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
```

11 ファブリック管理

11.1 TRILL

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、お互いに情報交換するスイッチの範囲を定義します。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。それは、互いに接続するルーティングブリッジ(RBridges)と呼ばれるデバイスをひとまとめにすることにより、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。
スパニングツリーではなく、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。VCS 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、Brocade's proven 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。FSPF は下記の目的で使われます。

- 任意の２つのスイッチ間で最短で最速のパスを確立することでファブリック全体にわたって動的にルートを計算します。
- 障害発生時に交代パスを選択します。FSPF は複数のパスをサポートし、障害パスを回避して自動的にパスを計算します。これにより、２つの等価なパスが利用できる場合、最適なルートを提供します。

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。
TRILL は、STP の forwarding-blocking モードと比べて、Active-Active モードのマルチパスが利用できます。Active-Active 構成はトラフィックのボトルネックを解消し、クラスタ全体の帯域を使用可能とします。

11.2 VCS ファブリックの形成

クラスタユニットの RBridge ID は、スイッチのドメイン ID と同じです。RBridge ID の割当は、ファイバーチャネル SAN でのドメイン ID 割当プロトコルを拡張して実現されています。
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 のドメイン ID の集中的な割当とファブリック内のドメイン ID 重複の解決を保証します。

NOTE
Network OS v2.0 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。

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"属性を持ったスイッチを探します。

NOTE

もしソフトウェアが"VCS enable"属性を持ったスイッチを見つけられなかった場合、スイッチはスタンドアロンモードに移行し、イーサネットスイッチとして動作します。

- スイッチが 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。
  - VCS ファブリックが利用可能なスイッチが演じポートと接続されているなら、Brocade Link Discovery Process (BLDP)が検出しようとします。更に詳細は、95 ページの『11.2.2　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。
- 一度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ると、Fibre Channel fabric formation protocols (RDI, DIA, and FSPF)の手順が実行されます。更に詳細は、96 ページの『11.2.4　ファブリックの形成』を参照下さい。

11.2.1　　RBridge の動作

RBridge は、リンクステートルーティングプロトコル Hello フレームを交換して、互いを検出します。全てのリンクステートルーティングプロトコルのように、TRILL Hello フレームは、ブリッジで転送されて、RBridge ポートで処理されます。Hello フレームの情報交換を使って、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、送受信オプションのような情報を含みます。指定 RBridge は、リンク上の各 VLAN の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 データフレームにフレームをカプセル化することです。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することです。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未学習のユニキャストやマルチ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、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。

11.2.2　　隣接デバイスの検出

VCS ファブリック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。

11.2.3 Brocade トランク

Brocade トランクは、なんの設定もなしに複数の最適なリンクを自動的に結合するためにハードウェアにビルトインされた特別な独自のリンクアグリゲーションメカニズムです。これらのリンクアグリゲーション手法は、規格に基づく LACP プロトコルとは違っています。トラフィックは、ラウンドロビンでフレームを分散することにより、トランクのメンバー間でロードバランスされます。

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、同一のポートグループで、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 ファイバー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。

ファブリックトランキングは、デフォルトで有効です。もし、ファブリックトランキングを無効にしたい場合は、108 ページの『12.2.7　ポートプロファイルの削除』を参照下さい。

11.2.4 ファブリックの形成

VCS ファブリックは、TRILL ファブリックを構築するため実績のあるファイバーチャネルファブリックプロトコルを拡張したものである。ファブリック形成プロトコルの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。

11.2.5 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、隣接情報を形成し始めて、トポロジと隣接との接続性を収集します。VCS ファブリックは、デフォルトで最も小さい 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。

11.3　VCS ファブリックの構成

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可能です。

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. 現在の設定に基づいて、次のコマンドの一つを入力して VCS ファブリックを有効にします。
   - VCS ファブリックが既に有効な場合、'vcs rbridge ID'コマンドを入力します。有効な RBridge ID は 1 から 239 です。全ての RBridge ID はユニークでなければ成りません。
   - VCS ファブリックが無効の場合、'vcs rbridgeID *rbid* enable'コマンドを入力します。
   - VCS ファブリックが既に有効で、デフォルトではない VCS ID を使う場合、'vcs rbridgeID *rbid* vcsId *vcsid* コマンドを使います。
   - VCS ファブリックが無効で、デフォルトではない VCS ID を使う場合、'vcs rbridgeID *rbid* vcsId *vcsid* enable'コマンドを使います。
2. スイッチが参加しているファブリックに基づいて、スイッチに対するユニークな RBridge ID を選択します。スイッチは一度割り当てられた RBridge ID を記憶しています。
3. システムをリブートします。システムは構成情報をクリアし、プロンプトに'Y'を入力すると自動的にリブートします。リブートの後、スイッチは RBridge ID アロケーションプロトコルを実行し、リブート後に割り当てられたリブート前に手動で設定された値を要求します。

NOTE

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、同様な CLI コマンドを使って新しい RBridge ID を選択してください。

VCS ファブリックの設定を変更するたびに、スイッチはデフォルトコンフィグレーションをリセットし自動的にリブートします。次の'vcs'コマンドを実行する前にコンフィグレーションを格納しているか確かめてください。

- vcs enable
- no vcs enable
- vcs rbridgeId # enable
- vcs vcsId # enable
- vcs vcsID # rbridgeId # enable

11.4　VCS ファブリック設定作業

表 11-1 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 11-1　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

同時にスイッチを無効化し、RBridge ID を設定、VCS ファブリックモードを有効化する場合	`switch# vcs rbridgeId 3 enable`
同時に VCS ID を設定し、VCS ファブリックモードを有効化する場合	`switch# vcs vcsId 1 enable`
スイッチを無効化し、VCS ID と RBridge ID を設定して VCS ファブリックモードを有効化する場合	`switch# vcs rbridgeId 3 vcsId 1 enable`

RBridge ID を 1,VCS ID を 1 に設定し VCS ファブリックモードを有効化し、RBridge ID を 3 に VCS ID を 1 に変更する場合	`switch# vcs enable`
	`switch# vcs rbridgeId 3`
	`switch# vcs vcsId 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`
VCS 設定を表示する場合	`switch# show vcs`
スイッチがスタンドアロンモードならば、'show vcs'コマンドは"disabled"を返します。'show fabric all'コマンドはスタンドアロンモードでは実行できません。	

11.5 ファブリック ISL の設定

VCS ファブリックの物理インタフェースは、エッジポートかファブリックポートのいずれかになります。

'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 のデフォルト設定は、有効です。このため、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、その後 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。この動作は、ISL を Admin Down 状態とし、物理インタフェースを ISDL Down 状態とします。

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、'shutdown'後のリンクがダウンする一方、'no fabric isl enable'後のリンクはアップのままです。

(1) ファブリック ISL の無効化

'no fabric isl enable'コマンドは、ISL の管理状態をダウンとします。ISL として自動検出されたインタフェースには影響がありません｡同じ VCS ID を共有する RBridge 間のポートでは､いつも ISL としてアップしています。'no fabric isl enable'コマンドは、エッジポートには働きません。

1．ファブリック ISL を無効化するために、'config-TenGigabitEthernet-x/x/x'コマンドを入力します。'x/x/x'にはスイッチ/スロット/ポート番号を指定します。
2．'no fabric isl enable'コマンドを入力します。

11.5.2 ファブリックトランク

Network OS v2.0 は、Brocade トランクをサポートしています。トランクの形成は、有効化・無効化することを除いてユーザの介入や設定を必要としません。スイッチソフトウェアは、グローバルレベルかどうかに係らず、トランクを形成します。

(1) 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。
ファブリックトランキングを再び有効化するために、'fabric trunk enable'コマンドを入力します。

11.5.3 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

Fabric Shortest Path First (FSPF)は、ファイバーチャネルファブリックで使われる標準的なパス選択プロトコルです。ファイバチャネルスイッチでは、FSPF 機能は、デフォルトで有効です。FSPF はファブリックにある２つのスイッチ間の最適パスを自動的に計算します。
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(BUM)は、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のルート選択

Network OS v2.0 は、次の分配ツリー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。マルチキャストルートが最も低い RBridge ID を持たない特定のスイッチになることを要求している場合、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選ばれる。
- バックアップマルチキャストルートは事前に選択されています。そして、それは次に高いプライオリティを持ったスイッチか、次に高いプライオリティを共有している残りのスイッチのうち最も小さい RBridge ID を持ったスイッチです。バックアップマルチキャストルートは、全てのスイッチが現在のマルチキャストルートが障害となった場合自動的に選択されます。

11.5.4 プライオリティ

ツリーのルートは、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、プライオリティを設定することが出来ます。(デフォルトは 0)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、0 より大きい値をプライオリティに設定します。(プライオリティは、0 から 255 です。) もし、プライオリティに関係があると、最も小さい RBridge ID はまた選択されたままです。例えば、もし RBridge ID 7 と 8 が両方ともプライオリティ 10 に設定されていれば、7 がルートになります。7 がファブリックからなくなると、8 がルートになります。その後、8 がファブリックからなくなると、1 がルートになります。

(1) RBridge ID プライオリティの変更

RBridge ID プライオリティを変更するため、'fabric route multicast rbridgeId'コマンドを入力します。

```
switch(config)# fabric route mcast rbridgeId 7 priority 10
```

11.5.5 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。

---

running configuration を表示するために、'show running-config fabric route mcast'コマンドを使います。

```
switch# show running-config fabric route mcast
```

12 AMPP の設定

12.1 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 ポートのポートプロファイルの自動マイグレーションを可能とすることで、VEB ポートプロファイルは一緒に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スイッチとサーバ仮想化インフラでサポートされるアクセスと QoS 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で動作するベアメタル OS が別のシステムに移動するオペレーティングシステムのように、物理的なものかもしれません。このマイグレーションは、また、あるシステム上の VMware 上で動作すして別のシステムの VMware で動作するオペレーティングシステムのような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、移動に対応した高度な制御を提供し、ポートプロファイルの関係を移動させます。

12.2 AMPP ポートプロファイルの構成

図 12-1 に示す通り、デフォルトのポートプロファイルは、VM が LAN にアクセスするために必要な構成全部を含んでいます。

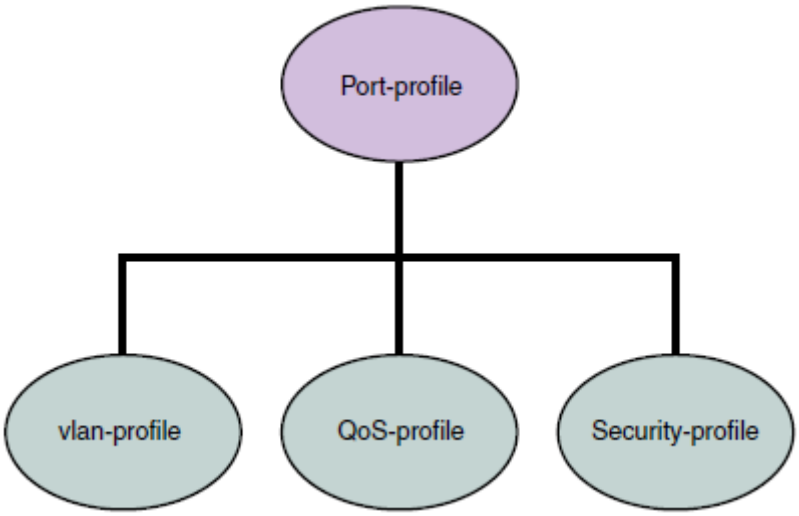

図 12-1 ポートプロファイルの内容

加えて、全ての組合せはセキュリティプロファイルの下、グループ化された幾つかのセキュリティルールと混合することができます。

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持っていません。

ポートプロファイルは、自給自足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。
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。

12.2.1 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、多数の状態を考慮します。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されたが、完全ではない状態を示します。ポートプロファイルが作成または修正された時です。
- 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全なものでなく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。任意のシグナリングプロトコルが欠如している状態で、システムは関連付けられた MAC アドレスが profiled ポートに現れないかを検出するため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、profiled ポートに共存できます。しかし、競合があると後のポートプロファイルの使用時に失敗となります。

表 12-1 に、AMPP イベントと AMP の動作及び適用できる操作を示します。

表 12-1 AMPP の動作及びユーザ操作

AMPP イベント	AMPP の動作と適用できるユーザ操作
Create port-profile	•ポートプロファイルが存在しない場合、生成されます。存在しているがまだ有効化されてない場合、修正可能です。
Activate port-profile	•ポートプロファイルが完全に構成されていなければ、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。 •全ての依存関係が評価されたなら、ポートプロファイルは ACTIVE 状態となり、関連付け可能な状態です。
De-activate port-profile	•このイベントは全てのポートから適用されたポートプロファイルの構成を削除します。 •MAC アドレスがポートプロファイルに関連付けれれてい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 状態に設定されます。 •ポートプロファイルは INACTIVE 状態に設定され、プロファイルの MAC アドレスへの関連付けが許容されません。
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、AMPP は 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ることを許可しません。 •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備えた MAC アドレスを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、プロファイルの削除は全ての MAC との関係を削除します。
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。

12.2.2 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)は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．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
Entering configuration mode terminal
switch(config)#port-profile vm1-port-profile
switch(config-pp)#vlan-profile
switch(conf-pp-vlan)#switchport trunk native-vlan 300
switch(conf-pp-vlan)#switchport trunk allowed vlan add 300
```

2．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
```

3．プロファイルを有効化します。

```
switch(config)#port-profile vm1-port-profile activate
```

4．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
```

12.2.3 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 v2.0 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(conf-pp)#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(conf-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(conf-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(conf-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(conf-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．変更したいインターフェースインターフェースのインターフェース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．物理インターフェースインター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)#
```

12.2.4 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つの側面を持ちます。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。
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(conf-pp)#qos-profile
switch(conf-pp-qos)#
```

３．CEE マップを適用します。

```
switch(conf-pp-qos)#cee default
```

４．デフォルト CoS 値を設定します。

```
switch(conf-pp-qos)#qos cos 7
```

５．CoS に対する QoS トラスト属性を設定します。

```
switch(conf-pp-qos)#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(conf-pp-qos)#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(conf-pp-qos)#qos cos-traffic-class vm1-cos2traffic-map
```

７．下記いずれかの Pause 機能を有効にします。

- PFC なし

```
switch(conf-pp-qos)#qos flowcontrol tx on rx on
```

- 各 CoS 値に対する PFC 付

```
switch(conf-pp-qos)#qos flowcontrol pfc 1 tx on rx on
switch(conf-pp-qos)#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(conf-pp-qos)#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．変更したいインターフェースインターフェースのインターフェース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．物理インターフェースインター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)#
```

12.2.5　　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、サーバー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(conf-pp)#security-profile
switch(conf-pp-security)#
```

3．ACL セキュリティ属性を修正します。詳細は 168 ページの『18 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(conf-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(conf-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．プロファイルに MAC アドレスを割り当てます。

```
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．変更したいインターフェースインターフェースのインターフェース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
```

9．物理インターフェースインター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)#
```

12.2.6　　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．変更したいインターフェースインターフェースのインターフェース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．物理インターフェースインター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
```

12.2.7　　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
Entering configuration mode terminal
switch(config)#
```

2．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
```

12.3　AMPP プロファイルの参照

AMPP プロファイルを参照するため、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
```

13 VLAN の設定

13.1 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 は物理的な位置に影響を受けない共通集合の要件を持っている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、インターフェース毎に設定できます。

13.2 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

native VLAN でタグ無しフレームを取り扱うためには、'no vlan dot1q tag native' を設定してください。

NOTE

入力の VLAN フィルターは、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 13-1 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。

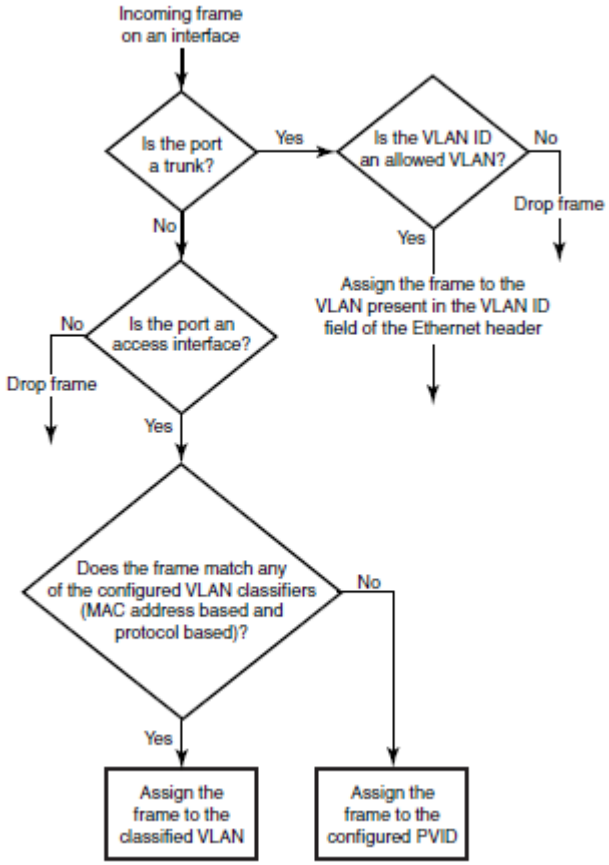

図 13-1 入力の VLAN フィルタ

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 メンバーに依存します。
- ポートの VLAN メンバーは 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。(ポートが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、44 ページの『4　レイヤ２イーサネットの概要』を参照下さい。

13.3　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。
- NOS 2.0 では、利用可能な VLAN 数は 1024 個までとなっています。1024 個以上定義した場合は、エラーの原因となる場合がありますのでご使用なさらないで下さい。

13.4　デフォルト VLAN 設定

表 13-1 はデフォルト VLAN の構成を示しています。

表 13-1 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
VLAN インタフェース割当	全インタフェース VLAN1 所属
VLAN 状態	アクティブ
MTU サイズ	2500bytes

13.5　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。

13.5.1 インタフェースポートの有効化・無効化

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。

```
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
```

13.5.2 インタフェースポートの MTU 設定

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
```

13.5.3 VLAN インタフェースの生成

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 3583 が利用できます。VLAN ID 3584 から 4094 はシステムで予約しています。

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．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。
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 1002
```

13.5.4 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 の全てのメンバーに対して Spanning Tree Protocol (STP)を有効にすることが出来ます。どのプロトコルでも、VLAN 単位に選択することが出来ます。一つのタイプの STP だけが同時に使用できます。
物理インタフェースポートは、複数 VLAN のメンバーとなります。例えば、物理ポートは、同時に VLAN 1002 と VLAN 55 のメンバになります。加えて、同時に VLAN1002 が STP 有効で VLAN55 が STP 無効とすることができます。

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
```

13.5.5 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 の全てのメンバーの 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 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)#interface vlan 55
```
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
```

13.5.6 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．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．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．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．running configuration のインタフェースの状態を表示するため、'do show command'コマンドを実行します。

```
switch(conf-if-te-0/1)#do show running-config interface
tengigabitethernet 0/1
```

13.5.7　　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．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．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 command'を入力します。

```
switch(conf-if-te-0/1)#switchport access vlan 20
```

13.5.8　　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．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．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．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
```

13.5.9　　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．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．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．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
```

13.6　プロトコルベース VLAN の分類ルールの構成

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。(119 ページの『13.6.4　VLAN classifier グループと付加ルールの生成』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)
- Fibre Channel over Ethernet (FCoE)
- FCoE Initialization Protocol (FIP)
- 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。

13.6.1 VLAN classifier ルールの生成

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 fcoe encap ethv2
```

13.6.2 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
```

13.6.3 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
```

13.6.4 VLAN classifier グループと付加ルールの生成

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 を生成してとルールを追加します。

```
switch(config)#vlan classifier group 1 add rule 1
```

13.6.5 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．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 0/10
```

3．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。

13.6.6 VLAN 統計情報のクリア

VLAN 統計情報をクリアするため、'clear'コマンドを入力します。VLAN_ID には 1 から 3583 が指定できます。
VLAN 統計情報をクリアする例

```
switch#clear counter interface vlan 20
```

13.6.7 VLAN 情報の表示

VLAN 情報を表示するため、特権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 brief
```

13.7 MAC アドレステーブルの設定

各ポートは 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。本装置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、残留した MAC アドレスは、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、44 ページの『4　レイヤ２イーサネットの概要』を参照下さい。

13.7.1 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
```

13.7.2 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塚するため、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、VLAN10 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
```

14 スパニングツリーの設定

14.1 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ーをスパニングツリートポロジーへ変更します。ネットワークスイッチは、ネットワークトポロジー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。
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。
- 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 142 ページの「14.8.4　guard root の設定」を参照下さい。
- PortFast BPDU guard と BPDU filter - 詳細は、144 ページの「14.8.8　port fast(STP)の有効化」を参照下さい。

14.1.1　　STP の構成

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、131 ページの『14.7.1　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、132 ページの『14.7.4　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、144 ページの『14.8.8　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。

```
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、142 ページの『14.8.4　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、131 ページの『14.7　スパニングツリーの構成と管理』を参照下さい。

14.2　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 の高速再構築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 の障害時に高速再構築が可能になります。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 14-1 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 14-1 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げが、代替・バックアップポートが参加していない有効なトポロジの一部となります。

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、131 ページの『14.7　スパニングツリーの構成と管理』を参照下さい。。

14.2.1　　RSTP の構成

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、131 ページの『14.7.1 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、132 ページの『14.7.4　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、133 ページの『14.7.5　ブリッジ転送遅延時間の設定』を参照下さい。

```
switch(conf-stp)#forward-delay 20
```

5．'bridge maximum aging time'を指定します。詳細は、133 ページの『14.7.6　bridge maximum aging time の設定』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、134 ページの『14.7.7　error disable timeout timer』を参照下さい。

```
switch(conf-stp)#error-disable-timeout enable
```

７．'error-disable-timeout interval'を設定します。134 ページの『14.7.8　error disable timeout interval』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、135 ページの『14.7.9　port-channel path cost』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、135 ページの『14.7.10　bridge hello time』を参照下さい。

```
switch(conf-stp)#hello-time 5
```

１０．VLAN FDB から MAC アドレスを削除します。詳細は、139 ページの『14.7.18　MAC アドレス(RSTP/MSTP)の破棄』を参照下さい。

```
switch(config)#spanning-tree tc-flush-standard
```

１１．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、144 ページの『14.8.8　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。

```
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。

１２．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、144 ページの『14.8.9　ポートプライオリティの設定』を参照下さい。

１３．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、142 ページの『14.8.4　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。

１４．特権実行モードに戻ります。

```
switch(config)#end
```

１５．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
```

14.3 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支援します。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
16 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

ョンを跨って動作すし、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。

14.3.1 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する。

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、131 ページの『14.7.1　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、138 ページの『14.7.16 MSTP』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、138 ページの『14.7.17 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、137 ページの『14.7.14　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、インター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、137 ページの『14.7.15　BPDU(MSTP)最大 hop 数の設定』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
```

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
```

MSTP に関する更に詳細な情報は、131 ページの『14.7　スパニングツリーの構成と管理』を参照下さい。

14.4　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ー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、すぐにどんどん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。

NOTE
このドキュメントでは、以降 PVST と RPVST という言葉を使用します。

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。
PVST や Rapid PVST を構成するために、パラメータとして VLAN ID を付加して、標準的な STP コマンドを使います。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 8 vlan 10
switch(conf-pvst)#forward-delay 4 vlan 10
switch(conf-pvst)#hello-time 2 vlan 10
switch(conf-pvst)#max-age 7 vlan 10
switch(conf-pvst)#mac-address-reduction enable
```

14.5 設定のガイドラインと制限

スパニングツリーを構成する場合、次のガイドラインと制限に従ってください。

- 異なるスパニングツリーのタイプを有効にする前にスパニングツリーを無効にしなければなりません。
- もしパラレルリンクの両サイドの全ての接続デバイスでスパニングツリーを有効にしない場合、パケットドロップやフラッディングが発生する可能性があります。
- LAG は通常の接続として扱われデフォルトではスパニングツリーが有効です。
- 16MSTP 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 インスタンスにマッピングする前に VLAN を作成してください。
- MSTP の'force-version'オプションはサポートしていません。
- ネットワーク上の冗長パスを跨るロードバランスを働かせために、全ての VLAN-インスタンスマッピングが一致してなければなりません。さもないと、全てのトラフィックは単一のリンク上に流れます。
- 'protocol spanning-tree mstp'グローバルコマンドで MSTP を有効にする時、RSTP は自動的に有効になります。
- 同一 MSTP リージョンにある２つ以上のスイッチには、同一の VLAN-インスタンスマップ、同一のレビジョン番号、同一の名前を定義する必要があります。
- スパニングツリートポロジは、サーバが直接接続している FCoE トラフィックが動作するような 10G イーサネットポートには有効にしてはいけません。これは FCoE ログインの失敗という結果になるかもしれません。

14.6　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、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 を参照下さい。

表 14-2 に、STP 構成のデフォルト値を示します。

表 14-2 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	By default, STP, RSTP, and MSTP are disabled
Bridge priority	32768
Bridge forward delay	15 seconds
Bridge maximum aging time	20 seconds
Error disable timeout timer	Disabled
Error disable timeout interval	300 seconds
Port-channel path cost	Standard
Bridge hello time	2 seconds
Flush MAC addresses from the VLAN FDB	Enabled

表 14-3 に、MSPT のみを設定下場合のデフォルト値を示します。

表 14-3 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	Disabled
Switch priority (when mapping a VLAN to an MSTP instance)	32768
Maximum hops	20 hops
Revision number	0

表 14-4 に、10GbE DCB インタフェースのデフォルト値を示します。

表 14-4 10Ge 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	Disabled on the interface
Automatic edge detection	Disabled
Path cost	2000
Edge port	Disabled
Guard root	Disabled
Hello time	2 seconds
Link type	Point-to-point
Port fast	Disabled
Port priority	128
DCB interface root port	Allow the DCB interface to become a root port
DCB interface BPDU restriction	Restriction is disabled

14.7 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。

14.7.1 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, Rapid-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
```

14.7.2 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, Rapid-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
```

14.7.3 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, Rapid-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
```

14.7.4 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この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セ託します。
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１がスイッチ２が広告する root ID より低い番号となる root ID を広告するならば、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。

NOTE
各 VLAN が異なるブロードキャストドメインにある場合、VLAN 毎にルートスイッチが必要です。

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, Rapid-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
```

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
```

14.7.5 ブリッジ転送遅延時間の設定

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)
```

ブリッジ転送遅延を指定するために、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．STP, RSTP, MSTP, PVST, Rapid-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してします。

```
switch(conf-stp)#forward-delay 20
```

14.7.6 bridge maximum aging time の設定

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。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)
```

'bridge maximum aging time'を指定するため、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．STP, RSTP, MSTP, PVST, Rapid-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
```

14.7.7　　error disable timeout timer の有効化

STP,RSTP,MSTP のどのモードでも、ポートを disable 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 disable 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 disalbe のままです。このコマンドにより、ポートを disable 状態から有効化することが出行きます。'error disable timeout interval'設定の詳細については、134 ページの『14.7.8　error disable timeout interval』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, Rapid-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．'error disable timeout timer'を有効化します。

```
switch(conf-stp)#error-disable-timeout enable
```

14.7.8　　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, Rapid-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
```

14.7.9 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, Rapid-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
```

14.7.10 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)
```

'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, Rapid-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'の送信間隔を秒指定します。

```
switch(conf-stp)#hello-time 5
```

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
```

14.7.11　　transmit hold count (RSTP and MSTP)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
```

14.7.12　　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この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
```

14.7.13　　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
```

14.7.14　　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このコマンドを使用します。VLAN の集合をインスタンスに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出来ます。VLAN インスタンスマッピングは、含まれる 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 4096
```
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
```

14.7.15　　BPDU(MSTP)最大 hop 数の設定

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
```

14.7.16 MSTP リージョン名称の設定

MSTP モードで、MSTP リージョン名称を設定す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
```

14.7.17 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
```

14.7.18　　MAC アドレス(RSTP/MSTP)の破棄

RSTP と MSTP に対して、VLAN filgering database (FDB)から MAC アドレスを破棄するためにこのコマンドを使用します。VLAN FDB は、受信フレームの転送先を決定します。VLAN FDB は、MAC アドレスと VLAN ID に基づく到着フレームの転送を決定する情報を含みます。(113 ページの『13.3 VLAN 設定のガイドラインと制限』を参照下さい。)

MAC アドレスの破棄には２つの方法があります。

- 標準的な方法 - ポートでトポロジチェンジフラグを持った BPDU フレームを受信した場合、スイッチの他のポートの FDB を破棄します。もし、トポロジチェンジフラグを持った BPDU フレームが継続的に受信されると、スイッチは FDB を破棄し続けます。この挙動はデフォルトの挙動です。
- Brocade 独自の方法 - この方法では、FDP は最初と最後のトポロジチェンジフラグを持った BPDU に対してだけ破棄します。

両方の方法とも、トポロジチェンジフラグを持った BPDU を受信した時に FDB を破棄しますが、Brocade 独自の方法は破棄回数を低減することができます。

VLAN FDBkaraMAC アドレスを破棄するために、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．アドレスをどのように破棄したいかにより、適切な'spanning-tree'コマンドを入力します。
   - 標準的な方法で MAC アドレスを破棄する

     ```
     switch(config)#spanning-tree tc-flush-standard
     ```
   - Brocade 独自の方法で MAC アドレスを破棄する。

     ```
     switch(config)#no spanning-tree tc-flush-standard
     ```

14.7.19　　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．全てのインター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 やポート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
   ```

14.7.20　　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．全てのインター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 やポート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
```

14.7.21　　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。

14.8　ポート毎の STP, RSTP, MSTP の設定

この章では、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, rapid PVST をサポートしています。

14.8.1　　自動エッジ検出機能の有効化

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。

インタフェースでの自動エッジ検出機能を有効化するため、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．インタフェースのタイプと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．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．インタフェースでの自動エッジ検出機能を有効化するため'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)#spanning-tree autoedge
```

14.8.2　　パスコストの設定

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。デフォルトは、2000 です。

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．インタフェースのタイプと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．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 cost
```
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
```

14.8.3　　エッジポートの設定

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。(144 ページの『14.8.8　port fast(STP)の有効化』を参照下さい。)

インタフェースをエッジポートに指定するため、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．インタフェースのタイプと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．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
```

14.8.4　　guard root の設定

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。

インタフェースに guard root を設定するために、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．インタフェースのタイプと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．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 guard root 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 guard root
```

14.8.5　　MSTP hello time の設定

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指定します。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。(133 ページの『14.7.6　bridge maximum aging time の設定』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。

インタフェースに MSTP hello time を設定するため、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．インタフェースのタイプと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．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 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
```

14.8.6 MSTP インスタンスの制限の指定

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。

MSTP インスタンスの制限を指定するためこ、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．インタフェースのタイプと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．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 cost 3550
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
```

14.8.7 リンクタイプの設定

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。

インタフェースにリンクタイプを指定するために、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．インタフェースのタイプと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．インタフェースをリンクタイプを設定するため、'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
```

14.8.8　　port fast(STP)の有効化

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。

MSTP と RSTP には'spanning-tree edgeport'コマンドを使用下さい。(141 ページの『14.8.3　エッジポートの設定』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．インタフェースのタイプと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．インタフェースをリンクタイプを設定するため、'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
```

14.8.9　　ポートプライオリティの設定

インタフェースで、ポートプライオリティを設定するため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。

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．インタフェースのタイプと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．インタフェースをリンクタイプを設定するため、'no shutdown'コマンドを入力します。
4．インタフェースにの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
```

14.8.10　　ルートポート遷移の抑止

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、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．インタフェースのタイプと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．インタフェースをリンクタイプを設定するため、'no shutdown'コマンドを入力します。
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
```

14.8.11　　トポロジチェンジ通知の抑止

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．インタフェースのタイプと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．インタフェースをリンクタイプを設定するため、'no shutdown'コマンドを入力します。
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
```

14.8.12　　スパニングツリーの有効化

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．インタフェースのタイプと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．インタフェースをリンクタイプを設定するため、'no shutdown'コマンドを入力します。
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
```

14.8.13　　スパニングツリーの無効化

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．インタフェースのタイプと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．インタフェースをリンクタイプを設定するため、'no shutdown'コマンドを入力します。
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
```

15 リンクアグリゲーションの設定

15.1 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。

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
- 高速な構成設定と再構成

本スイッチはハードウェアレベルで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
- 動的名標準 LAG

15.1.1 リンクアグリゲーショングループの設定

本装置では標準 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

本装置での各リンクは一つの LAG と関連付けることができるが、一つ以上の 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。

15.1.2 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 にまとまます。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。

15.1.3 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。

15.1.4 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。

15.1.5 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、リンクメンバー間のファイバー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。

15.1.6 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

15.2 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。

15.2.1 vLAG の構成

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、147 ページの『15.1.1 リンクアグリゲーショングループの設定』を参照下さい。一度、VCS ファブリックが LAG 構成が多数のスイッチ間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。

2. FCoE MAC アドレスが LAN トラフィックに類似したマルチホームホストとして扱われるよう各 vLAG を設定します。
   デフォルトコンフィグは FCoE を非 vLAG トラフィックとして扱います。vLAG の全てのポートチャネルでこのコマンドを実行しなければなりません。

```
switch(config)#interface port-channel 10
```

3. 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
```

4. 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 ?
Aggregator Po 10 (vLAG)
Member switches:
RBridge id 1 (4)
RBrideid 2 (4)
Actor System ID -0x8000,01-e0-52-00-01-00
Actor System ID Mapped Id: 0
Admin Key: 0010 -OperKey 0010
Receive link count: 4 -Transmit link count: 4
Individual: 0 -Ready: 1
Partner System ID -0x0001,01-80-c2-00-00-01
Link: Te 1/0/21 (0x18150014) sync: 1
Link: Te 1/0/22 (0x18160015) sync: 1 *
Link: Te 1/0/23 (0x18170016) sync: 1
Link: Te 1/0/24 (0x18180017) sync: 1
```

5. 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 operport: 100
```

15.3 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。

- 本装置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 ― "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 として定義できます。

15.4　デフォルト LACP 構成情報

表 15-1 はデフォルトの LACP 構成情報を一覧しています。

表 15-1 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

15.5　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。

15.5.1　　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．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．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 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
```

15.5.2　　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
```

15.5.3 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．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．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．インタフェースのタイムアウト時間を指定します。

```
switch(conf-if-te-0/1)#lacp timeout short
```

15.5.4 LAG 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
```

15.5.5 全 LAG グループの LAG 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、'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
```

15.5.6 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 Operating System Command Reference』を参照してください。

15.6　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。
IEEE802.3 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。いずれ一方がアクティブでなければなりません。
- 両装置の port-channel インタフェースが"up"状態となっているか確認する。
- LAG のポートが同一スイッチに接続されているか確認する。
- スイッチのシステム ID がユニークかを確認する。'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。

16 NIC 冗長(track)の設定

16.1 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。

16.2 NIC 冗長(track)の構成

16.2.1 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 0/5
```

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
NOS 2.0 では、track 機能を設定し物理ポートを監視対象に指定した後、監視対象ポートがリンクダウンすると、’running-config’上の track 指定したポート状態が’shutodwn’となります。この状態になった場合は、’startup-config’に格納する場合は、track 指定したポートを’no shutdown’に再設

定してください。

16.2.2 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 0/5
```

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
```

16.2.3 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 0/5
```

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
```

17 LLDP の設定

17.1 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。

17.2 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 拡張を負荷しています。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 を含む。
  - 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。

17.3　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と特徴に互いに影響します。

- 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、LLCP 基盤上に構築されれている。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"

17.3.1 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なわず、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 17-1 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 17-1 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 17-1 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

17.3.2 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。

17.4　他社ベンダデバイスとの DCBX 相互作用

内蔵 DCB スイッチが他社ベンダデバイスと接続される時、他社ベンダデバイスは、内蔵 DCB スイッチと同じ DCBX バージョンをサポートしてないかもしれない。内蔵 DCB スイッチは、２つの DCBX バージョンをサポートしています。

- CEE バージョン(1.0.1) - DCB 規格に基づくバージョン
- Pre-CEE バージョン

異なる DCBX バージョンに適用するために、内蔵 DCB スイッチは次のポイントを支援します。

- Auto-sense(plug and play)

これがデフォルトです。内蔵 DCB スイッチハードウェアは、隣接との接続及び CEE バージョンと pre-CEE バージョンとの自動的な切替により使用されるバージョンを検出します。

- CEE バージョン

Auto-sense をオフにして、強制的に CEE バージョンを使用します。

- Pre-CEE バージョン

Auto-sense をオフにして、強制的に Pre-CEE バージョンを使用します。

17.5　LLDP 設定のガイドラインと制限

LLDP を設定する時、LLDP 構成のガイドラインと制約に従ってください。

- Brocade の LLDP あｈ、標準的な LLDP 情報に加えて、Brocade が規定する TLV の交換をサポートしています。
- 必須 TLV はいつも広告されます。
- LLDP リンクレベルパラメータの交換は、その他のレイヤ２プロトコルに透過です。LLDP リンクレベルパラメータは、その他の関連するプロトコルに LLDP により通知されます。

NOTE

DCBX 構成は、広告される DCBX 関連の TLV 構成を単純に含むものです。詳細な情報は、161 ページの『17.7　LLDP の構成と管理』に記載しています。

17.6　デフォルト LLDP 構成情報

表 17-2 にデフォルト LLDP 構成情報を示します。

表 17-2 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

17.7　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。

17.7.1　　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 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
```

17.7.2　　装置全体の LLDP の無効化・リセット

'protocol lldp'コマンドは、'protocol lldp'を使って設定した全ての設定を表示します。LLDP はデフォルトで有効となっています。
LLDP を全体で無効化及び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 を無効化します。

```
switch(config)#no protocol lldp
```

17.7.3　　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。

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

NOTE

もし、'advertise optional-tlv'コマンドがキーワード無しで入力された場合は、全てのオプション TLV が広告されます。

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

NOTE
デフォルトでは、'dot1-tlv', 'dot3-tlv', 'dcbx-fcoe-app-tlv', 'dcbx-fcoe-logical-link-tlv'という DCBX 関連 TLV は広告されません。

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
```

(9)　下記のコマンドを使って、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`

(10)　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 p ら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
```

4．TLV を広告します。

```
switch (conf-lldp)#advertise dcbx-isci-app-tlv
```

(11)　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'コマンドを使うと、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．プロファイル名称の設定

```
switch(conf-lldp)#profile UK_LLDP_IT
```

４．プロファイルのディスクリプションの指定

```
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)#mode tx rx
```

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
```

(12)　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、優先ビットは各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．もしまだ生成されていなければ cee-map を作成します。

```
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
```

2．LLDP 構成モードに移行します。

```
switch(conf-ceemap)#protocol lldp
```

3．iSCSI の LLDP プロファイルを生成します。

```
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ステップ５から７を繰り返します。

```
switch(conf-if-te-0/1)#interface te 0/7
switch(conf-if-te-0/7)#cee default
switch(conf-if-te-0/7)#lldp profile iscsi_config
switch(conf-if-te-0/7)#lldp iscsi-priority-bits 5
```

17.7.4　　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、装置のコンフィグレーションが使われます。もし、装置の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 プロファイルを割り当てます。

```
switch(conf-if-te-0/10)#lldp profile network_standard
```

3．DCB インタフェースに対して DCBX バージョンを設定します。これらのバージョンコマンドのキーワードの詳細な情報は、160 ページの『17.4　他社ベンダデバイスとの DCBX 相互

作用』を参照下さい。デフォルトは DCBX バージョンを自動的に検出します。

```
switch(conf-if-te-0/10)#lldp version cee
```

4．特権実行モードに戻ります。

```
switch(conf-if-te-0/10)#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
```

17.7.5 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 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 tengigabitethernet 0/1
```

17.7.6 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
```

18 アクセスコントロールリスト(ACL)の設定

18.1 ACL 概要

NOTE
Network OS v2.0 は、レイヤ２MAC アクセスコントロールリスト(ACL)のみサポートしています。

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。VLAN やレイヤ２インタフェースに ACL を適用することが d 系ます。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(LAGs)
- VLAN

18.2 デフォルト ACL 設定

表 18-1 にデフォルトの ACL 設定を示します。

表 18-1 デフォルト MAC ACL 設定

パラメータ	デフォルト設定
デフォルト定義の MAC ACL	設定なし

18.3 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。最初のルールはトラフィックにマッチすると、フレームへの以降の処理が行われません。
- 標準 ACL と拡張 ACL は同じ名称にできません。

18.4 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。

18.4.1 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、171 ページの『18.4.5 MAC ACL のシーケンス番号の並び替え』を参照下さい。

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 MAC ACL の名称は"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
```

18.4.2　　拡張 MAC ACL の生成とルールの追加

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、171 ページの『18.4.5　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。
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
```

18.4.3　　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。
もし現在許可されているシーケンス番号の間にルール追加したい場合は、シーケンス番号を再設定するために'seq'コマンドを使います。詳細は、171 ページの『18.4.5　MAC ACL のシーケンス番号の並び替え』を参照下さい。
修正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 (config)#no seq 100
```

4．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
```

18.4.4 MAC ACL の削除

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
```

18.4.5 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できます。シーケンス番号を並び替えは、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。

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
```

18.4.6 ポートへの MAC ACL の割当

適用したい ACL が存在して、そのポートで必要となるトラフィックをフィルタするよう設定されているかを確認してください。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。ポートで受信されるフレームはフィルタされます。

ポートに MAC ACL を適用するため、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．ポートのタイプと番号を指定して'interface'コマンドを入力します。

```
switch(config)#interface tengigabitethernet 0/1
```

3．ポートをレイヤ２スイッチポートとして定義するため、'switchport'コマンドを入力します。

4. レイヤ２ポートの入力に適用する MAC ACL を指定するため、'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
```

18.4.7 VLAN インタフェースへの MAC ACL 適用

適用したい ACL が存在して、その VLAN で必要となるトラフィックをフィルタするよう設定されているかを確認してください。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(conf-if-vl-82)# mac access-group test_02 in
```

19 QoS の設定

19.1 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 の目的は各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。

19.2 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る。

19.3　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することで開始する。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つに割り当てられる。

19.3.1　　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)信頼されない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、信頼できないと設定された場合は、デフォルトで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。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 19-1 は、レイヤ２での QoS における信頼できないユーザプライオリティのマッピングです。

表 19-1 信頼できない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は上書きすることが出来ます。隣接デバイスが信頼できて、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 19-2 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 19-2 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 の信頼モードでの構成方法
QoS の信頼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 の信頼モードコマンドは使用できません。CEE マップは CoS 信頼モードのインタフェースに対して適用できます。

QoS 信頼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入ります。

```
switch#configure terminal
```

2．10 gigabit Ethernet interface を指定します。

```
switch(config)#interface tengigabitethernet 0/2
```

3．インタフェースモードを'trust'に設定します。

```
switch(conf-if-te-0/2)#qos trust cos
```

4．特権実行モードに戻ります。

```
switch(conf-if-te-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
```

(3)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入ります。

```
switch#configure terminal
```

2．10 gigabit Ethernet interface を指定します。

```
switch(config)#interface tengigabitethernet 0/2
```

3．インタフェースモードを'3'に設定します。

```
switch(conf-if-te-0/2)#qos cos 3
```

4．特権実行モードに戻ります。

```
switch(conf-if-te-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
```

(4)CoS-to-Cos 変換マップの作成

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入ります。

```
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
```

3．特権実行モードに戻ります。

```
switch(conf-if-te-0/2)#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
```

(5)CoS-to-CoS 変換マップの適用

CoS-to-CoS 変換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入ります。

```
switch#configure terminal
```

2．10 gigabit Ethernet interface を指定します。

```
switch(config)#interface tengigabitethernet 0/2
```

3．CoS-to-CoS 変換マップを有効化または変更を適用する。下記例では'test'を使用。

```
switch(conf-if-te-0/2)#qos map cos-mutation test 0 1 2 3 5 4 6 7
```

4．入力トラフィックに対して信頼モードを指定

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 信頼モードを指定す

るこのコマンドを使います。信頼モードで無い場合、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-0/2)#qos trust cos
```

5．特権実行モードに戻ります。

```
switch(conf-if-te-0/2)#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
```

19.3.2 トラフィッククラスマッピング

当装置は、分離とアプリケーションデータに対して異なる優先度の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 19-3 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 19-3 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駆用されます。

(2)マルチキャストトラフィック
当装置は、分離とアプリケーションデータに対して異なる優先度の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 19-3 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 19-4 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	0
1	0
2	1
3	1
4	2
5	2
6	3
7	3

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駆用されます。

(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。

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)CoS-to-Traffic-Class マッピングの有効化
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
```

2．10 gigabit Ethernet interface を指定します。

```
switch(config)#interface tengigabitethernet 0/2
```

3．名称を指定して CoS-to-Traffic-Class マッピングを有効化します。

```
switch(conf-if-te-0/2)#qos cos-traffic-class test
```

4．特権実行モードに戻ります。

```
switch(conf-if-te-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
```

(5) CoS-to-Traffic-Class マッピングの確認

CoS-to-Traffic-Class マッピングを確認するため、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．名称とマッピングを指定することにより、CoS-Traffic-Class マッピングを確認します。

```
switch(config)#show qos map cos-traffic-class test
```

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
```

19.4 輻輳制御

19.4.1 Tail drop

Tail drop 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 設定が無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 19-1 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る。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る。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。

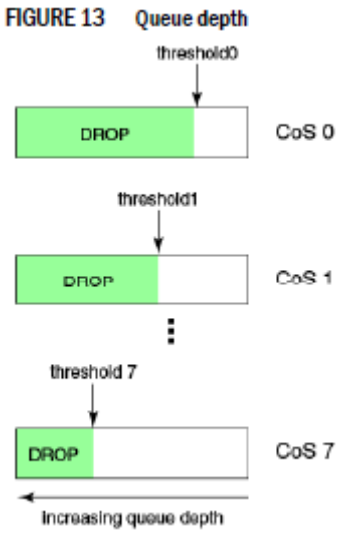

図 19-1 キューの深さ

(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 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
```

19.4.2 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 メッセージは付加的な 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 Pause 番号を持っています。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。標準的な仕組みを使って、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 では決定されません。
- 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)Pause の有効化

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
```

2．10 gigabit Ethernet interface を指定します。

```
switch(config)#interface tengigabitethernet 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-0/2)#qos flowcontrol tx on rx on
```

4．特権実行モードに戻ります。

```
switch(conf-if-te-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
```

19.4.3　　イーサネット優先フロー制御

キューは、幾つかの理由で溢れることがあります。例えば、リンクのオーバーサブスクリプションや下流デバイスからのバックプレッシャーです。大きなキューを構成すると、一般的にネットワーク上の輻輳発生を意味し、キュー滞留時間の増加、フレームロスなどからアプリケーションのパフォーマンスに影響を与えます。

輻輳制御は、輻輳が発生した時にシステムがどのように応答し、ネットワークが輻輳状態に陥ることから防ぐ方法を含んでいます。

19.5　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、同一の受信キューが使用されるので、受信キューへの入力時(第一段階拡張)と出力時(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。

19.5.1　　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
```

19.6　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。本装置では、絶対優先(Strict Priority:SP)スケジューリングと不足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。

19.6.1　　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し続ける前に、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を使い尽くすポテンシャルがあることです。

図 19-2 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。

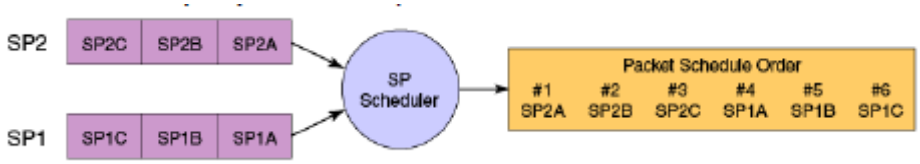

図 19-2 2つのキューでの SP スケジューリング

19.6.2 不足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る。WRR はそれぞれのキューに重み付けを行う。その値は、キューに割り付けられた帯域の合計を決定する。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する。

図 19-3 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る。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る。図 19-3 の WRR2 は帯域の６６%を受信し、WRR1 は３３%受信する。

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く。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る。

図 19-3 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。

19.6.3 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。本装置では、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(8 を経由した SP1)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はWRRサービスとなります。表 19-5 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 19-5 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 19-4 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 19-4 SP スケジューラと WRR スケジューラ

19.6.4 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 scheduler strict-priority 4 dwrr 10 20 30
40
```

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
```

19.6.5　　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。

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受け継がれる。正確なマッピングの等価性の詳細については、184 ページの表 19-5 を参照下さい。

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を同時にサポートする複合スケジューラを利用します。

(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 30 40
```

3．特権実行モードに戻ります。

```
switch(conf-if-te-0/2)#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
```

19.7　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 19-6 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 マップが適用されるて、インタフェースが CNA と接続されると、絶対優先 PGID(PGID 15.0 to PGID 15.7)だけが許容されます。

表 19-6 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 19-7 は、デフォルト DCB Priority Table の設定を示します。

表 19-7 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

19.7.1 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
```

19.7.2 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. 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. PGID 0 の CEE マップを定義します。

```
switch(config-cee-map)#priority-group-table 0 weight 50 pfc on
```

4. PGID 1 の CEE マップを定義します。

```
switch(config-cee-map)#priority-group-table 1 weight 50
```

5. 特権実行モードに戻ります。

```
switch(config-cee-map)#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
```

19.7.3 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 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. マップを定義します。

```
switch(config-cee-map)#priority-table 1 1 1 0 1 1 1 15.0
```

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
```

19.7.4　　インタフェースへの CEE プロビジョニングマップの適用

CEE 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
```

2．10G ポートを指定します。この例では、0/2 を使っています。

```
switch(config)#interface tengigabitethernet 0/2
```

3．インタフェースに CEE マップを適用します。

```
switch(conf-if-te-0/2)#cee default
```

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
```

19.7.5　　CEE マップの確認

CEE マップを確認するため、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します。

```
switch#configure terminal
```

2．指定した名称でプロビジョニングされる CEE マップを確認します。

```
switch(config)#do show cee maps default
```

19.8　VCS ファブリック QoS

VCS ファブリック QoS には、非常にわずかなユーザ設定が必要です。修正しなければならないオプションは、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。

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 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。

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。

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。

19.8.1 Configuring VCS fabric QoS

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、特権実行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. 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 2
```

3. 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、'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(config-cee-map-default)#remap fabric 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のコンフィグレーションモードに移行します。

```
switch(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
```

20 8021x ポート認証の設定

20.1 802.1x 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。

20.2 802.1x 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。

20.3 802.1x 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 で利用かのうなコマンドの解説は、『Network OS Command Reference』を参照下さい。

20.3.1 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 1/121
```

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
```

20.4　802.1x のインタフェース指定の管理作業

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 は有効化され 190 ページの『20.3　802.1x 認証設定作業』にある設定を行ったら、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このセクションにある作業を行います。

20.4.1　　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
```

20.4.2 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
   ```

20.4.3 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
   ```

20.4.4 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
```

20.4.5 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．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 interface tengigabitethernet 1/12
```
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
```

20.4.6 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
```

20.4.7 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
```

20.4.8 802.1x 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
```

21 sFlow の設定

21.1 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、内蔵 DCB スイッチから統計情報を収集し、ネットワーク上のどこかの IP アドレスにある sFlow コレクタにデータ送信します。sFlow コレクタは、後で処理するためにネットワーク上の全てのエージェントから集めた sFlow データを格納します。
sFlow データは、sFlow バージョン、エージェント IP アドレス、シーケンス番号、サンプル数に関する情報を提供し、通常 10 のフローかカウンタのサンプルを持ちます。
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

21.1.1 フロー採取インタフェース

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。

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。

21.1.2 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。もし、レギュラースケジュール選ばれた場合、各カウンタの開始時間は、ネットワークパフォーマンスでのボトルネックを見積もってランダムに選択されます。

21.2 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、196 ページの『21.3 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、196 ページの『21.3.1 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、特権実行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。
```
switch(config)#sFlow collector 192.10.138.176
```
3．sFlow polling ingerval を設定します。
```
switch(config)#sFlow polling interval 135
```
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
```

21.3　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る。sFlow を有効化して特定インタフェースの必要なカスタマイズを行うために、このセクションの作業を行います。

NOTE
インタフェースの 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。

21.3.1　　特定インタフェースの sFlow の有効化とカスタマイズ

インタフェースの sFlow を有効化並びにカスタマイズするために、特権実行モードで次の手順を実行します。

1．インタフェースのタイプと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 1/16
```
2．sFlow polling ingerval を設定します。
```
switch(conf-if-te-1/16)#sFlow polling interval 135
```

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-1/16)#sflow enable
```

4．sFlow sample-rate を設定します。

```
switch(conf-if-te-1/16)#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 1/16
te 1/16
Configured sampling rate :8192
Actual sampling rate :8192
Counter polling interval :135
Samples rcvd from h/w :33
```

21.3.2 特定インタフェースの sFlow の無効化

NOTE

インタフェースの sFlow を無効化することは、インタフェースの通信を停止することではありません。

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 interface tengigabitethernet 1/12
```

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 1/12
```

22 スイッチドポートアナライザ(SPAN)設定

22.1 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 は元のポートにもトラフィックを送信します。

22.1.1 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。
- もしソースポートがバーストトラフィックを受信して、宛先のミラーポートで全てのバーストを処理できなかった場合は、バーストトラフィックの一部はミラーされません。
- LAG のミラーリングはサポートしていませんが、LAG のメンバーはミラー可能です。

22.2 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-mon-sess-1)#source tengigabitethernet 1/0/15
destination tengigabitethernet 1/0/1 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-mon-sess-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。

22.3　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-mon-sess-1)#source tengigabitethernet 1/0/15
destination tengigabitethernet 1/0/1 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-mon-sess-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。

22.4　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-mon-sess-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-mon-sess-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。

22.5　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-mon-sess-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
```

22.6　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
```

23 RMON の設定

23.1 RMON 概要

Remote monitoring(RMON)は、様々なネットワークエージェントとコンソールシステムにネットワーク監視データを交換することを可能とする Internet Engineering Task Force (IETF)規格の監視仕様です。RMON 仕様は、RMON 準拠のコンソールマネージャとネットワークプローブとの間で交換される統計情報と機能のセットを定義したものです。このように、RMON は包括的なネットワーク障害の診断、計画、パフォーマンスチューニングの情報を提供します。

23.2 RMON の構成と管理

アラームとイベントが構成可能な RMON パラメータです。

- イベント - アラームによりイベントが引き起こされたとき採るべきアクションを決定します。アクションは、ログや SNMP Trap やその両方を生成します。アラームが設定される前にイベントを定義する必要があります。もし、RMON イベントを先に設定しなくても、アラーム設定をするとエラーを受信します。
- アラーム - 指定された間隔で特定の MIB オブジェクトを監視し、閾値を持った特定の値でアラームを発行し、閾値を下回った時アラームを解除します。アラームはイベントと共に発生し、アラームがログや SNMP Trap といったイベントを引き起こします。

23.2.1 デフォルト RMON 設定

デフォルトでは、RMON アラームやイベントは設定されていません。RMON の統計情報収集も無効です。

23.2.2 RMON イベントの設定

RMON アラーム番号と関連づいた RMON イベントテーブルにイベントを定義または削除します。RMON イベントを設定するため、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。

```
switch#configure terminal
```

2．RMON イベントを設定します。

```
switch(config)#rmon event 27 description Rising_Threshold log owner
john_smith trap syslog
```

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
```

23.2.3 RMON イーサネットグループ統計情報収集の設定

インタフェースの ROMN イーサネットグループ統計情報を収集することが出来ます。RMON アラームとイベントは収集された統計情報を表示するために設定されなければなりません。デフォルトでは、RMON イーサネットグループ統計情報は無効です。

インタフェースの RMON イーサネットグループ統計情報を収集するため、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。

```
switch#configure terminal
```

2．インタフェースタイプとポート番号を指定するために、'interface'コマンドを入力します。

```
switch(config)#interface tengigabitethernet 0/1
```

3．インタフェースを有効化します。

```
switch(conf-if-te-0/1)#no shutdown
```

4．インタフェースの RMON イーサネットグループ統計情報を設定します。

```
switch(conf-if-te-0/1)#rmon collection stats 200 owner john_smith
```

5．特権実行モードに戻ります。

```
switch(conf-if-te-0/1)#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
```

23.2.4 RMON アラーム設定

RMON アラームとイベントを設定するため、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。

```
switch#configure terminal
```

2．RMON アラームを設定します。

アラーム発行閾値のために全てのサンプルをテストするアラームの例

```
switch(config)#rmon alarm 5 1.3.6.1.2.1.16.1.1.1.5.65535 interval 30
absolute
rising-threshold 95 event 27 owner john_smith
```

アラーム停止閾値のためサンプル間の差分をテストするアラームの例

```
switch(config)#rmon alarm 5 1.3.6.1.2.1.16.1.1.1.5.65535 interval 10
delta
falling-threshold 65 event 42 owner john_smith
```

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
```

24 IGMP の設定

24.1 IGMP 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 v2.0 は IGMPv1 と IGMPv2 をサポートしています。

24.1.1 Active IGMP snooping

IGMP snooping は普通は受動的で、フィルタリングなしで IGMP トラフィックを単純に監視します。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 から脱落すると、スイッチはルーターが VLAN ステータスを変更無しのままにするので、この情報を必要としないと決定します。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。

24.1.2 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。

- 求められていない 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のレイヤ２フォワーディングテーブルに 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。

24.2 IGMP 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。

24.3 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 レスポンスの切っ掛けとなる 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．last-member-query-interval 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
```

24.4　IGMP の監視

IGMP トラフィックの性能監視は、スイッチでのどんな潜在的な問題も分析することを可能としています。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、205 ページの『24.2 IGMP の構成』か 205 ページの『24.3　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。