BladeSymphony 10Gb DCB スイッチ

Network OS 管理者ガイド

４．１ 対応

HITACHI

■対象製品

このマニュアルは BladeSymphony 10Gb DCB スイッチモジュールを対象に記載しています。また、DCB スイッチモジュールのソフトウェア Network OS 4.1 までの利用頻度の高い機能について記載しています。各バージョンでサポートされる機能については、リリースノートならびに、旧 Networ OS 管理者ガイドを参照ください。

■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

２０１５年　３月　(第１版)

■著作権

目　次

1 NETWORK OS と VCS ファブリック テクノロジ イントロダクション.....22

1.1 NETWORK OS イントロダクション.....22
1.1.1 VCS ファブリック用語.....23
1.2 VCS ファブリック テクノロジ イントロダクション.....23
1.2.1 自動化.....24
1.2.2 分散インテリジェンス.....26
1.2.3 ロジカルシャーシ.....26
1.2.4 イーサネットファブリックの形成.....27
1.2.5 自動的隣接検出.....27
1.2.6 自動 ISL 形成とハードウェアベーストランキング.....28
1.2.7 PRINCIPAL RBRIDGE の選択.....28
1.3 VCS ファブリック テクノロジ の使用例.....28
1.3.1 従来のイーサネットアクセスとアグリゲーションの使用例.....28
1.3.2 大規模サーバ仮想化の使用例.....29
1.4 トポロジとスケーリング.....30
1.4.1 コア・エッジトポロジ.....31
1.4.2 リングトポロジ.....31
1.4.3 フルメッシュトポロジ.....32
1.5 レイヤ 2 イーサネットの概要.....33
1.5.1 レイヤ 2 転送.....34
1.5.2 VLAN タグ付け.....35
1.5.3 フレーム分類(着信).....36
1.5.4 輻輳制御とキューイング.....36
1.5.5 アクセス制御.....38
1.5.6 トランキング.....39
1.5.7 フロー制御.....39

2 NETWORK OS CLI の使い方.....41

2.1 コマンドラインインタフェース(CLI).....41
2.1.1 コンフィグレーションの変更の格納.....41
2.1.2 NETWORK OS CLI インタフェースの RBAC 権限.....41
2.1.3 デフォルトロール.....41
2.1.4 TELNET を使った NETWORK OS CLI へのアクセス方法.....42
2.1.5 NETWORK OS CLI コマンドモード.....42
2.1.6 NETWORK OS CLI キーボードショートカット.....45

2.1.7 ショートカットとしての'DO'コマンド使用方法 46
2.1.8 NETWORK OS CLI コマンド表示とコマンドシンタックス 46
2.1.9 NETWORK OS CLI コマンド補完機能 48
2.1.10 NETWORK OS CLI コマンド出力修飾子 48

3 スイッチ管理の基本 50

3.1 スイッチ管理の概要 50
3.1.1 スイッチへの接続 50
3.1.2 TELNET 及び SSH 概要 51
3.1.3 SSH サーバ鍵交換と認証 51
3.1.4 TELNET サポート機能 52
3.1.5 SSH サポート機能 52
3.1.6 TELNET または SSH での FIRMWARE アップグレードとダウングレード 52
3.1.7 TELNET と SSH の留意事項および制限事項 53
3.2 動作モード 53
3.2.1 ロジカルシャーシクラスタモード 54
3.2.2 ファブリッククラスタモード 56
3.2.3 スタンドアロンモード 56
3.3 スイッチへ接続する 56
3.3.1 ケーブルの接続 56
3.3.2 マネジメントモジュール経由でスイッチに接続する 58
3.3.3 スイッチへ直接接続する 58
3.3.4 TELNET サービス 59
3.3.5 SSH での接続 61
3.4 スイッチの管理と設定 63
3.4.1 ロジカルシャーシモードのスイッチ設定 63
3.4.2 ファブリッククラスタモードの設定 73
3.4.3 スタンドアロンモードの設定 73
3.4.4 管理インタフェースの表示 73
3.4.5 管理インタフェースの速度の設定 75
3.4.6 バナーの設定と表示 75
3.4.7 スイッチの情報設定 75
3.4.8 装置の有効化・無効化 76
3.4.9 装置のリブート 77
3.5 トラブルシューティング 77
3.5.1 サポートデータの採取 77
3.5.2 メッセージロギング 78

4 ネットワークタイムプロトコル 79

4.1 日付と時刻の設定 79
4.2 タイムゾーンの設定 79
4.2.1 タイムゾーン設定 80
4.2.2 現在の時刻とタイムゾーンの表示 80
4.2.3 タイムゾーン設定の削除 80
4.3 NETWORK TIME PROTOCOL 80
4.3.1 外部ソースへのローカル時間の同期 81
4.3.2 アクティブな NTP サーバの表示 81
4.3.3 NTP サーバ IP アドレスの削除 81

5 構成情報の管理 82

5.1 スイッチ構成情報の概要 82
5.2 フラッシュメモリ上のファイル管理 82
5.2.1 フラッシュメモリファイルの一覧表示 82
5.2.2 フラッシュメモリからファイルの削除 82
5.2.3 ファイル名の変更 83
5.2.4 フラッシュメモリ上のファイルの内容表示 83
5.3 コンフィグレーションファイルのタイプ 83
5.3.1 DEFAULT CONFIGURATION 84
5.3.2 STARTUP CONFIGURATION 84
5.3.3 RUNNING CONFIGURATION 85
5.4 コンフィグレーションの変更の格納 85
5.4.1 RUNNING CONFIGURATION の格納 86
5.4.2 RUNNING CONFIGURATION の一般ファイルへの格納 86
5.4.3 以前に格納したコンフィグレーション変更の適用 86
5.5 コンフィグレーションのバックアップ 86
5.5.1 STARTUP CONFIGURATION の外部ホストへのアップロード 87
5.6 コンフィグレーションの回復 87
5.6.1 以前の STARTUP CONFIGURATION の回復 87
5.6.2 DEFAULT CONFIGURATION の回復 88
5.7 VCS ファブリックモードでの構成情報管理 89
5.7.1 多数のスイッチへの構成情報のダウンロード 89
5.7.2 設定パラメータの自動配布 89

6 ファームウェアのインストールと管理 90

6.1 ファームウェア管理の概要 90
6.1.1 ファームウェアの入手と展開 90
6.1.2 ファームウェアのアップグレード 91
6.1.3 ファームウェアのアップグレードとダウングレード 91
6.2 ローカルスイッチでのファームウェアアップグレード 91
6.2.1 ファームウェアダウンロードの準備 91
6.2.2 ファームウェアバージョンの確認 92
6.2.3 FIRMWARE DOWNLOAD コマンドの使用方法 92
6.2.4 デフォルトモードでのファームウェアダウンロード 92
6.2.5 NOACTIVATE オプションを使用したファームウェアダウンロード 93
6.2.6 MANUAL オプションを使用したファームウェアダウンロード 93
6.2.7 MANUAL オプションを使用したファームウェアアップグレード 94
6.2.8 DEFAULT-CONFIG オプションを使用したファームウェアダウンロード 94
6.2.9 ファームウェアダウンロードセッションの確認 94
6.3 ファブリッククラスタモードでのファームウェアアップグレード 95
6.4 ロジカルシャーシクラスタモードでのファームウェアアップグレード 95
6.4.1 ロジカルシャーシクラスタモードでのファームウェアダウンロードの確認 98

7 ライセンスの管理 99

7.1 ライセンスの管理 100
7.1.1 スイッチライセンスＩＤの表示 100
7.1.2 ライセンスキーの取得 100
7.1.3 ライセンスのインストール 101
7.1.4 ライセンスの表示 101
7.1.5 ライセンスの削除 102

8 SNMP 管理 104

8.1 SNMP プロトコル概要 104
8.1.1 ＳＮＭＰマネージャ 104
8.1.2 ＳＮＭＰエージェント 104
8.1.3 ＭＩＢ(MANAGEMENT INFORMATION BASE) 104
8.1.4 ＳＮＭＰの基本動作 105
8.1.5 ＭＩＢ(MANAGEMENT INFORMATION BASE) 106
8.2 ＳＮＭＰの設定 109
8.3 SNMP コミュニティ設定 109
8.3.1 SNMP コミュニティの追加 110
8.3.2 READ-ONLY コミュニティのアクセス権の変更 110

8.3.3 SNMP コミュニティの削除 110
8.3.4 SNMP コミュニティの表示 110
8.4 SNMP サーバ 111
8.4.1 SNMP サーバホストの設定 111
8.4.2 SNMP サーバホストの削除 112
8.4.3 SNMP システムグループの設定 112
8.4.4 SNMP 設定情報の表示 113

9 ファブリック管理 114

9.1 TRILL 114
9.2 VCS ファブリックの形成 114
9.2.1 RBRIDGE の動作 115
9.2.2 隣接デバイスの検出 116
9.2.3 BROCADE トランク 116
9.2.4 ファブリックの形成 116
9.2.5 ファブリックルーティングプロトコル 117
9.3 VCS ファブリックの構成管理 118
9.3.1 VCS ファブリック設定作業 118
9.4 ファブリックインタフェースの構成管理 119
9.4.1 ファブリック ISL の有効化 120
9.4.2 ファブリック ISL の無効化 120
9.4.3 ファブリックトランクの有効化 120
9.4.4 ファブリックトランクの無効化 120
9.4.5 ブロードキャスト、未学習ユニキャスト、マルチキャスト転送 121
9.4.6 プライオリティ 121
9.4.7 RUNNING CONFIGURATION の表示 121
9.4.8 ファブリックの ECMP 負荷分散 124
9.5 VCS ファブリック上での操作 126

10 NETWORK OS システムモニタ 127

10.1 システムモニタの概要 127
10.1.1 スイッチヘルス監視 127
10.1.2 ハードウェアプラットフォームのデフォルト閾値の設定 127
10.1.3 システム設定の閾値 127
10.1.4 スイッチヘルスステータスの表示 128
10.1.5 システムモニタ構成の表示 128
10.2 リソース監視 128

10.2.1 メモリ監視の設定 129
10.2.2 CPU 監視の設定 130
10.2.3 閾値監視設定の表示 130
10.3 セキュリティ監視 130
10.4 インタフェース監視 130

11 ユーザーアカウントの管理 131

11.1 ユーザーアカウント 131
11.1.1 ローカルスイッチユーザーデータベースのデフォルトアカウント 131
11.1.2 ユーザーアカウントの作成と変更 131
11.1.3 ユーザーアカウントの作成 132
11.1.4 ユーザーアカウント情報の表示 132
11.1.5 既存ユーザーアカウントの変更 133
11.1.6 ユーザーアカウントの無効化 133
11.1.7 ユーザーアカウントの削除 134
11.1.8 ユーザーアカウントのロック解除 134
11.2 ロールベースアクセス制御 135
11.2.1 デフォルトロール 135
11.2.2 ユーザー定義ロール 135
11.2.3 ユーザー定義ロールの作成 136
11.2.4 ロールの作成または変更 136
11.2.5 ロールの表示 136
11.2.6 ロールの削除 136
11.3 コマンドアクセスルール 137
11.3.1 複数オプションで指定するコマンド 137
11.3.2 コンフィグレーションコマンドのルール 138
11.3.3 運用コマンドのためのルール 138
11.3.4 インタフェース関連コマンドのためのルール 138
11.3.5 プレースホルダルールの設定 140
11.3.6 ルールの処理 140
11.3.7 ルールの追加 140
11.3.8 ルールの変更 141
11.3.9 ルールの削除 141
11.3.10 ルールの表示 142
11.3.11 コンフィグレーション例 142
11.4 パスワードポリシー 143
11.4.1 パスワード強度ポリシー 143
11.4.2 パスワード暗号化ポリシー 144

11.4.3 アカウントロックアウトポリシー 144
11.4.4 サービス妨害の拒否 145
11.4.5 アカウントロックアウト閾値の設定 145
11.4.6 パスワードポリシーの管理 145
11.5 セキュリティイベントのロギング 147

12 エッジループ検出の管理 148

12.1 エッジループ検出の概要 148
12.2 ELD がループを検出する方法 150
12.3 エッジループ検出の設定 151
12.3.1 VCS ファブリッククラスタのためのグローバル ELD パラメータの設定 152
12.3.2 ポートでのインターフェースパラメータの設定 152
12.4 エッジループのトラブルシューティング 153

13 AMPP の設定 155

13.1 AMPP 概要 155
13.1.1 AMPP OVER VLAG 155
13.1.2 AMPP とスイッチドポートアナライザー 157
13.1.3 スケーラビリティ 157
13.2 AMPP ポートプロファイルの構成 157
13.2.1 ポートプロファイルの状態 158
13.2.2 新しいポートプロファイルの構成 160
13.2.3 VLAN プロファイルの設定 160
13.2.4 QoS プロファイルの設定 161
13.2.5 セキュリティプロファイルの設定 162
13.2.6 ポートプロファイルポートの削除 163
13.2.7 ポートプロファイルの削除 163
13.2.8 サブプロファイルの削除 164
13.3 AMPP プロファイルの確認 164

14 VLAN の設定 166

14.1 VLAN 概要 166
14.2 入力の VLAN フィルタリング 166
14.3 VLAN 設定のガイドラインと制限 168
14.4 VLAN のデフォルト設定 168
14.5 VLAN の構成と管理 169

14.5.1 インタフェースポートの有効化・無効化 169
14.5.2 インタフェースポートの MTU 設定 170
14.5.3 VLAN の作成 170
14.5.4 VLAN での STP の有効化 170
14.5.5 VLAN の STP の無効化 171
14.5.6 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 171
14.5.7 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 171
14.5.8 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 172
14.5.9 トランクインタフェースの VLAN の無効化 172
14.6 プロトコルベース VLAN の分類ルールの設定 173
14.6.1 VLAN CLASSIFIER ルールの生成 173
14.6.2 MAC ADDRESS-BASED VLAN CLASSIFIER ルールの構成 174
14.6.3 VLAN CLASSIFIER ルールの削除 174
14.6.4 VLAN CLASSIFIER グループと付加ルールの作成 174
14.6.5 インタフェースポートの VLAN CLASSIFIER グループの有効化 174
14.6.6 VLAN 情報の表示 175
14.7 MAC アドレステーブルの設定 175
14.7.1 MAC アドレスのエージングタイムの指定と無効化 175
14.7.2 MAC アドレステーブルへの静的アドレス登録 176
14.8 ネイティブＶＬＡＮ 176
14.8.1 ネイティブ VLAN の設定 176
14.8.2 ネイティブ VLAN の変更 177
14.8.3 ネイティブ VLAN の無効化 178

15 スパニングツリーの設定 179

15.1 STP 概要 179
15.2 設定時の注意事項および制約事項 180
15.3 RSTP 概要 181
15.4 MSTP 概要 182
15.5 PVST+と RAPID PVST+の概要 183
15.5.1 PVST+と RPVST+のガイドラインと制限 184
15.6 スパニングツリーの構成と管理 184
15.6.1 デフォルトのスパニングツリー設定 184
15.6.2 STP の設定 186
15.6.3 RSTP の設定 187
15.6.4 MSTP の構成 188
15.6.5 STP, RSTP, MSTP, PVST の有効化 189
15.6.6 STP, RSTP, MSTP, PVST の無効化 189

15.6.7 STP, RSTP, MSTP を全面的に停止する 189
15.6.8 ブリッジパラメータの指定 190
15.6.9 ＳＴＰタイマの設定 192
15.6.10 PORT-CHANNEL PATH COST の指定 193
15.6.11 TRANSMIT HOLD COUNT (RSTP、MSTP、RPVST+)の設定 193
15.6.12 CISCO 相互接続性(MSTP)の設定 194
15.6.13 CISCO 相互接続性(MSTP)の無効化 194
15.6.14 VLAN の MSTP インスタンスへのマッピング 194
15.6.15 BPDU(MSTP)最大 HOP 数の指定 195
15.6.16 MSTP リージョン名称の指定 195
15.6.17 MSTP 構成のレビジョン番号の指定 196
15.6.18 スパニングツリーカウンタのクリア 196
15.6.19 スパニングツリー検出プロトコルのクリア 196
15.6.20 STP 関連情報の表示 197
15.6.21 DCB インタフェースポート毎の STP, RSTP, MSTP の設定 197

16 リンクアグリゲーションの設定 204

16.1 リンクアグリゲーション概要 204
16.1.1 リンクアグリゲーショングループの設定 204
16.1.2 リンクアグリゲーションコントロールプロトコル(LACP) 205
16.1.3 動的リンクアグリゲーション 205
16.1.4 静的リンクアグリゲーション 205
16.1.5 BROCADE 独自のアグリゲーション 206
16.1.6 LAG の分配プロセス 206
16.2 VIRTUAL LAG 概要 206
16.2.1 VLAG の構成 207
16.2.2 VLAG 分割を無視する設定 208
16.2.3 リモート RBRIDGE 上のロードバランスの設定 209
16.3 LACP 設定のガイドラインと制限 210
16.4 デフォルト LACP 構成情報 210
16.5 LACP の構成と管理 211
16.5.1 ポートの LACP 有効化 211
16.5.2 LACP システムプライオリティの設定 211
16.5.3 DCB インタフェースの LACP タイムアウト時間の設定 211
16.5.4 LAG の LACP 統計情報のクリア 212
16.5.5 全 LAG グループの LACP 統計情報のクリア 212
16.5.6 LACP 情報の表示 212
16.6 LACP トラブルシューティング 212

17 NIC 冗長(TRACK)の設定 214

17.1 NIC 冗長(TRACK)の概要 214
17.2 NIC 冗長(TRACK)の構成 214
17.2.1 ポート監視の有効化と設定(物理ポート) 214
17.2.2 ポート監視の有効化と設定(LAG) 215
17.2.3 ポート監視の無効化 215

18 LLDP の設定 216

18.1 LLDP 概要 216
18.2 レイヤ 2 トポロジマッピング 216
18.3 DCBX 概要 218
18.3.1 ENHANCED TRANSMISSION SELECTION 219
18.3.2 PRIORITY FLOW CONTROL 219
18.4 LLDP の設定に関する注意事項および制約事項 219
18.5 LLDP の構成と管理 220
18.5.1 デフォルト LLDP 設定情報 220
18.5.2 装置全体の LLDP の有効化 220
18.5.3 装置全体の LLDP の無効化・リセット 221
18.5.4 LLDP グローバルコマンドオプションの設定 221
18.5.5 LLDP のインタフェースレベルコマンドオプションの設定 226
18.5.6 LLDP 関連情報の消去 226
18.5.7 LLDP 関連情報の表示 226

19 アクセスコントロールリスト(ACL)の設定 227

19.1 ACL 概要 227
19.1.1 ACL の利点 227
19.1.2 IP ACL 228
19.1.3 IP ACL パラメータ 229
19.1.4 デフォルト ACL 設定 231
19.2 ACL の構成と管理 231
19.2.1 ACL 設定のガイドラインと制限 231
19.2.2 標準 MAC ACL の作成とルールの追加 232
19.2.3 拡張 MAC ACL の作成とルールの追加 233
19.2.4 DCB インターフェースへの MAC ACL の適用 234
19.2.5 VLAN インタフェースへの MAC ACL 適用 234
19.2.6 MAC ACL ルールの変更 235

19.2.7 MAC ACL の削除 235
19.2.8 MAC ACL のシーケンス番号の並び替え 236
19.2.9 標準 IP ACL の作成 236
19.2.10 拡張 IP ACL の作成 236
19.2.11 管理インターフェースへの IP ACL の適用 237
19.2.12 スタンドアロンモードまたはファブリッククラスタモードへの ACL の関連付け 237
19.2.13 IP ACL 設定の表示 238

20 QOS の設定 239

20.1 QoS 概要 239
20.1.1 QoS の機能 239
20.1.2 ユーザープライオリティマッピング 240
20.1.3 輻輳制御 240
20.1.4 イーサネット PAUSE(ETHERNET PAUSE) 243
20.1.5 BUM ストーム制御 244
20.1.6 スケジューリング 245
20.1.7 DCB での QoS 248
20.1.8 VCS ファブリック QoS 250
20.2 QoS の設定 251
20.2.1 QoS 設定の基本 251
20.2.2 トラフィッククラスマッピング 259
20.2.3 輻輳制御機能の設定 263
20.2.4 マルチキャストレート制限の設定 265
20.2.5 BUM ストーム制御の設定 266
20.2.6 スケジューリングの設定 266
20.2.7 DCB QoS の設定 267
20.2.8 VCS ファブリックの QoS 設定 269

21 SFP BREAKOUT モードの設定 270

21.1 SFP BREAKOUT 概要 270
21.1.1 BREAKOUT MODE PROPERTIES 270
21.1.2 BREAKOUT モードのサポート 270
21.1.3 BREAKOUT モードインタフェース 270
21.1.4 BREAKOUT モードの制限 271
21.2 BREAKOUT モードの設定 272
21.3 追加の BREAKOUT モードシナリオの設定 272
21.3.1 40G QSFP ポートを BREAKOUT モードに設定する 273

21.3.2 BREAKOUT モード中に 40G QSFP ポートを予約する 273
21.3.3 BREAKOUT モード中に 40G QSFP ポートを開放する 274

22 スイッチドポートアナライザ(SPAN)設定 275

22.1 スイッチドポートアナライザプロトコルの概要 275
22.1.1 ロジカルシャーシモードにおける SPAN 275
22.1.2 RSPAN 275
22.1.3 標準 SPAN のガイドライン及び制限 276
22.1.4 ロジカルシャーシモードにおける SPAN のガイドライン及び制限 277
22.1.5 REMOTE SPAN (RSPAN)のガイドライン及び制限 277
22.1.6 RSPAN ミラーリングにおける制限 278
22.2 入力(INGRESS)SPAN の設定 279
22.3 出力(EGRESS)SPAN の設定 279
22.4 双方向(BIDIRECTIONAL)SPAN の設定 280
22.5 セッションから SPAN 接続の削除 280
22.6 SPAN セッションの削除 280
22.6.1 ロジカルシャーシモードにおける SPAN の設定 281
22.7 RSPAN の設定 282

23 スイッチのインバンド管理 284

23.1 インバンド管理の概要 284
23.1.1 前提条件 284
23.1.2 サポートインタフェース 285
23.1.3 インバンド管理方式のサポート状況 286
23.1.4 インバンド管理における接続トポロジ 287
23.2 インバンド管理インタフェースの設定 289
23.2.1 スタンドアロンモードでのインバンド管理インタフェースの設定 289

24 IGMP の設定 294

24.1 IGMP の概要 294
24.2 IGMP SNOOPING 概要 294
24.2.1 MULTICAST ルーティングと IGMP SNOOPING 294
24.2.2 VLAG および LAG プライマリポート 295
24.2.3 IGMP スケーラビリティ 296
24.3 IGMP SNOOPING の設定 297
24.3.1 IGMP SNOOPING の有効化 297

24.3.2 IGMP SNOOPING クエリヤーの設定 298
24.3.3 IGMP の監視 299

25 トラブルシュート 300

25.1 トラブルシュート概要 300
25.2 問題解決情報の収集 300
25.2.1 SUPPORTSAVE データの採取 300
25.2.2 トラブルシュートのアプローチ 301
25.3 トラブルシュートのホットスポットを理解する 302
25.3.1 ライセンス 302
25.3.2 他社スイッチとの STP 接続性 302
25.3.3 負荷分散配信 303
25.3.4 RBRIDGE ID の静的割当 304
25.3.5 FSPF 経路変更 304
25.3.6 VCS ファブリックとスタンドアロンモード 304
25.3.7 VLAG 304
25.3.8 VLAG とスプリット・ブレイン 305
25.3.9 PRINCIPAL RBRIDGE の可用性 307
25.3.10 BROCADE トランク 307
25.3.11 VLAG と NIC チーミング 307
25.3.12 MTU の選択 307
25.3.13 オーバーサブスクリプションの回避 307
25.3.14 ACL の制限事項 309
25.4 トラブルシューティング手順 309
25.4.1 AMPP が動作しない 310
25.4.2 不意の CPU 利用率高騰 313
25.4.3 期待通り ECMP が負荷分散しない 313
25.4.4 ENS の機能チェック 314
25.4.5 ISL が動作しない 315
25.4.6 ライセンスが正しくインストールされない 318
25.4.7 ハードウェアでのパケット破棄 318
25.4.8 PING 失敗 324
25.4.9 TAIL DROPS の原因となる QOS 設定 324
25.4.10 QOS は正しくパケットをマーキング・取り扱わない 324
25.4.11 RBRIDGE ID の重複 324
25.4.12 SNMP MIB の不正値報告 325
25.4.13 SNMP TRAP 通知の失敗 325
25.4.14 スイッチへの TELNET 失敗 325

25.4.15 TRUNK メンバ未使用 326
25.4.16 アップデート失敗 327
25.4.17 VCS ファブリックが形成されない 327
25.4.18 VLAG が形成されない 328
25.5 トラブルシューティングと診断ツール 330
25.5.1 LAYER 2 TRACEROUTE 330
25.5.2 SHOW コマンド 336
25.5.3 DEBUG コマンド 338
25.5.4 SPAN ポート及びトラフィックミラーリング 338
25.5.5 ハードウェア診断 339
25.5.6 'SHOW FABRIC ROUTE PATHINFO'コマンドによる経路情報の参照 339

26 サポートされているタイムゾーンと地域 340

26.1 アフリカ(AFRICA) 340
26.2 アメリカ(AMERICA) 342
26.3 南極大陸(ANTARCTICA) 344
26.4 北極(ARCTIC) 344
26.5 アジア(ASIA) 344
26.6 大西洋(ATLANTIC) 346
26.7 オーストラリア(AUSTRALIA) 346
26.8 ヨーロッパ(EUROPE) 346
26.9 インド(INDIAN) 348
26.10 太平洋(PACIFIC) 348

図一覧

図 1-1　従来のイーサネットと VCS アーキテクチャの比較 24
図 1-2　マルチパスを持ったイーサネットファブリック 25
図 1-3　イーサファブリック内の分散インテリジェンス 26
図 1-4　イーサファブリック内のロジカルシャーシ 27
図 1-5　サーバラック上部の Brocade VDX スイッチのペア 29
図 1-6　仮想マシンの移動を可能にしたフラットなレイヤ 3 ネットワーク 30
図 1-7　コア・エッジトポロジ 31
図 1-8　リングトポロジ 32
図 1-9　フルメッシュトポロジ 33
図 1-10　複数のスイッチファブリック構成 34
図 3-1　ロジカルシャーシクラスタ内のコンフィグレーションデータベース 55
図 3-2　BS500 システムの場合 57
図 3-3　BS2000 システムの場合 58
図 3-4　BS2500 システムの場合 58
図 3-5　５ノードで構成するロジカルシャーシクラスタ 63
図 3-6　ロジカルシャーシクラスタから N5 ノードを削除 70
図 8-1　ＳＮＭＰの構造 105
図 8-2　ＳＮＭＰ　Ｇｅｔ/Ｓｅｔ 105
図 8-3　ＳＮＭＰ　Ｔｒａｐ 105
図 8-4　ＭＩＢ　Ｔｒｅｅ 107
図 12-1　LAG を失ったことが原因のループ 149
図 12-2　相互接続した VCS ファブリッククラスタが原因となるループ 149
図 12-3　ELD が有効な相互接続の VCS ファブリッククラスタ 150
図 13-1　ポートプロファイルの内容 158
図 14-1　入力の VLAN フィルタ 167
図 16-1　ignore split の VLAG 設定 208
図 20-1　キューの深さ 241
図 20-2　２つのキューでの SP スケジューリング 245
図 20-3　２つのキューでの WRR スケジューリング 246
図 20-4　SP スケジューラと WRR スケジューラ 247
図 23-1　スタンドアロンモードにおけるインバンド管理接続トポロジ 288
図 23-2　VCS モードにおけるインバンド管理接続トポロジ 289
図 24-1　VCS ファブリックモードの IGMP スヌーピング 295
図 25-1　VCS ファブリックを通過する通常のレイヤ 2 パケット 331
図 25-2　隣接スイッチとのパス一貫性の検証 333
図 25-3　第２ホップへのパス一貫性の検証 335

表一覧

表 2-1　Network OS CLI コマンドモード....42
表 2-2　Network OS CLI キーボードショートカット....46
表 2-3　CEE CLI コマンド出力修飾子....49
表 3-1　スイッチへの接続方式別サポート仕様....50
表 3-2　動作モード別の利用可能管理ポート....56
表 3-3　マネジメントモジュールからスイッチへコンソールへの接続方法....58
表 3-4　管理ポートからスイッチへ直接接続方法....59
表 3-5　グローバル/ローカルコンフィグレーションコマンド....72
表 3-6　管理インタフェースの表示方法....74
表 5-1　標準のスイッチコンフィグレーションファイル....83
表 7-1　Network OS のオプション機能のライセンス一覧....99
表 7-2　ライセンスのインストール後にアクティブにするための要件....101
表 7-3　ライセンスの削除後に非アクティブにするための要件....102
表 8-1　ＭＩＢアクセスレベル....107
表 8-2　プライベートＭＩＢ依存関係....109
表 9-1　ロジカルシャーシクラスタモードを有効化するコマンド例....119
表 9-2　ファブリッククラスタモードを有効化するコマンド例....119
表 9-3　いずれかの VCS モードが既に有効になっている場合のコマンド例....119
表 9-4　構成のシナリオ....123
表 9-5　VCS ファブリック設定作業の例....125
表 9-6　VCS ファブリック上での操作....126
表 10-1　ハードウェアプラットフォームのデフォルト設定....127
表 10-2　CPU およびメモリの閾値の工場出荷時のデフォルト....129
表 11-1　ユーザーアカウントの属性....132
表 11-2　ロールの属性....136
表 11-3　ルールの属性....137
表 11-4　パスワードポリシーのパラメータ....143
表 13-1　AMPP スケーラビリティ値....157
表 13-2　AMPP の動作および障害の説明....159
表 14-1　VLAN デフォルト設定....169
表 14-2　ネイティブ VLAN 動作仕様....176
表 15-1　STP と RSTP の状態比較....181
表 15-2　STP デフォルト構成パラメータ....185
表 15-3　MSTP デフォルト構成パラメータ....185
表 15-4　10GbE DCB インタフェースデフォルト構成パラメータ....185
表 16-1　ロードバランス条件....209
表 16-2　デフォルト LACP 構成パラメータ....210
表 18-1　IPC,LAN,SAN トラフィックの ETS プライオリティグループ....219

表 18-2　デフォルト LLDP 構成情報 220
表 19-1　IP ACL パラメータ 230
表 20-1　Pause ネゴシエーション結果 244
表 20-2　サポートしているスケジューリング構成 247
表 20-3　マルチキャストトラフィッククラス同等のマッピング 248
表 20-4　デフォルト DCB Priority Group Table 設定 249
表 20-5　デフォルト DCB Priority Table 設定 250
表 20-6　untrust インタフェースのデフォルトユーザープライオリティ値 251
表 20-7　IEEE802.1Q のデフォルトプライオリティマッピング 252
表 20-8　デフォルト DSCP 優先度マッピング 255
表 20-9　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ープライオリティ 259
表 20-10　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ープライオリティ . 260
表 21-1　Breakout モードをサポートするスイッチ 270
表 21-2　SFP Breakout 設定値 271
表 21-3　breakout インタフェースの LED 272
表 23-1　インバンド管理用にサポートされるアプリケーション 284
表 23-2　インバンド管理が設定可能なポート 285
表 23-3　インバンド管理でのサポート状況 286
表 23-4　アウトバンド管理でのサポート状況 286
表 23-5　インバンド管理のためのトポロジ 287
表 24-1　スタンドアロンモードの動作条件 296
表 24-2　4 ノードクラスタの動作条件 297
表 24-3　20 ノードクラスタの動作条件 297
表 24-4　IP マルチキャスト動作条件 297
表 25-1　負荷分散アルゴリズム 303
表 25-2　ACL の制限 309
表 25-3　VCS ファブリックを通過するレイヤ 2 パケットのヘッダ詳細 332
表 25-4　レイヤ 2traceroute の第一ホップのパケットヘッダ詳細 334
表 25-5　レイヤ 2traceroute の第２ホップへのパケットヘッダ詳細 335
表 25-6　トラブルシュートに使われる show コマンド 337
表 26-1　アフリカの地域/都市タイムゾーン 340
表 26-2　アメリカの地域/都市タイムゾーン 342
表 26-3　南極大陸の地域/都市タイムゾーン 344
表 26-4　北極の地域/都市タイムゾーン 344
表 26-5　アジアの地域/都市タイムゾーン 344
表 26-6　大西洋の地域/都市タイムゾーン 346
表 26-7　オーストラリアの地域/都市タイムゾーン 346
表 26-8　ヨーロッパの地域/都市タイムゾーン 346
表 26-9　インドの地域/都市タイムゾーン 348

表 26-10　太平洋の地域/都市タイムゾーン..... 348

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

1.1 Network OS イントロダクション

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

- 簡単化されたネットワーク管理
  VCS ファブリックは、自己形成、自己修復機能を持ち、非常に大規模で動的なクラウドでのデプロイメントに必要なスケーラブルな運用基盤を提供します。マルチノードのファブリックは、単一の論理要素として管理することができ、ファブリックが配備されて、特定のワークロードのニーズに最適化されたさまざまな構成に簡単に再配備することができます。
  概要については 23 ページの『1.2 VCS ファブリック テクノロジ イントロダクション』を参照下さい。VCS ファブリック テクノロジの詳細は、114 ページの『9 ファブリック管理』を参照下さい。
- 高い回復力
  VCS ファブリックはハードウェアベースの ISL トランキングを使用し、トラフィックが中断することなく、自動リンクフェイルオーバーを提供します。
- ネットワーク利用率の改善
  Transparent Interconnection of Lots of Links (TRILL)に基づくレイヤ 2 ルーティングサービスは、ネットワークに等価コストマルチパスを提供し、その結果、ネットワークの利用率を改善します。VCS ファブリック テクノロジは、レイヤ 2 ドメインの成長に対する制約を取り除き、トロンボーンネットワークを排除し、ファブリック内での VLAN 間ルーティングを有効にする、複数のアクティブな、完全にロードバランスされたレイヤ 3 ゲートウェイを提供します。
  Virtual Router Redundancy Protocol (VRRP)は、参加しているホストへの仮想 IP ルーターを動的に割り当てることによって、静的なデフォルトルート環境での単一障害点を排除します。仮想ルーター内のすべてのルーターのインタフェースは、同じ IP サブネットに属している必要があります。異なる LAN 上の別のアドレス・マッピングを使用して仮想ルーターID(VRID)を再利用することに対する制限はありません。
  TRILL に関する追加情報は、114 ページの『9.1 TRILL』を参照下さい。
  VRRP/VRRP-E の概要については、114 ページの『9 ファブリック管理』参照下さい。
- サーバ仮想化
  Automatic Migration of Port Profile (AMPP)機能は、イーサネットポリシーに基づくファブリック全体のコンフィグレーションを提供し、ポート毎のプロファイルの転送を行い、仮想マシン(VM)の可搬性を支援するためのネットワークレベルの機能を有効にします。
  AMPP に関する更に詳細な情報は、155 ページの『13 AMPP の設定』を参照下さい。

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

1.1.1 VCS ファブリック用語

このドキュメントでは次の言葉が使われます。

エッジポート	イーサネットファブリック内でエンドステーションやスイッチやルーターを含む末端装置に接続される全てのスイッチポート
イーサネットファブリック	分散インテリジェンスを実現するため情報を交換するイーサネットスイッチが結合されたグループ
ファブリックポート	イーサネットファブリック内のインタースイッチリンク(ISL)の両端のポート
インタースイッチリンク(ISL)	VCS ファブリック内のスイッチ間を接続するインタフェース。イーサネットファブリック内のスイッチ間の接続インタフェースの両端のポートは、ISL ポートかファブリックポートと呼ばれます。ISL は、単一リンクもしくは Brocade トランクで構成する複数リンクとなる。このトランクには、Brocade 独自のトランク、または標準の IEEE 802.3ad ベースのリンクアグリゲーションとして作成することができます。
ルーティングブリッジ(RBridge)	VCS ファブリック内の物理スイッチ
RBridge ID	RBridge のユニークな識別子。コマンドでは、VCS ファブリック内の全てのインタフェースを参照する際に RBridge ID が使われる。RBridge ID の設定に関する詳細は、118 ページの『9.3 VCS ファブリックの構成管理』を参照下さい。
VCS ID	VCS ファブリックのユニークな識別子。デフォルトの VCS ID は 1 です。VCS ファブリック内の全てのスイッチは、同じ VCS ID が必要です。
WWN	工場でスイッチに設定されるグローバルにユニークな識別子。

1.2 VCS ファブリック テクノロジ イントロダクション

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

VCS ファブリック テクノロジは 3 つのコアな設計に基づいています。

- 自動化
- 弾力性
- 進化的デザイン

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

図 1-1 に、従来の階層的イーサネットアーキテクチャを使ったデータセンタと VCS アーキテクチャを使った同じデータセンタの例を示します。VCS ファブリック アーキテクチャはアクセス及びアグリゲーションレイヤを結合し、サーバラックを追加するといった拡張性があります。

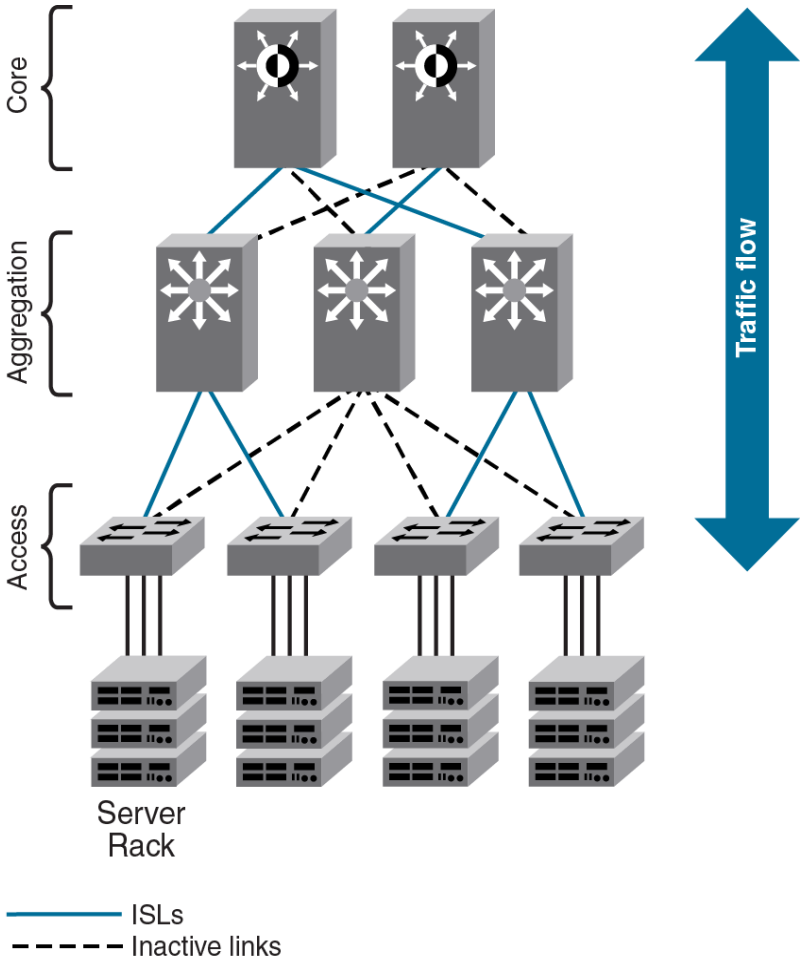

図 1-1　従来のイーサネットと VCS アーキテクチャの比較

1.2.1　　自動化

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

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

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

形成します。

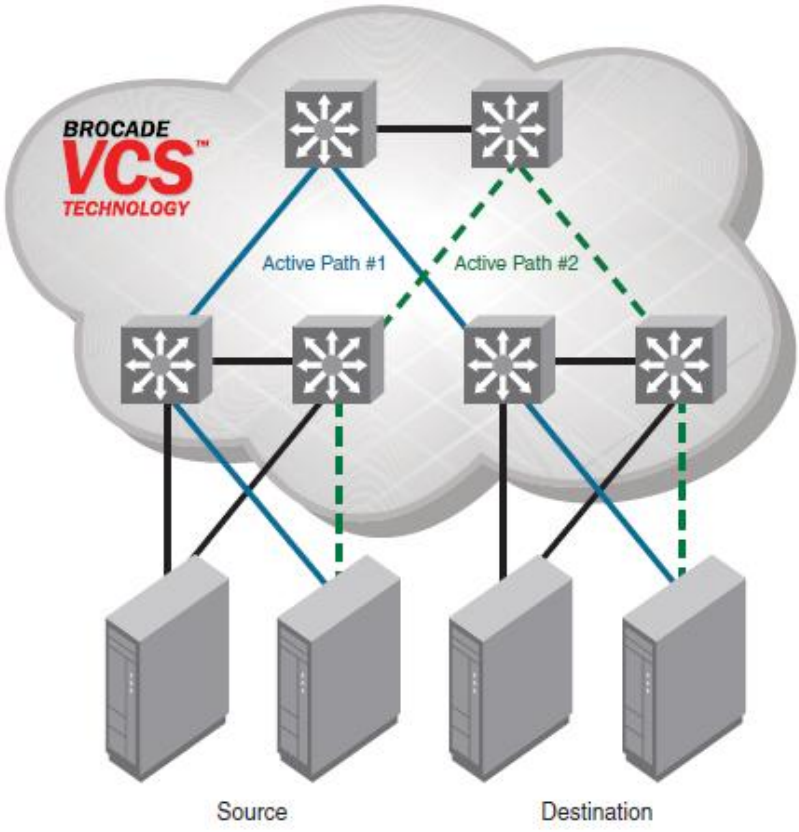

図 1-2　マルチパスを持ったイーサネットファブリック

イーサネットファブリックは次の特徴を持ちます。

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

1.2.2　分散インテリジェンス

VCS ファブリックテクノロジでは、すべての関連情報は、図 1-3 に示すように、結合されたファブリック機能を提供するために、スイッチの各メンバに自動的に配布されます。ブロケードの VCS ファブリックは、それぞれの新しいスイッチがファブリックの設定を継承し、新しいポートがすぐに利用できるように、一つの "論理的なシャーシ"として管理できるように設計されています。ファブリックは、一つのスイッチとしてもとのネットワークに戻ります。これは、大いに信頼性を向上させ、トラブル低減し、管理レイヤの複雑さを軽減します。

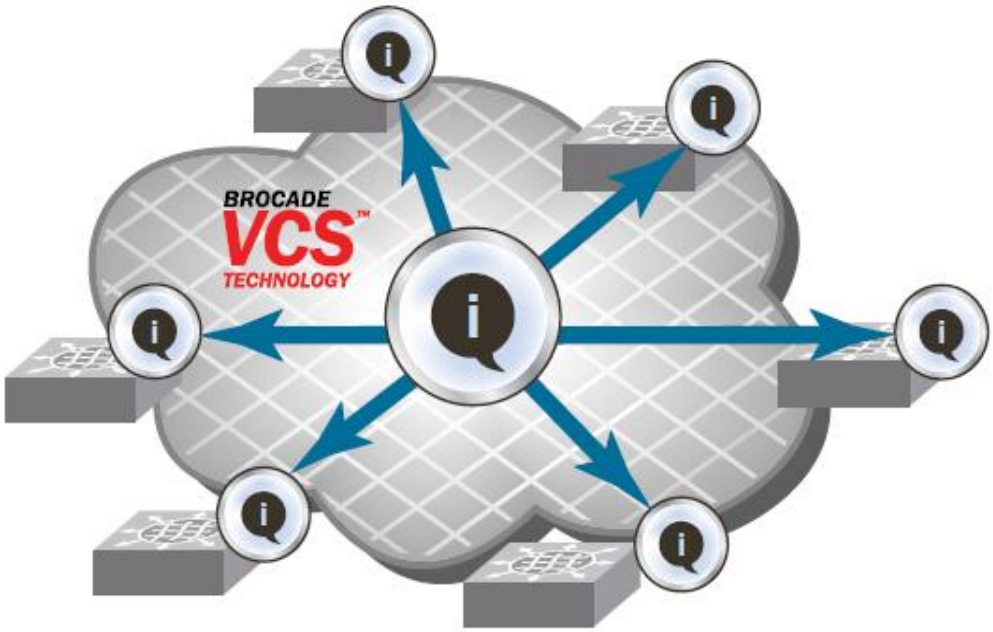

図 1-3　イーサファブリック内の分散インテリジェンス

分散インテリジェンスは次の特徴を持ちます。

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

1.2.3　ロジカルシャーシ

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

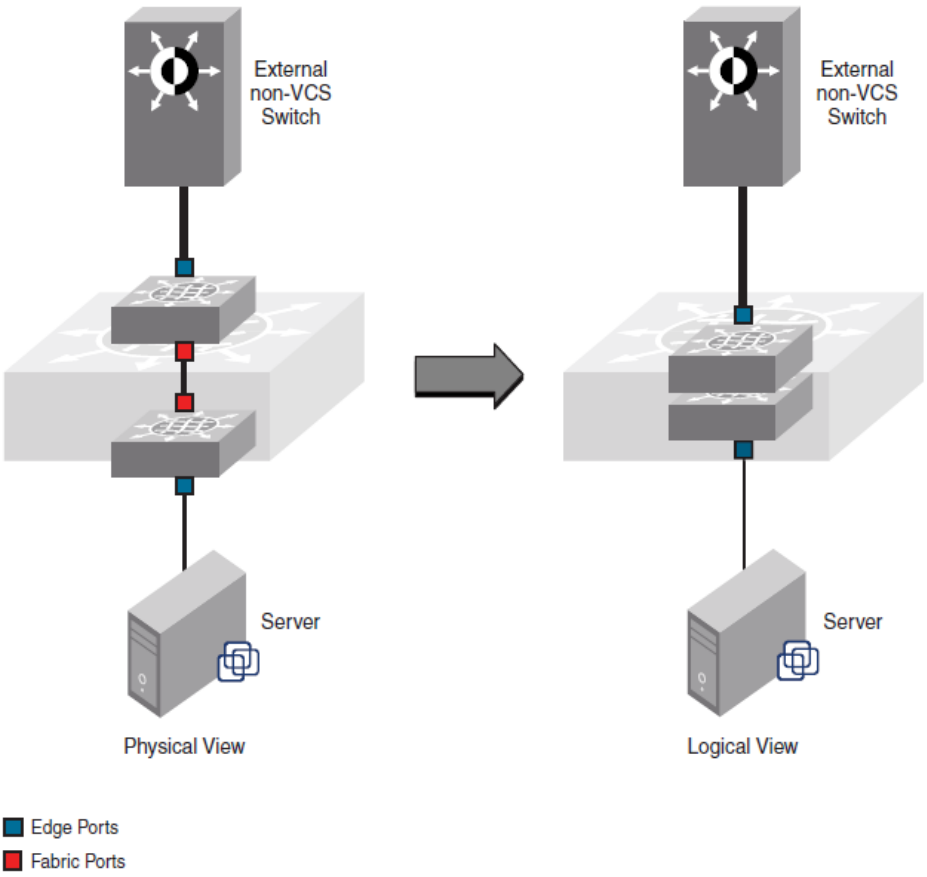

図 1-4　イーサファブリック内のロジカルシャーシ

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

1.2.4　　イーサネットファブリックの形成

VCS ファブリックプロトコルは、最小のユーザー設定でイーサネットファブリックの形成を支援するように設計されています。イーサネットファブリックの形成手順に関する詳細な情報は、114 ページの『9.2　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、118 ページの『9.3 VCS ファブリックの構成管理』を参照下さい。

内蔵 DCB スイッチは、VCS ファブリックモードを無効にした状態で出荷されています。VCS ファブリックモードを有効にする方法については、118 ページの 『9.3.1 VCS ファブリック設定作業』を参照してください。

1.2.5　　自動的隣接検出

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

VCS ID を変更する方法は、118 ページの『9.3 VCS ファブリックの構成管理』参照下さい。

1.2.6　自動 ISL 形成とハードウェアベーストランキング

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

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

ISL とトランクの有効・無効に関する情報は、119 ページの『9.4 ファブリックインタフェースの構成管理』を参照下さい。

1.2.7　Principal RBridge の選択

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

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

RBridge ID の設定に関する情報は、118 ページの『9.3 VCS ファブリックの構成管理』を参照下さい。

1.3 VCS ファブリック テクノロジ の使用例

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

- 従来のイーサネット
- 大規模なサーバ仮想化

1.3.1　従来のイーサネットアクセスとアグリゲーションの使用例

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

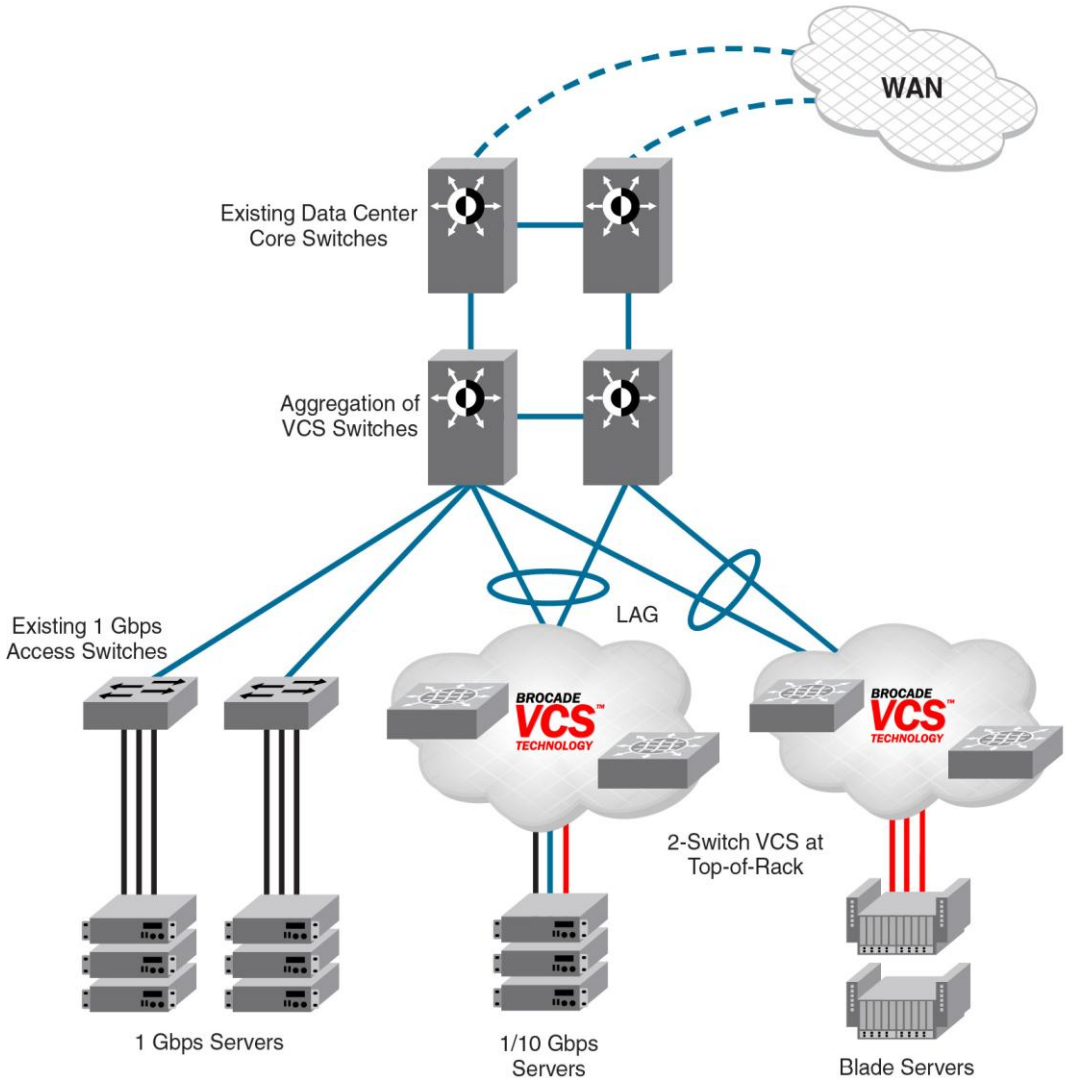

図 1-5　サーバラック上部の Brocade VDX スイッチのペア

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

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

1.3.2　　大規模サーバ仮想化の使用例

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

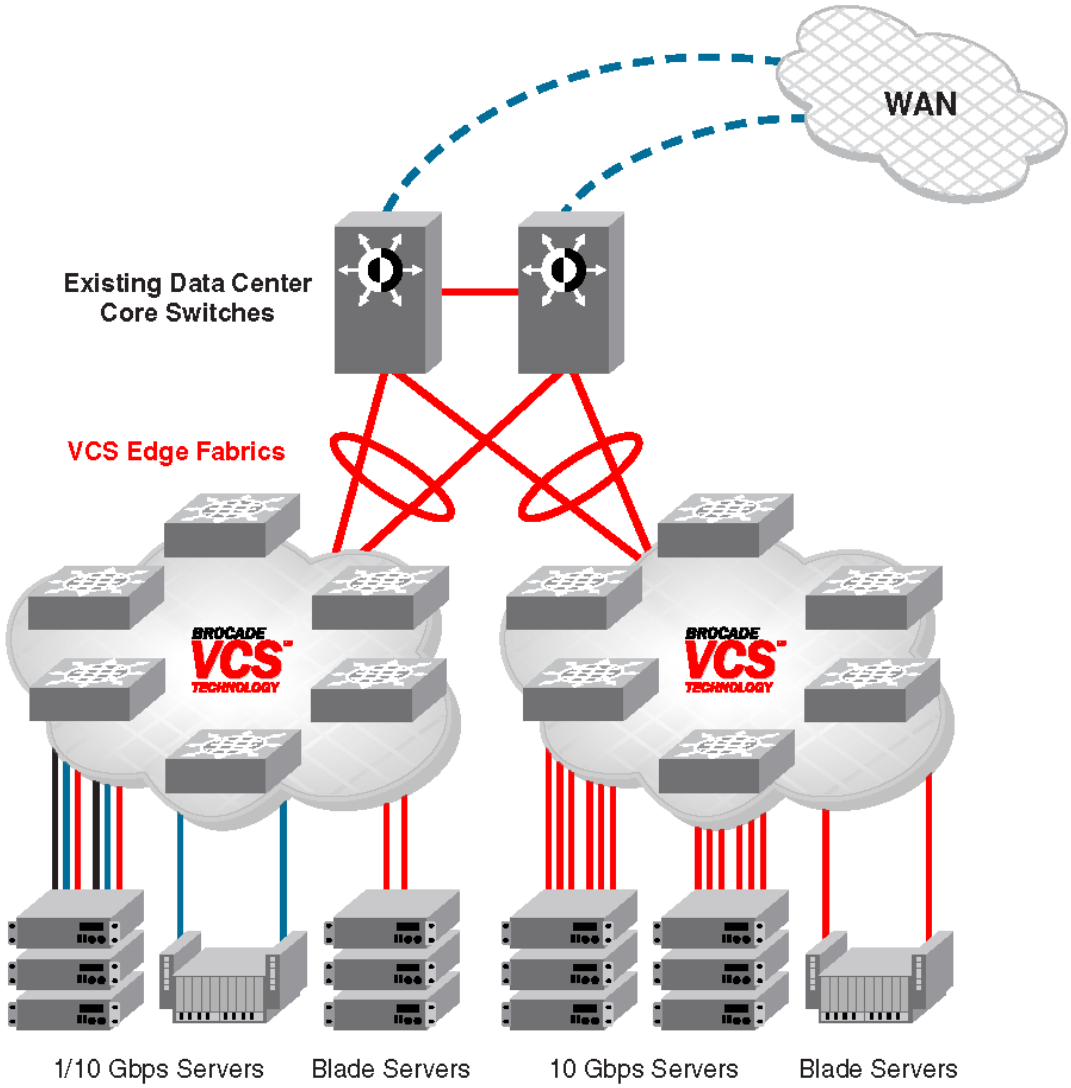

図 1-6　仮想マシンの移動を可能にしたフラットなレイヤ 3 ネットワーク

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

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

1.4　トポロジとスケーリング

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

- コア・エッジトポロジ
- リングトポロジ
- フルメッシュトポロジ

1.4.1　　コア・エッジトポロジ

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

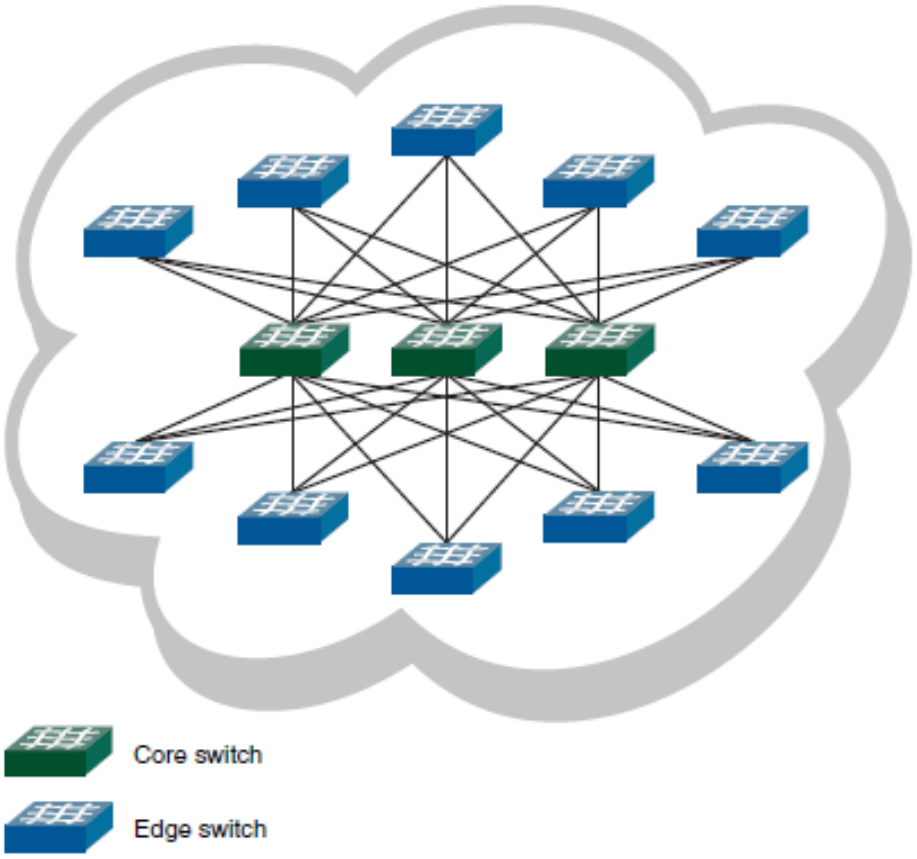

図 1-7　コア・エッジトポロジ

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

1.4.2　　リングトポロジ

リングトポロジでは、単一の連続した経路を形成し、正確に 2 つの他のノードに各ノードを接続しま

す。各ノードがすべてのパケットを扱って経路に沿ってノードからノードへ伝わります。図 1-8 にリングトポロジを示します。

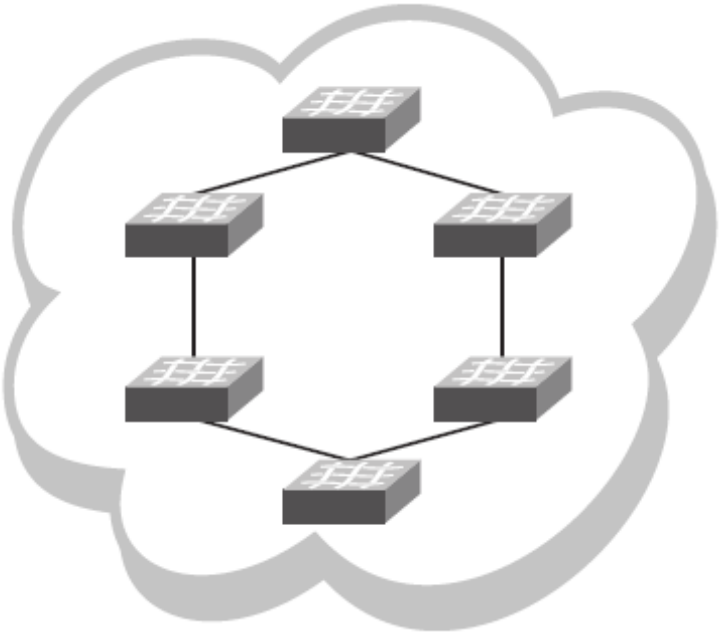

図 1-8　リングトポロジ

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

1.4.3　フルメッシュトポロジ

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

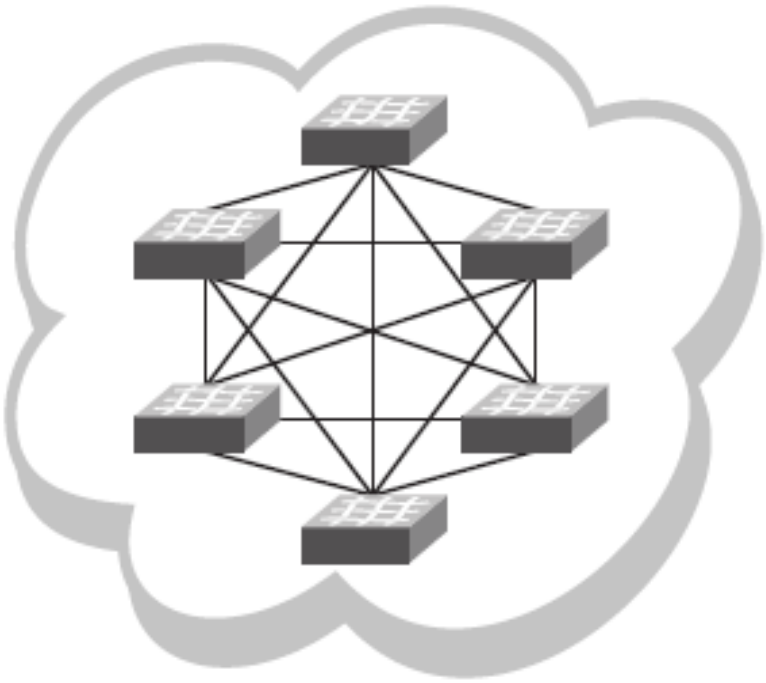

図 1-9　フルメッシュトポロジ

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

1.5 レイヤ２イーサネットの概要

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

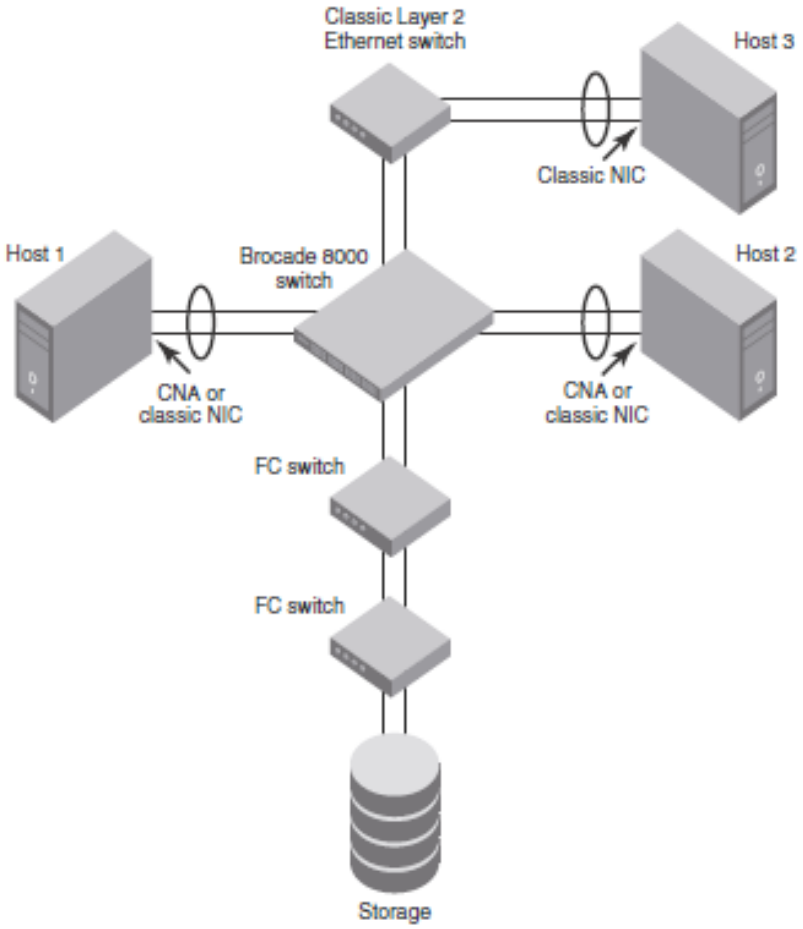

図 1-10　複数のスイッチファブリック構成

1.5.1　　レイヤ 2 転送

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

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

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

これらのプロトコルの設定の詳細については、179 ページの『15 スパニングツリーの設定』を参照してください。

内蔵 DCB スイッチは、次のようにイーサネットフレームを処理します。

- 宛先 MAC アドレスがルックアップテーブルに登録されていない場合、フレームは入力ポートを除い

て、同じ VLAN 内のすべてのポートにフラッディングされます。

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

NOTE

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

1.5.2 VLAN タグ付け

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

以下に、VLAN タグ付けの 3 つの例を示す。

- DCB ポートが着信フレームに単一の VLAN ID をタグ付けするように構成されている場合、タグが付いていない着信フレームは、VLAN ID でタグ付けされます。
- DCB ポートが着信フレームに複数の VLAN ID をタグ付けするように構成されている場合、タグが付いていない着信フレームは、ポートの設定に基づいて、適切な VLAN ID でタグ付けされます。
- DCB ポートが外部からタグ付きフレームを受け入れるように構成されている場合は、VLAN ID でタ

グ付けされている着信フレームは、変更されずに渡されます。
VLAN の設定の詳細については、166 ページの『14 VLAN の設定』を参照してください。

1.5.3 フレーム分類(着信)

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

- ポート番号
- プロトコル
- MAC アドレス

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

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

QoS を設定する詳細については、239 ページの『20 QoS の設定』を参照してください。

1.5.4 輻輳制御とキューイング

内蔵 DCB スイッチは、いくつかの輻輳制御とキューイング機能をサポートしています。出力キューが輻輳状態に近づくと、ランダム早期検出(RED)を選択的に使用され、最大リンク利用率を維持するために積極的にフレームをドロップします。着信フレームは、着信フレームのレイヤ 2 CoS が設定に基づいて、プライオリティキューに分類されるか、レイヤ 2 CoS フィールドが DCB ポートまたは VLAN のセッティングに基づいた書き換えによって分類されます。
内蔵 DCB スイッチは、出力ポートにキューのフレームに 2 つのスケジューリング機能(厳密な優先順位キューイング、不足加重ラウンドロビン(DWRR)キューイング)の組み合わせをサポートしています。

802.1Qaz Enhanced Transmission Selection(ETS)で指定されるようにスケジューリングアルゴリズムは、8 つのトラフィッククラスに取り組んでいます。
キューイング機能を、次に説明します。

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

クグラウンドトラフィックが混雑しています。混雑していないポートへの切り替えは、トラフィックストリームのトラフィックレートは高いままとなります。すべてのアウトバンドポートは、すべての着信ポートからのいくつかのマルチキャストフレームを運ぶ必要があります。これは、設定された閾値に対する相対的な値でマルチキャストトラフィックの配信を可能にします。

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

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

QoS を設定する詳細については、239 ページの『20 QoS の設定』を参照してください。

1.5.5 アクセス制御

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

ACL は、次のように機能します。

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

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

ACL の設定の詳細については、227 ページの『19 アクセスコントロールリスト(ACL)の設定』を参照してください。

1.5.6 トランキング

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

802.1ab Link Layer Discovery Protocol(LLDP)は、接続されたスイッチまたはホストへのリンクを検出するために使用されます。トランクは、隣接するスイッチまたはホストおよび内蔵 DCB スイッチの間で設定することができます。
Data Center Bridging Capability Exchange Protocol(DCBX)は、隣接するスイッチ、またはホスト上の DCB 対応ポートを識別するために使用されています。LLDP および DCBX の設定の詳細については、214 ページの『17 NIC 冗長(track)の設定』を参照してください。
802.3ad Link Aggregation Control Protocol(LACP)は、すべての個々のリンクの組み合わせた帯域幅を持つトランクを作成するために複数のリンクを結合するために使用されます。LACP の設定の詳細については、204 ページの『16 リンクアグリゲーションの設定』を参照してください。

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

1.5.7 フロー制御

802.3x イーサネットポーズとイーサネットの Priority-based Flow Control (PFC)は、リンクの送信元側

でトラフィックを遅くすることにより、フレーム破棄を防ぐために使用されます。多くは輻輳などが原因で、スイッチまたはホスト上のポートが送信元から多くのトラフィックを受信する準備ができていない場合、送信元へポーズフレームを送信し、トラフィックフローを一時停止します。輻輳が解消された時、送信元へトラフィックフローを一時停止する要求を止め、任意のフレームを落とすことなく、トラフィックを再開します。
イーサネットポーズが有効になっている場合、ポーズフレームは、トラフィックの送信元に送信されます。同様に、PFC が有効になっている場合、ポーズフレームが送信元スイッチに送信され、フレームのドロップはありません。
イーサネットポーズと PFC の設定の詳細については、239 ページの『20 QoS の設定』を参照してください。

2 Network OS CLI の使い方

2.1 コマンドラインインタフェース(CLI)

Network OS CLI は、イーサネット/IP ネットワーク管理でよく知られた業界標準の階層化コマンドラインインタフェースとなっています。
システムは、Network OS のデフォルトコンフィグレーションとスタートアップコンフィグレーションを使って立ち上がります。ログイン後は、Network OS シェルモードとなります。Network OS シェルモードでの CLI コマンドの使用方法は、42 ページの『2.1.5 Network OS CLI コマンドモード』を参照下さい。

2.1.1 コンフィグレーションの変更の格納

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

特権実行モードでの running-config ファイルの適用例

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

2.1.2 Network OS CLI インタフェースの RBAC 権限

ロールベースアクセス制御(RBAC)は、アカウントに割当られているロール(役割)に基づいて、ユーザーアカウントの権限を定義するものです。ロールは、スイッチのユーザーアカウントのアクセス権限が定義されたものです。ユーザーは、何れか一つのロールに関連付けられます。RBAC に関する詳細は、135 ページの『11.2 ロールベースアクセス制御』を参照下さい。

2.1.3 デフォルトロール

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

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

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

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

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

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

telnet セッションで、複数のユーザーが特権実行モードを使って操作することは可能です。
Network OS は 32 の telnet セッションまでをサポートしています。

2.1.5　Network OS CLI コマンドモード

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

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

表 2-1　Network OS CLI コマンドモード

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

表 2-1　Network OS CLI コマンドモード(続き)

コマンドモード	プロンプト	コマンドモードへの移行方法	説　明
Interface configuration	Port-channel: switch(config-Port-channel-63)# 10-Gigabit Ethernet (DCB port): switch(conf-if-te-0/1)# VLAN: switch(config-Vlan-1)#	特権実行モードから次のいずれかのコマンドを入力してインタフェースを指定します。 · interface port-channel · interface tengigabitethernet · interface vlan	インタフェース個別の表示設定を行います。
Protocol configuration	LLDP: switch(conf-lldp)# Spanning-tree: switch(config-mstp)# switch(config-rstp)# switch(config-stp)# switch(config-pvst)# switch(config-rpvst)#	特権実行モードから次のいずれかのコマンドを入力してプロトコルを指定します。 · protocol lldp · protocol spanning-tree mstp · protocol spanning-tree rstp · protocol spanning-tree stp · protocol spanning-tree pvst · protocol spanning-tree rapid-pvst	各プロトコルの表示設定
AMPP port-profile mode	AMPP port-profile: switch(config-port-profile-name)# VLAN-profile sub-mode: switch(config-vlan-profile)# QoS-profile sub-mode: switch(config-qos-profile)# Security-profile sub-mode: switch(config-security-profile)#	特権実行モードからポートプロファイルコンフィグレーションモード port-profile コマンドを入力して port-profile コンフィグレーションモードを開始します。 port-profile コンフィグレーションモードから、次のいずれかのコマンドを入力することにより、AMPP サブモードを指定します。	AMPP 機能のアクセスおよび設定をします。

		· vlan-profile · qos-profile · security-profile	
Feature configuration	CEE map: switch(config-cee-map-default)# Standard ACL: switch(conf-macl-std)# Extended ACL: switch(conf-macl-ext)#	特権実行モードから次のいずれかのコマンドを入力してDCB機能を指定します。 · cee-map default · mac access-list standard · mac access-list extended	CEEマップ機能のアクセスおよび設定をします。
DSCP mutation mapping	DSCP Mutation Map: switch(dscp-mutation-mapname)#	特権実行モードから次のコマンドを使用して着信したDSCP値を再配置します。 qos map dscp-mutation *mapname*	
DSCP to CoS priority mapping	DSCP to CoS Map: switch(dscp-cos-mapname)#	特権実行モードから次のコマンドを使用してCoSプライオリティマップにDSCPを作成します。 qos map dscp-cos *mapname*	
DSCP to traffic class mapping	DSCP to Traffic Class Map: switch(dscp-traffic-class-mapname)#	特権実行モードから次のコマンドを使用してDSCPにトラフィッククラスマップを作成します。 qos map dscp-traffic-class *mapname*	

表 2-1　Network OS CLI コマンドモード(続き)

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

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

2.1.6　Network OS CLI キーボードショートカット

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

表 2-2　Network OS CLI キーボードショートカット

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

NOTE

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

2.1.7　ショートカットとしての’do’コマンド使用方法

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

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

```
switch(conf-lldp)# do dir
total 24
drwxr-xr-x   2 root     sys          4096 Feb  2 22:22 .
drwxr-xr-x   3 root     root         4096 Jan 15  2013 ..
-rw-r--r--   1 root     sys           557 Sep 27 04:00 defaultconfig.novcs
-rw-r--r--   1 root     sys           800 Sep 27 04:00 defaultconfig.vcs
-rw-r--r--   1 root     root         7108 Feb  3 10:44 startup-config

2021769216 bytes total (921006080  bytes free)
```

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

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

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

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

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

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

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

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

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

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

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

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

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

装置がコマンドを認識できない場合は、エラーメッセージを表示します。

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

不完全なコマンドが入力された場合は、エラーメッセージを表示します。

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

2.1.9 Network OS CLI コマンド補完機能

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

```
switch#ter
```

CLI は次のコマンドを表示します。

```
switch#terminal
```

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

```
switch#show l
```

CLI は次のコマンドを表示します。

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

2.1.10 Network OS CLI コマンド出力修飾子

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

表 2-3　CEE CLI コマンド出力修飾子

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

3 スイッチ管理の基本

3.1 スイッチ管理の概要

スイッチへの接続に加えて、ネットワークの設定と管理を成功させるためには、スイッチの属性や動作モードを理解することが必須です。この章では、動作モードとコマンドモード・コマンドサブモード、他の関連するスイッチの動作について説明し、毎日の管理業務に参考となる情報を提供します。

3.1.1 スイッチへの接続

内蔵 DCB スイッチに接続するには、管理ポートへの telnet/SSH か、シリアルポートを使ったコンソールセッション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、装置にデフォルト設定として事前定義された管理者アカウントをご使用ください。

- シリアルポートの接続は、BS500/2000 ではマネジメントモジュール装備のシリアルポート経由で、BS2500 については、DCB スイッチ装備のシリアルポート経由で行います。BS500/2000 については、更にマネジメントモジュールのコマンドで、接続先を DCB スイッチに切替える必要があります。詳細は、BS500 は『CLI コンソール ユーザーズガイド』、BS2000 については『ユーザーズガイド』をご参照下さい。
- BS2500 では、シリアルポートに接続するために、別売の「Management cable for SW module」(GV-LR4MNC1N1)が必要です。

DCB スイッチに接続する方法には、シャーシ内部の DCB スイッチ管理ポートから接続する方法(アウトバンド接続)と、DCB スイッチのフロントに装備された通信ポートから接続する方法(インバンド接続)の２種類があります。次表に、それぞれの接続方式のサポート仕様を示します。

表 3-1 スイッチへの接続方式別サポート仕様

接続方式	設定箇所	静的アドレス設定		動的アドレス設定 (DHCP,AutoConf)	
		IPv4	IPv6	IPv4	IPv6
アウトバンド方式	マネジメント モジュール	○	○	×	×
インバンド方式	DCB スイッチ (Network OS)	○	×	×	×

アウトバンド方式については、56 ページの『3.3 スイッチへ接続する』を参照してください。

インバンド方式については、284 ページの『23 スイッチのインバンド管理』を参照してください。

NOTE
アウトバンド方式の場合、DCB スイッチの CLI(Network OS)では設定しないでください。マネジメントモジュールとの設定情報不整合が発生し、接続できなくなる場合があります。

3.1.2 Telnet 及び SSH 概要

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

SSH および telnet のサポートは、特権実行モードで有効であり、IPv4 アドレスと IPv6 アドレスをサポートしています。
Telnet と SSH サービスは、工場出荷時に両方有効となっています。Telnet サーバまたは SSH サーバが無効化されると、インバンド Telnet または SSH 接続を許可しません。すなわち、スイッチへのリモートアクセスを制限します。
ロジカルシャーシモード(54 ページの『3.2.1 ロジカルシャーシクラスタモード』参照)では、Telnet や SSH サービスを有効化/無効化するコマンドは、クラスタ全体には適用されません。指定された RBridge ID のノード個別に設定されます。
Telent または SSH が有効かどうかは、'show'コマンドで確認することが出来ます。

3.1.3 SSH サーバ鍵交換と認証

Secure Sockets Handling(SSH)プロトコルは、パスワードの代わりに、公開鍵/非公開鍵を使って認証するものです。パスワードベースの認証では、認証のためにパスワードを入力しなければなりません。公開鍵認証では、ローカルマシンにある非公開鍵とリモートマシンにある公開鍵を使います。ユーザーは、認証のためにローカルマシンにログインするのみです。もし、公開鍵と非公開鍵で生成されパスフレーズが提供されると、認証される間、非公開鍵を暗号化するためにパスフレーズが入力されます。
SSH の鍵交換は、暗号化のために一度限りの鍵を生成する方法を指定したり、SSH サーバとの認証方法を指定します。ユーザーは、DH Group 14 に SSH サーバとの鍵交換の方法を設定することが出来ます。SSH サーバ鍵交換方法が DH Group 14 に設定されると、リモート SSH クライアントからの SSH 接続は、クライアントの鍵交換方法が DH Group 14 に設定されているときのみ、可能となります。
次の手順は、公開鍵認証を簡単に説明しています。

1．次に示すような公開鍵/非公開鍵と共に'ssh-keygen'コマンドを使って、ローカルマシン上で暗号鍵の対を生成します。

```
switch# ssh-keygen -t rsa
generates RSA public and private keypair
switch# ssh-keygen -t dsa
generates DSA public and private keypair
```

2．非公開鍵をローカルマシンに保存し、公開鍵をスイッチに取り込みます。
3．リモートホストにログインしようとすると、リモートホストから公開鍵を含んだ暗号化されたメッセージを受信します。メッセージが非公開鍵により復号された後、ユーザー認証され、アクセス権を得る。
'ssh-keygen'コマンドは、クラスタ中に配信されません。個々のノードのサービスを設定するために RBridge ID が使用されます。

3.1.4 Telnet サポート機能

次の機能は、Telnet でサポートしていません。

- Telnet セッションの表示
- ハングアップした Telnet セッションの中断

3.1.5 SSH サポート機能

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

次の暗号アルゴリズムをサポートしています。

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

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

- **hmac-md5**：128 ビットキーによる MD5 暗号化アルゴリズム(デフォルト)
- **hmac-md5-96**：96 ビットキーによる MD5 暗号化アルゴリズム
- **hmac-sha1**：160 ビットキーによる SHA1 暗号アルゴリズム
- **hmac-sha1-96**：96 ビットキーによる SHA1 暗号アルゴリズム

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

- SSH セッション表示
- 古い SSH キーの削除

3.1.6 Telnet または SSH での Firmware アップグレードとダウングレード

Telnet サーバか SSH サーバが無効になっている時、NOS 4.0 より前のバージョンへのダウングレードはできません。ダウングレードするためには、Telnet サーバか SSH サーバを有効にしてください。
アップグレードは、デフォルトで Telnet か SSH が有効になっているため可能です。

更に詳細な情報は、90 ページの『6 ファームウェアのインストールと管理』を参照してください。

3.1.7 Telnet と SSH の留意事項および制限事項

- Telent サーバまたは SSH サーバが無効化されていると、IPv4 と IPv6 の両方からのインバンドアクセスは出来ません。
- スイッチから Telnet または SSH で他のデバイスへの接続は、Telnet または SSH サーバの有効/無効設定の影響を受けます。
- Telnet または SSH サーバが無効化または有効化されている時、RASlog 及び auditlog メッセージは出力されません。

3.2 動作モード

Network OS は、次の３つのモードをサポートしています。スイッチが起動した時、これらのモードのいずれかになります。工場出荷時は、BS500/BS2000 ではスタンドアロンモード、BS2500 ではファブリッククラスタモードで起動します。

- ロジカルシャーシクラスタモード － ２つの VCS モードの一つです。このモードは、Network OS 4.0.0 以降が必要です。このモードでは、データとコンフィグレーションの両方のパスが分散されます。クラスタ全体が、principal ノードから設定できます。更に詳細な情報は、54 ページの『3.2.1 ロジカルシャーシクラスタモード』を参照してください。
- ファブリッククラスタモード － ２つの VCS モードのもう一つのタイプです。このモードでは、データパスは分散されますが、データパスは分散されません。各ノードは、個々のコンフィグレーションを維持します。更に詳細な情報は、56 ページの『3.2.2 ファブリッククラスタモード』を参照ください。
- スタンドアロンモード － BS500/2000 搭載の DCB スイッチモジュールのみサポートします。詳細は、56 ページの『3.2.3 スタンドアロンモード』を参照ください。

スイッチが起動すると、スイッチのモデルによってスタンドアロンモードか、ファブリッククラスタモードのいずれかで起動します。

NOTE

特に注意書きが無い場合、本マニュアルでの"VCS モード"という表現は、ファブリッククラスタモードとロジカルシャーシクラスタモードの両方を指します

NOTE

BS2500 向け内蔵 DCB スイッチは、スタンドアロンモードおよびロジカルシャーシクラスタモードは未サポートです。

3.2.1　ロジカルシャーシクラスタモード

(1) ロジカルシャーシクラスタモードの特徴

ロジカルシャーシクラスタモードの主な特徴を次に示します。

- ロジカルシャーシクラスタモードを構成できる最大ノード数は、BS500/2000 で 24 です。
- ロジカルシャーシクラスタに必要とする物理接続要件は、ファブリッククラスタモードと同じです。
- ノード個別のローカルコンフィグを含むことができ、全ノードにまたがる単一のグローバルなコンフィグレーションが存在します。各ノードはクラスタ内の他のノードのローカルコンフィグレーションを含みます。
- ロジカルシャーシクラスタ全体のグローバル/ローカルコンフィグレーションは、一つのノードから分配されます。これを principal ノードと呼びます。
- Startup コンフィグレーションは、クラスタには存在しません。各ノードが running コンフィグを保存します。
- ロジカルシャーシクラスタは、次節以降の手順に従ってコンフィグレーションを保存すれば、ファブリッククラスタに遷移できます。
- 存在しているファブリッククラスタは、次節以降の手順に従ってコンフィグレーションを保存すれば、ロジカルシャーシクラスタに遷移できます。
- ロジカルシャーシクラスタのメンバであるノードは、スタンドアロンモードに遷移できます。但し、BS500/2000 搭載の DCB スイッチモジュールのみです。
- クラスタ全体でのファームウェアのアップデートが可能です。
- クラスタ全体での supportsave を取得可能です。

(2) ロジカルシャーシクラスタモードでのコマンド制限

ロジカルシャーシクラスタモードでは、幾つかのコマンドが他のコマンドや処理実行中に実行出来ません。

もし次の CLI コマンドタイプがクラスタで実行中であれば、以下に列挙された CLI コマンドタイプや処理は、実行中のコマンドが完了するまでリジェクトされます。

- copy file running-config
- VCS ID/RBridgeID 変更コマンド
- ロジカルシャーシクラスタからファブリッククラスタへのクラスタモード変更
- copy default-config startup-config
- 個別コマンドでのコンフィグレーションの更新
- 最初のクラスタ化、セカンダリのクラスタへの追加といったクラスタ構成中

これらのコマンドや処理は、同時実行されないように考慮されています。しかし、principal ノードが変更になると、新しい principal ノードは、抑止状態となるべきコマンドや処理の経過を維持できません。

抑止されるコマンドの場合、次に示すエラーメッセージが実行結果として出力されます。

- Cluster formation is in progress. Please try again later.
- User Configuration update is in progress. Please try again later.
- Configuration file replay is in progress. Please try again later.
- HA failover is in progress in the cluster. Please try again later.
- VCS Config change is in progress in the cluster. Please try again later.
- Copy default-config startup-config is in progress. Please try again later.

(3) ロジカルシャーシクラスタモードの設定

ロジカルシャーシクラスタモードでは、コンフィグレーションデータベースに記録されるいずれの操作も自動的に分配されます。例外はありません。ロジカルシャーシクラスタの各ノードは、クラスタの高可用性を実現するためコンフィグレーションの個々のコピーをメンテナンスします。次にロジカルシャーシクラスタのノードを図示します。各ノードは、自身のデータベースを持ち、各ノードに保持されるデータベースは常に一致しています。

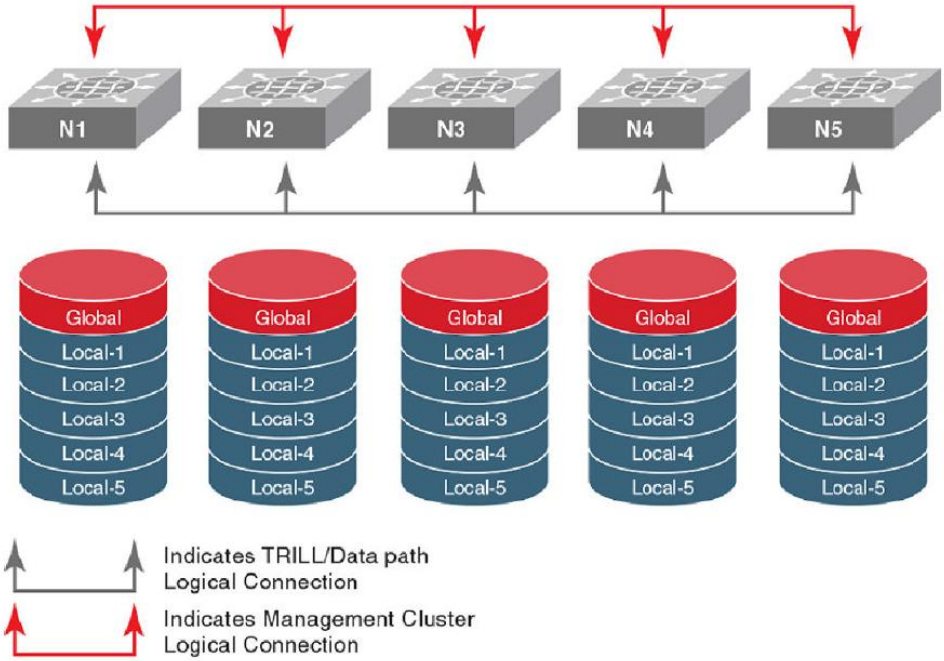

図 3-1　ロジカルシャーシクラスタ内のコンフィグレーションデータベース

Network OS スイッチは、グローバルとローカルコンフィグレーションの両方を保持しています。ロジカルシャーシクラスタでは、個々のメンバ自身のローカルなコンフィグレーションを持ちつつ、単一のグローバルなコンフィグレーションが、クラスタの全メンバにまたがり存在します。(逆に、ファブリッククラスタモードでは、クラスタの各メンバが自身で単一のグローバルコンフィグレーションを持っています。)

グローバルコンフィグレーションは、クラスタ全体の動作に必要とされますし、ローカルコンフィグレーションは、個別のノードの動作に必要となります。各コンフィグレーションの詳細な情報と例は、72 ページの『3.4.1 (14)グローバルコンフィグレーションとローカルコンフィグレーションの例』を参照してください。

3.2.2　ファブリッククラスタモード

NOS Ver. 3.x 以前での"VCS モード"モードです。ファブリッククラスタモードは、データパスは分散されますが、コンフィグレーションパスは分散されないファブリックとして定義されます。各ノードは、個別にコンフィグレーションデータベースを保持します。

3.2.3　スタンドアロンモード

従来からのレイヤ 2 スイッチと同等に動作するモードです。BS500/2000 搭載の DCB スイッチでは、デフォルトは、スタンドアロンモードで起動します。
この制限されたモードでは、スイッチは、IP スタティック・ルートとインバンド管理を除いて Network OS V2.0.0 で利用できたレガシー機能だけをサポートします。他のすべてのレイヤ 3 機能、および Network OS v3.0.0 以降で導入された他の機能は、スタンドアロンモードでは使用できません。

3.3 スイッチへ接続する

ここでは、シャーシ内部の DCB スイッチ管理専用ポートから接続する方式(アウトバンド接続)について説明します。

3.3.1　ケーブルの接続

DCB スイッチの管理専用ポートは、シャーシ内部で BladeSymphony の管理ポートと接続されており、マネジメントモジュールを中継する方法と、DCB スイッチモジュールに直接アクセスする方法の２種類のアクセス方法があります。(BladeSymphony の管理ポートは、装置モデルにより、マネジメントモジュールに装備されているか、専用のＬＡＮモジュールとして装備されています。)

NOTE

BS2500 搭載の DCB スイッチには、フロントパネルの管理用 RJ-45 ポートが装備されています。このポートは、DCB スイッチの動作モードにより利用可否が異なります。詳細については、次表を参照ください。

表 3-2　動作モード別の利用可能管理ポート

DCB スイッチ 動作モード	スタンドアロンモード※１	ファブリッククラスタモード	ロジカルシャーシクラスタモード
シャーシ内部管理ポート	○	○	※２
パネル搭載管理ポート (BS2500 DCB スイッチのみ)	－	×	－

※１：BS500/2000 搭載 DCB スイッチのみサポート

※２：BS500/2000 搭載 DCB スイッチは利用可(○) / BS2500 搭載 DCB スイッチは未サポート

NOTE

ロジカルシャーシクラスタモードは、ファブリック全体を Principal ノードにより操作・設定してください。スイッチの管理ポート使って個々に操作・設定するのは例外的な操作となります。この章では、スタンドアロンモード及びファブリッククラスタモード時の接続方法を示しています。

DCB スイッチの管理ポートに接続するために、BladeSymphony の管理ポートにケーブルを接続します。各モデル毎の接続イメージを次図に示します。BladeSymphony の管理ポートの位置はモデル毎に異なりますが、次図を参考に RJ-45 ポートに接続してください。

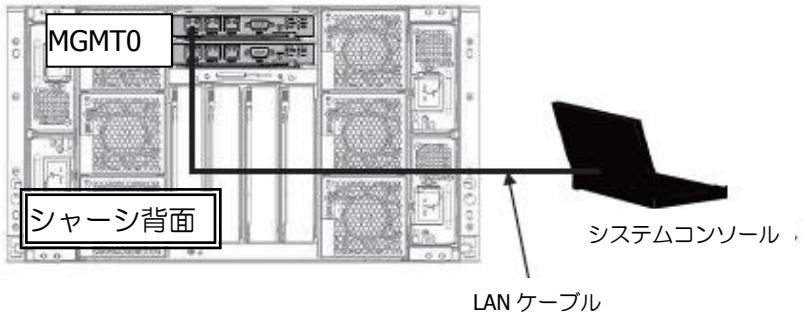

図 3-2　BS500 システムの場合

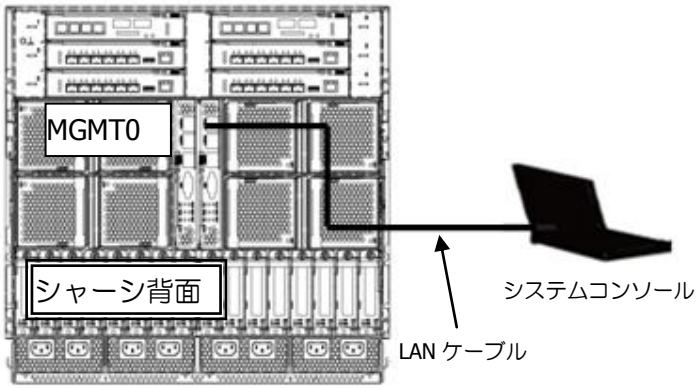

図 3-3　BS2000 システムの場合

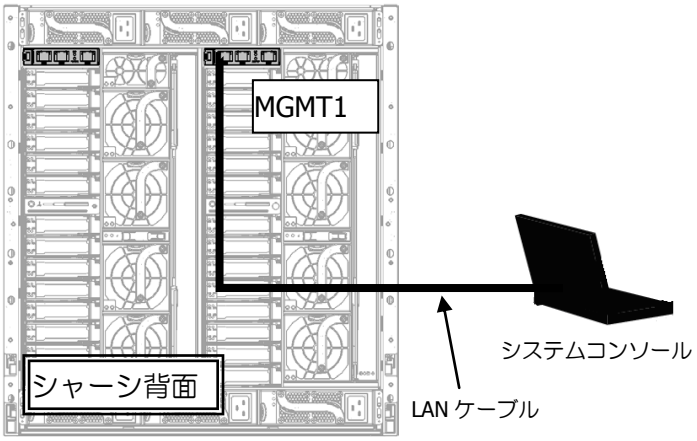

図 3-4　BS2500 システムの場合

3.3.2　　マネジメントモジュール経由でスイッチに接続する

BladeSymphony の管理ポートは、デフォルトではマネジメントモジュールとのみ接続されており、マネジメントモジュールにのみアクセス可能です。
しかし、マネジメントモジュールには、DCB スイッチのコンソールへ接続する機能を装備しているため、下記の操作により DCB スイッチに接続することができます。これにより、DCB スイッチの CLI を使った操作は可能となります。

表 3-3　マネジメントモジュールからスイッチへコンソールへの接続方法

装置モデル	接続先切替え方法
ＢＳ５００	マネジメントモジュールに Telnet または SSH で接続し、 CLI コマンドの'change console'を実行。 DCB スイッチの CLI に切り替わります。
ＢＳ２０００	マネジメントモジュールに Telnet または SSH で接続し、 メインメニューから「SW. Start switch module console session.」メニューを選択。 DCB スイッチのログイン画面に切り替わります。
ＢＳ２５００	マネジメントモジュールに Telnet または SSH で接続し、 CLI コマンドの'change console'を実行。 DCB スイッチのログイン画面に切り替わります。

3.3.3　　スイッチへ直接接続する

SNMP や NTP といったスイッチの管理機能を使うためには、スイッチに直接接続する必要があります。

次表に、シャーシの管理ポートから直接 DCB スイッチへ接続する方法を示します。

表 3-4　管理ポートからスイッチへ直接接続方法

装置モデル	接続先切替え方法
ＢＳ５００	マネジメントモジュールの Web コンソールから、［Resources］タブー［Systems］のツリービューから［ネットワーク管理］－［管理 LAN］を選択し、DCB スイッチの管理ポートのＩＰアドレスを入力し、「接続種別」を「直接接続する」に設定します。
ＢＳ２０００	マネジメントモジュールに Telnet または SSH で接続し、メインメニューから「S. System command mode.」メニューを選択し、マネジメントモジュールのシステムコンソールにアクセスします。 「LC」コマンドを使って、スイッチモジュールのＩＰアドレス等を設定する際、「Ext setting」に対して「1」(Ext)を設定します。
ＢＳ２５００	マネジメントモジュールの Web コンソールから、［Resources］タブー［Systems］のツリービューから［ネットワーク管理］－［管理 LAN］を選択し、DCB スイッチの管理ポートのＩＰアドレス等を設定します。

3.3.4　Telnet サービス

(1) telnet 接続の確立

Telnet 接続は、ポート２３(デフォルト設定)を使って、ネットワーク経由でリモートホストからスイッチへアクセスできるようにします。しかし、Telnet はセキュアではありません。セキュアな接続が必要な場合は、SSH を使用してください。

１．Telnet 接続を確立するには、'telnet'コマンドとスイッチの IP アドレスを入力します。

```
> telnet 10.17.37.157
```

スイッチが起動しており、Telnet サービスが有効であれば、次に示す応答があります。

```
Trying 10.17.37.157...
Connected to 10.17.37.157.
Escape character is '^]'.
Network OS (sw0)
switch# login:
```

２．一旦 Telnet 接続が確立されると、正常にログインすることが出来ます。

NOTE

'telnet'コマンドに、オプションの"port"引数を指定して、デフォルトポートを変更することができます。しかし、接続するにはスイッチ側でそのポート番号を listen するよう設定しておく必要があります。

以下の例では、デフォルトポートを変更します。

```
> telnet 10.17.37.157 87
```

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

Network OS (sw0)
sw0 login:
```

次の機能は、telnet ではサポートしていません。

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

(2) Telnet サービスの停止

Telnet サービスの停止は、スイッチ上で動作している全ての Telnet 接続を強制的に切断します。Telnet サービスを停止するには、グローバルコンフィグレーションモードで設定します。

1．Telnet サービスを停止するために、'telnet sever shutdown'を入力します。

```
switch(config)# telnet server shutdown
switch(config)#
```

全ての Telnet 接続は即座に切断され、Telnet サービスが有効化されるまで全ての Telnet 接続することができません。

NOTE

もし、VCS モードの場合は、次に示すように、コマンド入力する前に RBridge ID を設定する必要があります。

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# telnet server shutdown
```

(3) Telnet サービスの有効化

Telnet サービスを有効化すると、スイッチへの Telnet アクセスが可能となります。Telnet サービスを有効化するには、グローバルコンフィグレーションモードで設定します。

1．Telnet サービスを有効化するために、'no telnet sever shutdown'入力します。

```
switch(config)# no telnet server shutdown
switch(config)#
```

NOTE

もし、VCS モードの場合は、次に示すように、コマンド入力する前に RBridge ID を設定する必要があります。

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# no telnet server shutdown
```

3.3.5　SSH での接続

SSH(Secure Socket Handling)プロトコルを使った接続は、暗号化されたセキュアな接続が可能となります。

(1) SSH 接続の確立

1．特権実行モードでデフォルトのパラメータを使用して SSH 接続を確立するためには、'ssh -l '<username> <ip_address>コマンドを入力します。

```
switch# ssh -l admin 10.20.51.68
```

2．プロンプトに対して、'yes'を入力します。

```
The authenticity of host '10.20.51.68 (10.20.51.68)' can't be established.
RSA key fingerprint is ea:32:38:f7:76:b7:7d:23:dd:a7:25:99:e7:50:87:d0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.20.51.68' (RSA) to the list of known hosts.
admin@10.20.51.68's password: ********
WARNING: The default password of 'admin' and 'user' accounts have not been
changed.
Welcome to the Brocade Network Operating System Software
admin connected from 10.20.51.66 using ssh on C60_68F
```

NOTE

デフォルトの暗号化およびハッシュアルゴリズムを変更するには、-m および-c オプションを使用します。

```
switch# ssh -l admin -m hmac-md5 -c aes128-cbc 10.20.51.68
```

(2) SSH 公開鍵の取り込み

スイッチに対して認証されたログインを確立することが出来ます。特権実行モードでスイッチに公開鍵を取り込みます

NOTE

次の例は、証明書を使ってリモートホストから"admin"ユーザーに対する公開鍵を取り込んでいます。

1．公開鍵を取り込むために、'certutil import sshkey' user <Username> host <IP_Address> directory <File_Path> file <Key_filename> login <Login_ID>コマンドを入力します。

```
switch# certutil import sshkey user admin host 10.70.4.106 directory /users/
home40/bmeenaks/.ssh file id_rsa.pub login fvt
```

2．パスワードを入力します。

```
Password: ***********
switch# 2012/11/14-10:28:58, [SEC-3050], 75,, INFO, VDX6720-60, Event: sshutil,
Status: success, Info: Imported SSH public key from 10.70.4.106 for user 'admin'.
```

NOTE

もし、VCS モードの場合は、次に示すように、RBridge ID を引数に設定する必要があります。

```
switch# certutil import sshkey user admin host 10.70.4.106 directory /users/home40/
bmeenaks/.ssh file id_rsa.pub login fvt rbridge-id 3
```

(3) SSH 公開鍵の削除

SSH 公開鍵を認証されたログインに使用されないようにします。特権実行モードで SSH 公開鍵を削除してください。

1．SSH 公開鍵を削除するために、'no certutil sshkey user <Username>'に続いて、'rbridgeid <rbridge-id>' か'rbridge-id all'を入力します。

```
switch# no certutil sshkey user admin rbridge-id all
```

指定した RBridge-ID から key が削除されるか、全ての RBridge-ID から key が削除されます。

(4) SSH サービスの停止

スイッチで実行されている全ての SSH 接続を強制的に切断します。グローバルコンフィグレーションモードで実行します。

1．SSH サービスを停止するために、'ssh server shutdown'を入力します。

```
switch(config)# ssh server shutdown
switch(config)#
```

全ての SSH 接続は即座に切断され、SSH サービスが有効化されるまで全ての SSH 接続することができません。

NOTE

もし、VCS モードの場合は、次に示すように、コマンド入力する前に RBridge ID を設定する必要があります。

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# ssh server shutdown
```

(5) SSH サービスの有効化

S サービスを有効化すると、スイッチへの SSH アクセスが可能となります。SSH サービスを有効化するには、グローバルコンフィグレーションモードで設定します。

1．SSH サービスを有効化するために、'no ssh sever shutdown'入力します。

```
switch(config)# no ssh server shutdown
switch(config)#
```

NOTE

VCS モードの場合は、次に示すように、コマンド入力する前に RBridge ID を設定する必要があります。

```
switch(config)# rbridge-id 3
switch(config-rbridge-id-3)# no ssh server shutdown
```

3.4 スイッチの管理と設定

3.4.1 ロジカルシャーシモードのスイッチ設定

26 ページの『1.2.3 ロジカルシャーシ』を参照してください。

(1) ロジカルシャーシクラスタの設定

この章では、全ての物理接続要件が満足されている想定で、ロジカルシャーシクラスタを生成する手順を説明しています。

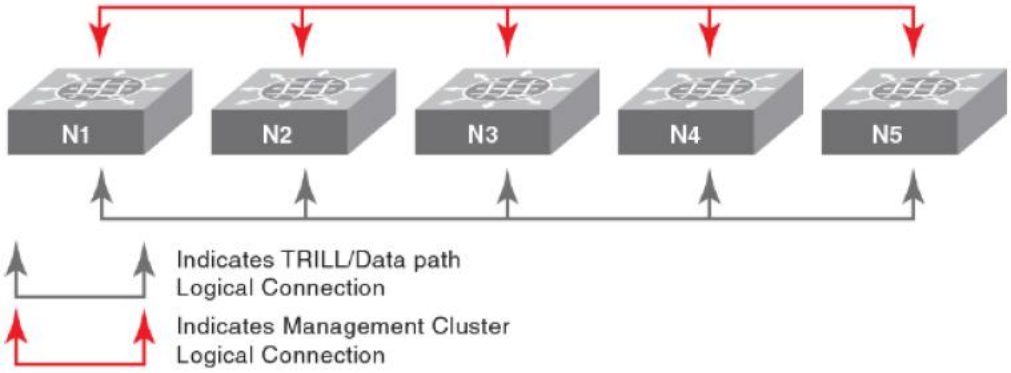

図 3-5 ５ノードで構成するロジカルシャーシクラスタ

ロジカルシャーシクラスタを生成するため、次の例に示す手順を実行します。

1. ロジカルシャーシのメンバとしたいスイッチにログインします。
2. 特権実行モードで、'vcs'コマンドを VCD ID,RBridge ID 付きで実行し、ロジカルシャーシモードを有効化します。以下に示す VCS ID と RBridge ID は、この例用に選択したものです。

```
switch# vcs vcsid 22 rbridge-id 15 logical-chassis enable
```

3. 'vcs'コマンドを実行した後、スイッチはリブートします。"if you want to apply the default configuration" のプロンプトには、"y"と応答します。
4. クラスタ内の各ノードに、RBridge ID だけを変更しながら、上記の手順を繰り返します。しかし、VCS ID はクラスタに属する各ノードで同じ値にしなければなりません。
5. クラスタの各ノードでロジカルシャーシモードを有効にしたら、どのノードが principal ノードに割り当てられたかを確認するため、'show vcs'コマンドを実行します。山形括弧(>)が principal ノードを示します。アスタリスク(*)は、現在ログインしているノードを示します。

```
switch# show vcs
Config Mode    : Distributed
VCS ID         : 1
VCS GUID       : 86024da1-b2c2-4b35-955d-41c27598aaa0
Total Number of Nodes          : 2
RBridge-Id       WWN                              Management IP   Status           HostName
-----------------------------------------------------------------------------------------
154             >10:00:00:05:33:51:63:42*         10.17.37.154    Online           switch
                                                  2607:f0d0:1002:ff51:ffff:ffff:ffff:fff5
165              10:00:00:05:33:B7:F0:00          10.17.37.165    Online
```

山形括弧が示す WWN を持つ Bridge ID は、クラスタの principal です。この例では、RBridge ID が 154 です。

6. principal ノードで、時計とタイムゾーンを設定します。時刻は、全てのノードにわたって同期されます。詳細は、79 ページの『4 ネットワークタイムプロトコル』を参照してください。

7．クラスタの principal にログインし、グローバルコンフィグ/ローカルコンフィグを変更します。これらの変更は、ロジカルシャーシクラスタ内の全てのノードに自動的に配信されます。

NOTE
principal ノードから、いずれの RBridge に対しても、RBridge ID のコンフィグレーションモードを変更することが出来ます。また、'logical-chassis principal priority'コマンドや'logical chassis principal switchover'コマンドを使って、principal ノードを変更することも出来ます。更に詳細な情報は、68 ページの『3.4.1 (5)クラスタの principal ノードの選択』を参照ください。

---

(2) モード切替に対する事前注意事項
遷移した全てのノードが Network OS の同じバージョンで動作していることを保証してください。ロジカルシャーシクラスタモードは、Network OS 4.1 以降でサポートしています。
もし、一つの新しいグローバルコンフィグレーションを生成するため、多数のグローバルコンフィグレーションファイルをマージするなら、同じエンティティ名称がマージされたファイルに無いことを確認してください。例えば、"mac access-list extended test1"が、下記に示すように"Node 1 global configuration"と"Node 2 global configuration"を含むなら、ファイルをマージする際に、"Combined global configuration"に示すように、Node2 の"mac access-list extended test1"を"mac access-list extended test2"に変更しなければなりません。

(a) Node 1 global configuration

```
mac access-list extended test1
seq 10 permit any 1111.2222.333a ffff.ffff.ffff
seq 20 deny any 1111.2222.333b ffff.ffff.ffff
```

(b) Node 2 global configuration

```
mac access-list extended test1
seq 10 permit any 4444.5555.666d ffff.ffff.ffff
seq 20 deny any 4444.5555.666e ffff.ffff.ffff
```

(c) Combined global configuration

```
mac access-list extended test1
seq 10 permit any 1111.2222.333a ffff.ffff.ffff
seq 20 deny any 1111.2222.333b ffff.ffff.ffff
seq 30 deny any 1111.2222.333c ffff.ffff.ffff
seq 40 permit any any
!
```

Node2 のローカルコンフィグレーションも、また、同じように変更する必要があります。この例では、ローカルコンフィグレーション変更の一部が"interface TenGigabitEthernet"となっています。"test1"を

参照する代わりに、変更がグローバルコンフィグレーションとなるために、Node2 のローカルコンフィグレーションは変更する必要があります。これは、下記の"(e) グローバルコンフィグレーション整合後の Node 2 local configuration "に示されます。

(d) グローバルコンフィグレーション整合前の Node 2 local configuration

```
interface TenGigabitEthernet 4/0/3
fabric isl enable
fabric trunk enable
switchport
switchport mode access
```

(e) グローバルコンフィグレーション整合後の Node 2 local configuration

```
interface TenGigabitEthernet 4/0/3
fabric isl enable
fabric trunk enable
switchport
switchport mode access
```

ATTENTION

下記の事前注意事項を確認してください。

- ロジカルシャーシクラスタモードでの'copy default-config startup-config'コマンドは、クラスタ全体のリブートを引き起こし、ロジカルシャーシクラスタ全体をデフォルトコンフィグレーションに戻します。このため、ロジカルシャーシクラスタに存在する全ての設定を破棄したい場合にだけ使用します。
- グローバル/ローカルコンフィグレーションのバックアップファイルは、回復中ロジカルシャーシクラスタに容易に取り出すことが出来る適切な SCP サーバか FTP サーバで利用できることを確かめてください。スイッチローカルには格納しないでください。理由は、ローカルコンフィグレーションは principal ノードでは利用できないためです。

(3) ファブリッククラスタからロジカルシャーシクラスタへの変換

デフォルトコンフィグレーションファイルを使って、既存のファブリッククラスタをロジカルシャーシクラスタに変換できます。

1. 全てのノードで同じファームウェアバージョンが動作していることを確かめてください。ロジカルシャーシクラスタモードは、Network OS 4.1 以降でサポートされます。
2. ファブリッククラスタからロジカルシャーシクラスタに遷移させたい全てのノードが稼働中であることを確認してください。ノードの状態をチェックするため、'show vcs'や'show vcs detail'コマンドを実行してください。

3. ファブリッククラスタモードからロジカルシャーシクラスタモードへ変更したいノードへログインしてください。
4. 特権実行モードで、'vcs logical-chassis enable'コマンドを必要なオプション付きで実行してください。例えば、次の一つのコマンドなら、全ての RBridge を変更できます。

```
switch# vcs logical-chassis enable rbridge-id all default-config
```

NOTE
特定の RBridge をファブリッククラスタモードからロジカルシャーシモードに変更するには、"all"の位置に RBridge ID を指定します。また、"1,3,4-6"のように範囲を指定することも出来ます。詳細は、『Network OS Command Reference』を参照ください。

5. 全てのノードが稼働中か、ロジカルシャーシクラスタモードとなっている("Distributed"と表示される)かを確認するため、'show vcs'か'show vcs detail'を実行します。
6. 'show vcs'コマンド出力は、どのノードが principal に割り当てられたかを確認することも出来ます。

```
switch# show vcs
R-Bridge   WWN                     Switch-MAC           Status
_____________________________________________________________
1      > 11:22:33:44:55:66:77:81    AA:BB:CC::DD:EE:F1    Online
2        11:22:33:44:55:66:77:82    AA:BB:CC::DD:EE:F2    Online
3        11:22:33:44:55:66:77:83*      AA:BB:CC::DD:EE:F3    Online
```

山形括弧が示す WWN を持つ Bridge ID は、クラスタの principal です。この例では、RBridge ID が 1 です。
7. クラスタの principal にログインし、グローバルコンフィグ/ローカルコンフィグを変更します。これらの変更は、ロジカルシャーシクラスタ内の全てのノードに自動的に配信されます。

NOTE
principal ノードから、いずれの RBridge に対しても、RBridge ID のコンフィグレーションモードを変更することが出来ます。また、'logical-chassis principal priority'コマンドや'logical chassis principal switchover'コマンドを使って、principal ノードを変更することも出来ます。更に詳細な情報は、68 ページの『3.4.1 (5)クラスタの principal ノードの選択』を参照ください。

(4) コンフィグレーションを保存しながらファブリッククラスタを変更
コンフィグレーションを保存しながらファブリッククラスタをロジカルシャーシクラスタに変更する特別なコマンドはありません。しかし、次の示す手順で実現できます。

1. 全てのノードで同じファームウェアバージョンが動作していることを確かめてください。ロジカルシャーシクラスタモードは、Network OS 4.1 以降でサポートされます。
2. ファブリッククラスタからロジカルシャーシクラスタに遷移させたい全てのノードが稼働中であることを確認してください。ノードの状態をチェックするため、'show vcs'や'show vcs detail'コマンドを実行してください。

3. ロジカルシャーシクラスタで使用したいグローバルコンフィグレーションを含むノードを決定します。そして、'copy global-running-config'コマンドを実行し、リモート ftp,scp,sftp のファイルにコンフィグレーションを格納することでバックアップを採ります。

NOTE

もし2つ以上のノードのグローバルコンフィグレーションを結合する必要がある場合、ロジカルシャーシクラスタモードへ遷移した後、'copy global-running-config <location_config_filename>'コマンドを使って生成されたーつのファイルに、必要とするファイルを手動で結合してください。詳細は、64 ページの『3.4.1 (2)モード切替に対する事前注意事項』を参照ください。

---

4. 各ノードで'copy local-running-configuration'コマンドを使って、リモート ftp,scp,sftp のファイルにコンフィグレーションを格納することで、全ての個々のノードのローカルコンフィグレーションをバックアップしてください。
5. 65 ページの『3.4.1 (3)ファブリッククラスタからロジカルシャーシクラスタへの変換』に示すように、'vcs logical-chassis enable rbridge-id all default-config'コマンドを使って、ファブリッククラスタからロジカルシャーシクラスタにモード遷移させます。
   ノードは、自動的にロジカルシャーシクラスタとして再起動します。モード遷移の間、暫く通信ダウンとなります。
6. 全てのノードが稼働中か、ロジカルシャーシクラスタモードとなっている("Distributed"と表示される)かを確認するため、'show vcs'か'show vcs detail'を実行します。
7. 'show vcs'コマンド出力は、どのノードが principal に割り当てられたかを確認することも出来ます。

```
switch# show vcs
R-Bridge   WWN                     Switch-MAC           Status
_____________________________________________________________
1     > 11:22:33:44:55:66:77:81    AA:BB:CC::DD:EE:F1   Online
2       11:22:33:44:55:66:77:82    AA:BB:CC::DD:EE:F2   Online
3       11:22:33:44:55:66:77:83*     AA:BB:CC::DD:EE:F3   Online
```

   山形括弧が示す WWN を持つ Bridge ID は、クラスタの principal です。この例では、RBridge ID が 1 です。
8. ロジカルシャーシクラスタの principal にログインし、リモートサーバに格納されたグローバルコンフィグレーションファイルを、次の通り principal ノードにコピーします。

```
copy <location_config_filename> running-config
```

9. 'show global-running-config'コマンドを実行し、グローバルコンフィグレーションが利用可能かを確認します。
10. ロジカルシャーシクラスタの principal にログインし、リモートサーバに格納されたローカルコンフィグレーションファイルを、次の通り principal ノードにコピーします。

```
copy <location_config_filename> running-config
```

NOTE

各ノードで格納したローカルコンフィグレーションファイルに対して、このコマンドを実行します。

コンフィグレーションファイルは、ロジカルシャーシクラスタの全てのノードに自動的に配信されます。各ノードは、上記の手順が実行された後、同じグローバルコンフィグレーションを持ちます。各ノードは、また、他の全てのノードのローカルコンフィグレーションも持ちます。

１１．'show local-running-config'コマンドを使って、ローカルコンフィグレーションが利用可能かを確認してください。

１２. クラスタの principal にログインし、グローバルコンフィグ/ローカルコンフィグを変更します。これらの変更は、ロジカルシャーシクラスタ内の全てのノードに自動的に配信されます。

NOTE

principal ノードから、いずれの RBridge に対しても、RBridge ID のコンフィグレーションモードを変更することが出来ます。また、'logical-chassis principal priority'コマンドや'logical chassis principal switchover'コマンドを使って、principal ノードを変更することも出来ます。更に詳細な情報は、68 ページの『3.4.1 (5)クラスタの principal ノードの選択』を参照ください。

---

(5) クラスタの principal ノードの選択

ロジカルシャーシクラスタ principal ノードは以下の通り動作します。

- ロジカルシャーシクラスタの全てのコンフィグレーションを principal ノードで実行します。
- デフォルトで、もっとも小さい WWN 番号を持つノードが principal ノードとなります。
- どのノードが principal かを確認するため、'show vcs'コマンドを実行します。山形括弧が principal ノードの WWN を示します。
- 次の例に示すように、'logical chassis principal priority'コマンドに続いて、'logical-chassis principal switchover'コマンドを使用することで、ロジカルシャーシクラスタ内のいずれのノードでも principal ノードにすることが出来ます。

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# logical-chassis principal-priority 1
```

小さい番号が高プライオリティを意味します。値の範囲は、1 から 128 です。

'logical-chassis principal switchover'コマンドを実行するまで、新しい principal ノードは有効になりません。

(6) ロジカルシャーシクラスタからファブリッククラスタへの変換

ロジカルシャーシクラスタの全てのノードをファブリッククラスタに遷移させるために、デフォルトコンフィグレーションを使用します。次の手順を実行してください。

１. ロジカルシャーシクラスタからファブリッククラスタに遷移させたい全てのノードが稼働中かを確認してください。ノードの状態をチェックするために、'show vcs'または'show vcs detail'コマ

ンドを実行してください。

2．ロジカルシャーシクラスタの principal ノードにログインします。

3．全ての RBridge ID を遷移させるために、'no vcs logical-chassis enable rbridge-id <all> default-config'コマンドを実行します。

NOTE

一つの RBridge ID だけを遷移するためには、'no vcs logicalchassis enable rbridge-id <rbridge-id> default-config'コマンドを実行します。

ノードは自動的にファブリッククラスタモードで再起動します。この遷移で暫く通信不可になります。

4. 全てのノードが稼動中でファブリッククラスタとなっているか("Local-only"と表示されます)を確認するために、'show vcs'か'show vcs detail'コマンドのいずれかを実行します。

(7) コンフィグレーションを保存しながらファブリッククラスタへの変換

コンフィグレーションを保持したまま、ロジカルシャーシクラスタからファブリッククラスタに変換するために特別なコマンドはありません。次の手順時実行してください。

1. ロジカルシャーシクラスタからファブリッククラスタに遷移させたい全てのノードが稼働中かを確認してください。ノードの状態をチェックするために、'show vcs'または'show vcs detail'コマンドを実行してください。

2．それぞれのノードで'copy rbridge-running-config rbridge-id'コマンドを実行し、リモート ftp,scp,sftp のファイルにコンフィグレーションを格納することで、全てのノードのコンフィグレーションをバックアップします。

```
copy rbridge-running-config rbridge-id <rbridge-id> <location_config_filename>
```

このコマンドは、指定した RBridge ID のグローバル/ローカルコンフィグレーションの両方をコピーします。

3．ロジカルシャーシクラスタの Principal ノードから、次のコマンドを使って、デフォルトコンフィグによりクラスタ全体をファブリッククラスタに遷移させます。

```
no vcs logical-chassis enable rbridge-id all default-config
```

ノードは自動的にファブリッククラスタモードで再起動します。この遷移で暫く通信不可になります。

4. 全てのノードが稼動中でファブリッククラスタとなっているか("Local-only"と表示されます)を確認するために、'show vcs'か'show vcs detail'コマンドのいずれかを実行します。

5. 各ノードで次のコマンドを実行することによりバックアップされたコンフィグに対してグローバルコンフィグとローカルコンフィグをレストアします。

```
copy <location_configfilename> running-config
```

6．各ノードに対してダウンロードしたコンフィグレーションを恒久的にするため、'copy running-config startup-config'を実行します。

(8) ロジカルシャーシクラスタへのノード追加
ノードは、既存のロジカルシャーシクラスタに動的にノードを追加できます。もし、既存のクラスタと新しいノードが正常な物理接続で接続されたなら、処理は自動的に実行されます。
新しいノードにログインして、'vcs logical-chassis enable'コマンドを実行します。新しいノードには、既存のクラスタの VCS ID を割り当てる必要があります。
追加したノードの状態が"online"かどうかを確かめるため、'show vcs'コマンドを実行します。

(9) ロジカルシャーシクラスタからノードの削除
ロジカルシャーシクラスタモードのスイッチで、'no vcs enable'コマンドを実行すると、スイッチはスタンドアロンモードで起動します。(BS500/2000 搭載の DCB スイッチのみ。)ロジカルシャーシクラスタモードのスイッチで、'no vcs logical-chassis'を実行すると、スイッチはファブリッククラスタモードで起動します。
一旦ノードが削除されると、そのノードに関連する全てのコンフィグレーションは、クラスタのコンフィグレーションデータベースから削除されます。同様に、削除されたノードは、クラスタ内の他のノードに関連するコンフィグレーションは保持されません。
次に、ノード N5 が削除された後のクラスタを示します。ノード N1 から N4 はクラスタに残っており、N5 は分離しています。ノード N5 とクラスタの間には、データパスも管理パスもありません。

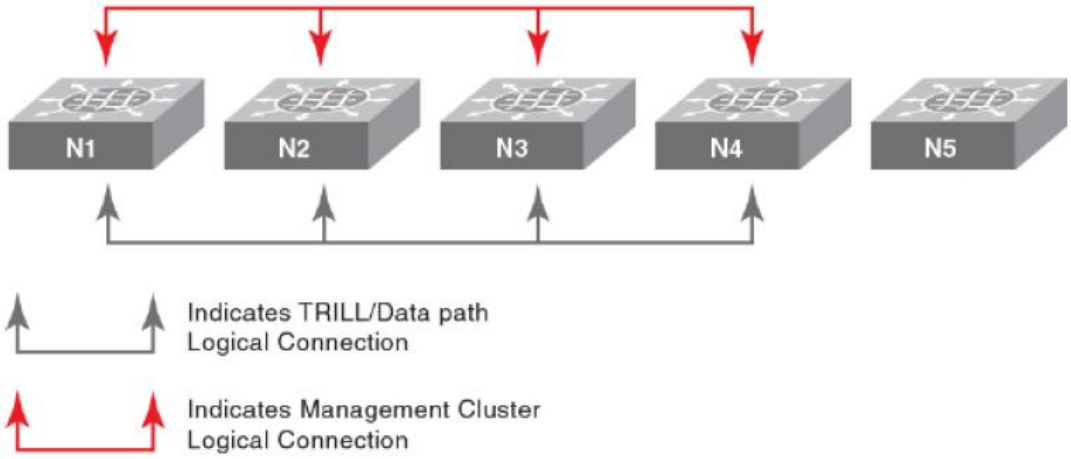

図 3-6　ロジカルシャーシクラスタから N5 ノードを削除

(10) クラスタへの再ノード追加
ロジカルシャーシクラスタから一時的に隔離されたノードは、削除されたノードかクラスタのいずれかでコンフィグレーションかクラスタメンバの変更が無い限り、再度参加することができます。ノードをクラスタに再度参加するため、'vcs logical-chassis enable'コマンドを実行します。
しかし、ノードが削除されてからノードまたはクラスタにコンフィグレーションの変更があった場合、分離されたノードに'copy default-config startup-config'コマンドを実行し、デフォルトコンフィグレーションでリブートさせなければなりません。

(11) ロジカルシャーシクラスタへのノードの交換

ロジカルシャーシクラスタのノードが故障し使用できなくなった場合、同一の機能をもった類似したノードが換わりに使われます。

新しいノードは、交換されたノードと同じ RBridge ID が使用されなければなりません。新しいノードが見つかると、新しいノードと見なされる代わりに以前知られていたノードとしてクラスタに参加します。

RBridge ID 3 のノードを交換し、新しいノードの WWN を入力するため、次の例にある手順を実行します。

1．Principal スイッチで次のコマンドを実行します。

```
switch# vcs replace rbridge-id 3
```

新しい交換用スイッチの WWN(11:22:33:44:55:66:77:81)を入力します。

2．新しいノードが既に VCS が有効化されている前提で、新しいノードで次のコマンドを実行して新しいノードに RBridge ID 3 を割り当てます。

```
switch# vcs rbridge-id 3
```

NOTE

新しいノードがまだ VCS 有効になってない場合、RBridge ID を割り当てるのと同時に有効にすることが出来ます。詳細は、『Network OS Command Reference』にある'vcs'コマンドのオプションを参照してください。

---

(12) ２つのロジカルシャーシクラスタのマイグレーション

同じ VCS ID を持つ２つのロジカルシャーシクラスタをマージすることができます。次の手順に従ってください。

1．２つの独立したクラスタ間を要求される物理接続で接続してください。

2．マージ後、どちらのクラスタのコンフィグレーションを保持するかを決めてください。保存できるコンフィグは一つだけです。

3．コンフィグを保持しないクラスタで、デフォルトコンフィグで再起動するよう'copy default-config startupconfig'コマンドを実行してください。

4．それぞのれクラスタで、全てのノードを再起動します。コンフィグレーションが保持されるロジカルシャーシクラスタは、他のクラスタを新しいノードとして認識し、それに応じて追加します。

5．コンフィグレーションを保持しないクラスタに、コンフィグレーションを再適用します。

(13) ファブリック内のスイッチの RBridge ID の変更

再起動してクラスタから孤立してしまったスイッチ上で、RBridge ID 番号を変更することが必要なことがあります。

1．ローカルコンフィグレーションがデフォルト値にリセットされているかも知れないので、RBridge ID を変更する前にグローバルコンフィグレーションをバックアップします。86 ページの『5.5 コ

ンフィグレーションのバックアップ』を参照してください。

2．再起動したスイッチ上で、'chassis disable'コマンドを実行します。

```
switch# chassis disable
```

3．ファブリック Principal スイッチから、'no vcs enable rbridge-id <rbridge-id>'コマンドを実行します。<rbridge-id>には、孤立したスイッチの RBridge ID を指定します。

```
switch# no vcs enable rbridge-id 3
```

4．再起動したスイッチ上で、'vcs rbridge-id <rbridge-id>'コマンドを実行します。<rbridge-id>には、使用したい RBridge ID を指定します。

5．'vcs rbridge-id <rbridge-id>'に VCS ID を指定しなければ、既に使用されているものが使われます。

6．孤立したスイッチを再起動します。

スイッチ再起動後、次の動作が有効となります。

- 全てのインタフェースは shutdown となります。スイッチがクラスタに再参加する前に、ISL インタフェースに対して、'no shutdown'を実行します。
- オリジナルのコンフィグレーションは失われ、スイッチは新しい RBridge ID でクラスタに再参加するときデフォルトコンフィグレーションが使われます。

7．スイッチがファブリックに組み込まれたかを確認するため、'show vcs detail'を使います。

```
switch# show vcs detail
Config Mode : Local-Only
VCS ID : 1
Total Number of Nodes : 6
Node :1
Serial Number : BKN2501G00R
Condition : Good
Status : Connected to Cluster
VCS Id : 1
Rbridge-Id : 38
Co-ordinator : NO
WWN : 10:00:00:05:33:52:2A:82
Switch MAC : 00:05:33:52:2A:82
FCF MAC : 0B:20:B0:64:10:27
Switch Type : BR-VDX6720-24-C-24
Internal IP : 127.1.0.38
Management IP : 10.17.10.38
Node :2
Serial Number : BZA0330G00P
```

(14) グローバルコンフィグレーションとローカルコンフィグレーションの例

次の表は、それぞれのコンフィグレーションモードで使用できる、グローバルコンフィグレーションコマンドとローカルコンフィグレーションコマンドの例です。これらの設定は、'show global-running-config'と'show local-running-config'コマンドによって、それぞれ表示することが出来ます。

表 3-5　グローバル/ローカルコンフィグレーションコマンド

グローバルコンフィグレーションコマンド	ローカルコンフィグレーションコマンド
Interface vlan	switch-attributes

interface port-channel	interface management
port-profile	interface ve
mac access-list	switch-attributes
ip access-list	fabric route mcast
snmp-server	rbridge-id
protocol lldp	ip route
cee-map	interface management
username	interface gigabitethernet
	interface tengigabitethernet
	interface fortygigabitethernet

ftp/scp サーバから、または、サーバへコンフィグレーションのスナップショットファイルをアップロード/ダウンロードする場合は、'copy snapshot'コマンドを使用してください。クラスタから切り離されたノードのコンフィグレーションのスナップショットをとる場合は、これらのコマンドを使う必要があります。
これらコマンド及びその他のロジカルシャーシサーバコマンドの詳細については、『Network OS Command Reference』を参照してください。

3.4.2 ファブリッククラスタモードの設定

装置の VCS 設定を表示するには、'show vcs' コマンドを発行します。以下のコマンド出力は、1 の VCS ID と 1 の RBridge ID を持つ単一ノードの VCS を示しています。デフォルト値を変更するには、VCS コマンドを使用します。56 ページの『3.2.2 ファブリッククラスタモード』も参照してください。

```
switch# show vcs
Config Mode     : Local-Only
VCS ID           : 1
Total Number of Nodes            : 2
Rbridge-Id    WWN                    Management IP    Status          HostName
-----------------------------------------------------------------------------
1         10:00:00:05:33:15:DE:CC  10.24.82.120     Online          dutA1-sw0
                                       fd00:60:69bc:64:205:33ff:fe15:decc
```

3.4.3 スタンドアロンモードの設定

BS500/2000 搭載の DCB スイッチで、工場出荷直後の VCS 設定を表示すると VCS モードが無効になっていることを示しています。VCS モードを有効にするには'vcs enable'コマンドを使用します。スイッチが再起動され、VCS モードで起動します。コンフィグレーション変更前は、常にスイッチの状態を確認してください。56 ページの『3.2.3 スタンドアロンモード』も参照してください。

```
switch# show vcs
state: Disabled
```

3.4.4 管理インタフェースの表示

管理インタフェースの設定を表示するには、いくつかの方法があります。次表に管理インタフェース

の表示方法を示します。

表 3-6　管理インタフェースの表示方法

コマンド	アウトバンドインタフェース (シャーシ内管理ポート or パネル装備管理ポート)	インバンドインタフェース (通信ポート)
show interface Management	○	―
show interface vlan *VLAN_ID*	―	○
oscmd ifconfig	eth0 または eth0.xxxx で表示 xxxx：内部管理用 VLAN ID	vlan0.*VLAN_ID* で表示

以下に、それぞれのコマンドの表示例を示します。

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

```
switch# show interface vlan 100
Vlan 100 is up, line protocol is down (link protocol down)
Address is 0005.338e.92b9, Current address is 0005.338e.92b9
Interface index (ifindex) is 1207959652
Queueing strategy: fifo
 Primary Internet Address is 192.168.100.75/24 broadcast is 192.168.100.255
Time since last interface status change: 00:25:20
```

```
switch# oscmd ifconfig
eth0      Link encap:Ethernet  HWaddr 00:05:33:8E:92:98
          inet addr:192.168.0.75  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:289722 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10305 errors:3 dropped:0 overruns:0 carrier:3
          collisions:0 txqueuelen:1000
          Base address:0x6000

eth0.4089 Link encap:Ethernet  HWaddr 00:05:33:8E:92:98
          inet addr:192.168.253.40  Bcast:192.168.253.47  Mask:255.255.255.240
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:75 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.255.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:36896 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36896 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

3.4.5　管理インタフェースの速度の設定

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

3.4.6　バナーの設定と表示

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

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

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

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

3.4.7　スイッチの情報設定

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

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

(1) ホスト名の設定と表示

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

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# switch-attributes ?
Possible completions:
```

```
  <NUMBER:1-239> Specify the rbridge-id 1
switch(config)# switch-attributes 1
switch(config-switch-attributes-1)# host-name lab1_vdx0023
lab1_vdx0023(config-switch-attributes-1)# exit
lab1_vdx0023(config)# do copy running-config startup-config
lab1_vdx0023(config)# do show running-config switch-attributes 1
switch-attributes 1
  chassis-name VDX6720-24
  host-name lab1_vdx0023
```

(2) シャーシ名の設定と表示

1．グローバルコンフィグレーションモードに入るため、'configure terminal'コマンドを実行します。

2．ローカル RBridge ID を決定するため、'switch-attributes'コマンドに続けてクエスチョンマーク("?")を入力します。

3．'switch-attributes'コマンドに続いて RBridge ID を入力します。

4．'chassis-name'オペランドに続いて、シャーシ名を入力します。

5．'copy running-config file startup-config'コマンドを使って、変更を格納します。

6．'do show running-config startup-config'コマンドに続けて rbridge-id を入力して構成の変更内容を確認します。

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

(3) スイッチタイプ

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

```
switch# show chassis
Chassis Family: VDX64xx
Chassis Backplane Revision: 1
switchType: 1000
Use table to convert this parameter
(output truncated)
```

3.4.8　装置の有効化・無効化

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

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

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

3.4.9 装置のリブート

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

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

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

3.5 トラブルシューティング

3.5.1 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。

(1) 外部ホストへの supportsave データのアップロード

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

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

(2) supportsave 操作のステータス表示

'show copy-support status'コマンドを入力します。

```
switch# show copy-support status

Slot Name        SS type         Completion Percentage
#########################################################
SWITCH            NORMAL          [100%]
```

(3) supportsave データの自動アップロード設定

supportSave 情報を収集するために faist-fault data capture(FFDC)とトレースデータファイルを自動的にリモートサーバにアップロードするようにスイッチを設定することができます。

この機能を有効にするには、専用サーバを構成する必要があります。この機能を有効にするには、以下の例に示す'autoupload enable'コマンドを使用します。

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

(4) 自動アップロード設定の表示

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

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

(5) 追加の supportsave コマンド

追加の supportsave データを収集するために次のコマンドを使用します。

- 'show support'コマンドで、core ファイルのリストを表示します。
- 'clear support'コマンドで、サポートデータを消去します。

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

3.5.2 メッセージロギング

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

NOTE

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

4 ネットワークタイムプロトコル

4.1 日付と時刻の設定

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

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

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

- YYYY は、年を指定します。年の値の範囲は 1970～2038 です。
- MM は、月を指定します。月の値の範囲は 01～12 です。
- DD は、日を指定します。日の値の範囲は 01～31 です。
- T は固定で"T"を入力します。
- HH は、時を指定します。時の値の範囲は 00～23 です。
- MM は、分を指定します。分の値の範囲は 00～59 です。
- SS は、秒を指定します。秒の値の範囲は 00～59 です。

以下に日付と時刻の設定および表示の例を示します。

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

4.2 タイムゾーンの設定

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

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

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

4.2.1 タイムゾーン設定

スイッチのタイムゾーンを設定するには、’clock timezone’コマンドを使用します。このコマンドを使用して、タイムゾーンを設定する必要のあるすべてのスイッチを設定する必要があります。タイムゾーンの設定は、不揮発メモリに格納されますので、各スイッチで一度、設定する必要があります。
設定可能な地域や都市の完全なリストについては、340 ページの『26 サポートされているタイムゾーンと地域』を参照してください。
'clock timezone region [/country|/state/] city'コマンドを入力します。

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

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

4.2.2 現在の時刻とタイムゾーンの表示

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

NOTE
このコマンドはローカルスイッチ上の現在をサポートします。

'show clock'コマンドを入力します。

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

4.2.3 タイムゾーン設定の削除

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

```
switch# no clock timezone
```

4.3 Network Time Protocol

Network Time Protocol (NTP)は、ネットワーク内のすべてのスイッチで同一な時間を維持します。NTP コマンドは、ネットワーク内のすべてのローカルクロック間の時刻同期を維持するために、外部のタイムサーバの設定をサポートします。
ネットワーク内の時間を最新の状態に維持するため、各スイッチは、少なくとも一つの外部 NTP サーバと時刻同期することをお勧めします。外部 NTP サーバはファブリック全体の時刻同期を維持するために、互いに同期させる必要があります。

ファブリック内のすべてのスイッチは、不揮発性メモリに現在のクロックサーバの値を維持します。デフォルトでは、この値は、スイッチのローカルクロックサーバになります。

NOTE

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

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

4.3.1 外部ソースへのローカル時間の同期

'ntp server'コマンドを使用して、NTP サーバとローカルスイッチの時刻を同期します。

'ntp server'コマンドは 5 つの IP アドレスを登録できます。リスト内の少なくともーつの IP アドレスが到達可能な NTP サーバを設定しなければなりません。

'ntp server <*ip_address*>'コマンドを入力します。

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

4.3.2 アクティブな NTP サーバの表示

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

NOTE

引数に"all"を指定すると、ローカルな情報のみを表示します。

'show ntp status'コマンドを入力します。

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

4.3.3 NTP サーバ IP アドレスの削除

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

‘no ntp server’コマンドを入力します。

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

5 構成情報の管理

5.1 スイッチ構成情報の概要

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

- running configuration を startup configuration ファイルへの格納(85 ページの『5.4 コンフィグレーションの変更の格納』参照)
- コンフィグレーションファイルのリモートサーバへのアップロード(86 ページの『5.5 コンフィグレーションのバックアップ』参照)
- アーカイブからのコンフィグレーションファイルの回復(87 ページの『5.6 コンフィグレーションの回復』参照)
- すべてのスイッチのコンフィグレーションファイルをリモートへのアーカイブ(89 ページの『5.7 VCS ファブリックモードでの構成情報管理』参照)
- リモートから複数のスイッチへのコンフィグレーションファイルのダウンロード(89 ページの『5.7 VCS ファブリックモードでの構成情報管理』参照)

5.2 フラッシュメモリ上のファイル管理

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

5.2.1 フラッシュメモリファイルの一覧表示

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

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

5.2.2 フラッシュメモリからファイルの削除

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

```
switch# delete myconfig
```

5.2.3　ファイル名の変更

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

```
switch#rename myconfig myconfig_20101010
```

5.2.4　フラッシュメモリ上のファイルの内容表示

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

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

NOTE

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

5.3 コンフィグレーションファイルのタイプ

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

表 5-1　標準のスイッチコンフィグレーションファイル

ファイルのタイプ	説　明
Default configuration ·defaultconfig.novcs ·defaultconfig.vcs	カスタマイズしたコンフィグレーションが利用できない場合は、デ default configuration が適用されます。 このコンフィグレーションはスタンドアロンと VCS ファブリックモード

	は、それぞれ別のコンフィグレーションファイルになります。
Startup configuration ·startup-config	起動時及びリブート後に有効になるコンフィグです。
Running configuration ·running-config	スイッチで現在使用しているコンフィグです。コンフィグレーションを変更する際は、running configuration に書き込まれます。running configuration は、startup configuration にコピーしなければ、リブート後に引き継がれません。

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

5.3.1 default configuration

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

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

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

(1) default configuration の表示

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

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

5.3.2 startup configuration

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

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

変更を保存すると、running configuration が startup configuration になります。

(1) startup configuration の表示

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

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

5.3.3 running configuration

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

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

(1) running configuration の表示

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

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

5.4 コンフィグレーションの変更の格納

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

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

NOTE

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

NOTE

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

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

・アクセスコントロールリスト(ACL)

・エッジループ検出機能(ELD)

・リンクアグリゲーション

5.4.1 running configuration の格納

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

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

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

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

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

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

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

2．ディレクトリの内容を表示して、作業内容を確認します。

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

5.4.3 以前に格納したコンフィグレーション変更の適用

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

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

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

5.5 コンフィグレーションのバックアップ

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

- ファブリック内のすべてのスイッチの startup configuration のバックアップコピーを採取する。

- 外部のホストにバックアップコピーをアップロードする。
- 一つのスイッチから別のコンフィグレーションファイルをコピーすることは避けてください。代わりにバックアップコピーからスイッチのコンフィグレーションファイルを復元します。

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

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

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

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

5.6 コンフィグレーションの回復

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

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

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

5.6.1 以前の startup configuration の回復

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

１．VCS ファブリックモードをディセーブルにしてスイッチを再起動します。
　VCS ファブリックモードに関連付けられているスタートアップコンフィグレーションは自動的

に削除されます。スイッチスタンドアロンモードで起動すると、対応するデフォルトコンフィグレーションをロードします。

2．FTP サーバから以前アーカイブした startup configuration ファイルを running configuration にコピーします。

3．スイッチの running configuration を startup configuration にコピーします。

```
switch# no vcs enable
```

ここでスイッチは自動的にリブートします。

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

ATTENTION

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

5.6.2 default configuration の回復

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

ファームウェアのデフォルト状態に回復するには、特権実行モードで以下の手順を実行します。

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

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

2．スイッチをリブートします。

```
switch# reload
```

スイッチがスタンドアロンモードまたは VCS ファブリックの一部であるかどうかに応じてコンフィグレーションの回復操作は異なります。

スタンドアロンモードでは、すべてのインタフェースがシャットダウンされます。スイッチが再起動後、回復したデフォルト設定が使用されます。次のパラメータは、このコマンドの影響を受けません。

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

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

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

5.7 VCS ファブリックモードでの構成情報管理

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

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

5.7.1 多数のスイッチへの構成情報のダウンロード

1. 一つのスイッチを設定します。
2. 86 ページの『5.4.1 running configuration の格納』に記載されている通り、running configuration を startup configuration へコピーします。
3. コンフィグレーションを外部のホスト(87 ページの『5.5.1 startup configuration の外部ホストへのアップロード』)にアップロードします。
4. それぞれの対象スイッチに構成情報をダウンロードします。詳細な情報は、87 ページの『5.6 コンフィグレーションの回復』を参照下さい。

5.7.2 設定パラメータの自動配布

VCS ファブリックの一部である一つの RBridge において、以下のパラメータを設定した時に、それらが自動的に VCS ファブリック内のすべてのスイッチに配信されます。

- 仮想 IP アドレス

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

6 ファームウェアのインストールと管理

6.1 ファームウェア管理の概要

アップグレードファームウェアは、.plist ファイルに記載されている複数のファームウェアパッケージから構成されます。.plist ファイルには、特定のファームウェア情報(タイムスタンプ、プラットフォームコード、バージョンなど)およびダウンロードされるファームウェアパッケージの名前が含まれています。'firmware download'コマンドは、新しいファームウェアパッケージを現在インストールされているパッケージと比較して、新機能が含まれていたり変更が加えられたパッケージのみをダウンロードします。

Network OS はファームウェアをダウンロードするためにコマンドラインインターフェース(CLI) を備えています。ファームウェアは、ファイル転送プロトコル(FTP)、SSH ファイル転送プロトコル(SFTP)セキュアコピープロトコル(SCP)を使用して、リモートサーバからダウンロードすることができます。リモートサーバからファームウェアをダウンロードする際は、スイッチの管理ポートがリモートサーバに接続されている必要があります。

Network OS v4.1 以降では、ロジカルシャーシクラスターモードにおいて、'logical-chassis firmware download'コマンドを使用して、複数のスイッチのファームウェアをアップグレードすることができます。'logical-chassis firmware download'コマンドは、Principal ノードからのみ実行できます。ファームウェアはファイルサーバから各スイッチの管理ポートを通じてダウンロードされるため、アップグレードを行う全てのスイッチの管理ポートがファイルサーバに接続されている必要があります。同時に複数の'logical-chassis firmware download'コマンドを実行することは出来ません。

ロジカルシャーシクラスターモードにおいて、ファームウェアのアップグレードを実行した後、スイッチのコンフィグレーションはデフォルトに戻ります。コンフィグレーションを保存するために、ファームウェアをダウンロードする前に'copy running-config *filename*'コマンドを使用してコンフィグレーションをバックアップしてください。アップグレードが完了した後に、'copy *filename* running-config'コマンドを使用してコンフィグレーションを復元してください。

ファームウェアのダウンロードが予期しない再起動によって中断された場合、Network OS は以前にインストールされたファームウェアへの復旧を試みます。復旧の成否はファームウェアダウンロードの状況に依存します。もう一度ファームウェアダウンロードを開始する前に、復旧処理が完全に完了するまで待つ必要があります。

6.1.1 ファームウェアの入手と展開

スイッチのファームウェアアップグレードを行うために、FTP サーバにファームウェアパッケージをダウンロードして展開してください。ファームウェアパッケージの展開には、UNIX の'tar'コマンド、'gunzip'コマンド、または Windows の unzip プログラムを使用してください。

ファームウェアパッケージは、ファームウェアバージョンに応じた名前のディレクトリに展開されます。ファームウェアパッケージが保存されたディレクトリへのパスを指定して'firmware download'コ

マンドや'firmware download logical-chassis'コマンドを実行すると、スイッチに関連するパッケージが自動的に検索されます。

6.1.2　ファームウェアのアップグレード

スイッチは、2 つのファームウェアイメージを格納するために、不揮発性記憶領域に 2 つのパーティション(プライマリとセカンダリ)を備えています。以下のステップは、スイッチで'firmware download'コマンド(オプションなし)を入力した後のデフォルトの動作です。

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

アップグレードプロセスは、最初にファームウェアをダウンロードして、その後ファームウェアをコミットします。アップグレードの進行状況を確認するには、'show firmwaredownloadstatus'コマンドを使用してください。

6.1.3　ファームウェアのアップグレードとダウングレード

ファームウェアは、現在スイッチで稼動しているバージョンよりも、より新しいバージョンへアップグレードする場合がほとんどです。しかし、状況によっては以前のバージョンへファームウェアをダウングレードする場合もあります。以下のセクションで説明する手順は、ファームウェアのアップグレードだけでなく、現在のファームウェアバージョンとダウングレードするバージョンに互換性があれば、ダウングレードにも適用できます。
BS500 内蔵 DCB スイッチでは、Network OS v2.0.1_kat4 以前のバージョンにファームウェアをダウングレードできません。また、BS2500 内蔵 DCB スイッチでは、Network OS v.4.0.1_hit1 以前のバージョンにファームウェアをダウングレードすることはできません。

6.2 ローカルスイッチでのファームウェアアップグレード

このセクションではファームウェアアップグレードの概要と操作例を説明します。

6.2.1　ファームウェアダウンロードの準備

ファームウェアをダウンロードする準備のため、このセクションに記載された操作を行ってください。ダウンロードの失敗やタイムアウトが発生した場合は、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。確認方法は 92 ページの『6.2.2 ファームウェアバージョンの確認』を参照してください。

2．ファームウェアパッケージを FTP サーバにダウンロードします。
3．ファームウェアパッケージを展開します。ファームウェアパッケージの展開方法は 90 ページの『6.1.1 ファームウェアの入手と展開』を参照してください。
4．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ます。コンフィグレーションのバックアップ方法は 86 ページの『5.5 コンフィグレーションのバックアップ』を参照してください。
5．補助的に、スイッチと操作端末のコンピュータをシリアルコンソールで接続します。シリアルコンソールにはトラブル時のログなどが出力されます。
6．ファームウェアのダウンロードを実行する前に、現在の core ファイルを採取するため'copy support'コマンドを実行します。この情報は、ファームウェアアップグレード作業中に発生した問題のトラブルシュートに役立ちます。
7．全てのメッセージを消去するために、'clear logging raslog'コマンドを実行します。

6.2.2 ファームウェアバージョンの確認

次の情報を得るために'show version'コマンドを実行します。

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

6.2.3 firmware download コマンドの使用方法

Release Notes に記載された情報に応じて、'firmware download'コマンドに異なるオプションを付加する必要があります。

CAUTION
ファームウェアダウンロ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、保守員による復旧作業が必要となります。

6.2.4 デフォルトモードでのファームウェアダウンロード

通常の環境では、デフォルトモードで'firmware download'コマンドを使用することを推薦します。何もオプションを指定せずに'firmware download'コマンドを実行すると、コマンドはデフォルトモードでファームウェアをスイッチへダウンロードし、スイッチをリブートし、新しいファームウェアをコミットします。
'firmware download'コマンドにオプションを指定する必要がある場合は、下記を参照してください。

- 93 ページの『6.2.5 noactivate オプションを使用したファームウェアダウンロード』

• 93 ページの『6.2.6 manual オプションを使用したファームウェアダウンロード』

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．『6.2.1 ファームウェアダウンロードの準備』に記載した手順を実行してください。
2．FTP または SSH サーバがリモートサーバで動作しており、有効なユーザーID とパスワード情報を取得していることを確認してください。
3．ファームウェアをアップグレードするスイッチに接続してください。
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'コマンドを実行してください。
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'コマンドを使用してください。入力プロンプトが表示された場合は、可能な限りデフォルトに指定された選択肢を選んでください。
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。

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

System sanity check passed.

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

6.2.5　noactivate オプションを使用したファームウェアダウンロード

'firmware download'コマンドに'noactivate'オプションを指定すると、スイッチがリブートすることなく、スイッチへファームウェアをダウンロードすることができます。
新しいファームウェアをダウンロードした後で、'firmware activate'コマンドを実行することでスイッチをリブートさせ、新しいファームウェアを有効化することができます。

CAUTION
新しいファームウェアを有効化するために'reboot'コマンドを実行しないでください。'reboot'コマンドを実行すると以前のファームウェアにリストアされます。

クラスタ環境においては、まず'noactivate'オプションを使用して各スイッチへファームウェアをダウンロードし、次に'firmware activate'コマンドを実行することで任意の順番で新しいファームウェアを有効化することが出来ます。この方法はクラスタ内のスイッチで異なるバージョンのファームウェアが動作する期間を短縮して、クラスタの分断を最小化することができます。

6.2.6　manual オプションを使用したファームウェアダウンロード

以下の手順をスイッチへ適用してください。

1．FTP、SFTP または SSH サーバがホストサーバで動作しており、有効なユーザーID があることを確認してください。
2．FTP、SFTP 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てください。
4．'show version'コマンドを使用して現在のファームウェアバージョンを確認してください。
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'コマンドを使用してください。
6．“Do Auto-Commit after Reboot [y/n]:”プロンプトに対して"n"を入力します。

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

System sanity check passed.

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

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

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

スイッチがリブートして新しいファームウェアで起動します。リブートの際にスイッチとの CLI セッションは自動的に切れます。
7．スイッチのプライマリパーティションが新しいファームウェアとなっているかを確認するため、'show version all-partitions'コマンドを入力します。

6.2.7 manual オプションを使用したファームウェアアップグレード

"manual"オプションを使用することで、ファームウェアダウンロード手順を制御するために、"noreboot"オプションや"nocommit"オプションを指定することが可能となります。

6.2.8 default-config オプションを使用したファームウェアダウンロード

スイッチが新しいファームウェアでリブートする前に、任意に VCS mode、VCS ID、RBridge ID を変更してファームウェアをダウンロードすることが出来ます。

6.2.9 ファームウェアダウンロードセッションの確認

指定したオプションにかかわらず、ファームウェアアップグレードを実行している間、スイッチに別な CLI セッションで接続して'show firmwaredownloadstatus'コマンドを使用することで、ファームウェアアップグレードの進捗状況を確認することができます。
ファームウェアダウンロードが完了した後、'show version all-partitions'コマンドを実行してファーム

ウェアのダウンロードが正常に完了したことを確認できます。

6.3 ファブリッククラスタモードでのファームウェアアップグレード

'firmware download'コマンドは、ローカルスイッチのアップグレードのみサポートしています。VCSファブリック内のすべてのスイッチをアップグレードするには、それぞれのスイッチで'firmware download'コマンドを実行する必要があります。

CAUTION
ファブリック内の各スイッチに対して、現在のスイッチのファームウェアダウンロードを完了させてから別なスイッチのファームウェアダウンロードを開始してください。この手順により、トラフィックの混雑を最小限に抑えることができます。

'show firmwaredownloadstatus'コマンドを入力してダウンロード処理が完了したことを確認してから、次のスイッチでの作業に移ってください。
また、"noactivate"オプションを指定して'firmware download'コマンドを実行することで、スイッチをリブートさせずファームウェアをダウンロードすることができます。クラスタ内の全てのスイッチへファームウェアをダウンロードした後に、各スイッチで'firmware activate'コマンドを実行することで新しいファームウェアを有効化できます。この方法では、クラスタ内のトラフィックの中断を回避するために、各スイッチのリブートの順番を制御することができます。
以下の例では、クラスタに 4 つのスイッチが含まれています。(RBridge ID 1 から 4)スイッチ 1 は Principal スイッチです。この例では、スイッチは特定の順番でリブートする必要があり、まずスイッチ 2 が、続いてスイッチ 3 が、次にスイッチ 4 が、そして最後にスイッチ 1 がリブートします。この操作はいずれかのスイッチから以下の手順でコマンドを実行することで実施できます。

1. 全てのスイッチで'firmware download noactivate'コマンドを実行してください。"noactivate"オプションはスイッチが自動的にリブートするのを回避します。
2. 全てのスイッチに新しいファームウェアがダウンロードされたら、'firmware activate'コマンドを以下の順序で実施してください。

a) firmware activate rbridge-id 2
b) firmware activate rbridge-id 3
c) firmware activate rbridge-id 4
d) firmware activate rbridge-id 1

6.4 ロジカルシャーシクラスタモードでのファームウェアアップグレード

ロジカルシャーシクラスタモードでは、ファブリッククラスタモードと同様に個別のノードにログインして‘firmware download’コマンドを実行することでファームウェアをアップグレードすることが出

来ます。
ロジカルシャーシクラスタモードでのもう一つのアップグレード方法としては、'firmware download'コマンドに"logical-chassis"と"rbridge-id"オプションを指定する方法があります。コマンドの詳細は、コマンドリファレンスの'firmaware download logical-chassis'を参照してください。このコマンドでは、Principal ノードからクラスタ内の複数のノードのファームウェアをアップグレードすることが出来ます。アップグレードするノードは"rbridge-id"オプションで指定されます。
`firmware download logical-chassis'コマンドを実行すると、ファームウェアはコマンドで指定された各ノードへ、各ノードの管理ポートを通じて同時にダウンロードされます。コマンドで指定するノードの数が増えてもダウンロードにかかる時間は変わりません。デフォルトでは、指定した全てのノードのファームウェアダウンロードが完了した後、'firmware download logical-chassis'コマンドは終了します。ノードはリブートしません。
ノードにダウンロードされた新しいファームウェアを有効化するためには、明示的に'firmware download logical-chassis'コマンドを実行する必要があります。この操作で、クラスタ内のノードのリブートを制御できます。新しいファームウェアを自動的に有効化するためには、"auto-activate"オプションを指定してください。

CAUTION
"auto-activate" オプションが指定されると、コマンドで指定された全てのノードが同時にリブートするため、通信が途絶える場合があります。そのため、"auto-activate"オプションの指定は推奨しません。

`firmware download logical-chassis'コマンドを実行している間、'show firmwaredownloadstatus rbridge-id all'コマンドでノードのダウンロードの状況を確認することができます。'logical-chassis firmware download'コマンドの動作を完了したノードの status は"Ready to activate"と表示されます。また、'show version rbridge-id all'コマンドでノードのファームウェアバージョンを確認することができます。
ロジカルシャーシクラスタモードにおける一般的なアップグレード手順は下記の通りです。

1．クラスタ内の全てのノードをアップグレードするために、'firmware download logical-chassis rbridge-id all'コマンドを実行してください。

```
switch# firmware download logical-chassis ftp host 10.10.10.10 user fvt
password buzz directory / file nos4.1.2a rbridge-id all
 Following is the result of the sanity check on the specified nodes.

Rbridge-id    Sanity Result           Current Version
-----------------------------------------------------------------
1             Disruptive              4.1.2a
5             Disruptive              4.1.2a

This command will download firmware to the nodes. Please run "firmware activate" after
the completion of installation.

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

2．ノードのファームウェアダウンロードの状況を確認するために、'show firmwaredownloadstatussummary rbridge-id all'コマンドと'show version rbridge-id all'コマンド

を実行してください。

```
switch# show firmwaredownloadstatus summary bridge-id all
rbridge-id 1
Firmware Download completed. Execute Firmware Activate for Activation.
rbridge-id 5
Firmware Download completed. Execute Firmware Activate for Activation.
switch# show version rbridge-id all
rbridge-id 1
Network Operating System Software
Network Operating System Version: 4.1.2a
Copyright (c) 1995-2014 Brocade Communications Systems, Inc.
Firmware name:      4.1.2a
Build Time:         04:03:59 Sep 27, 2014
Install Time:       22:14:04 Feb  2, 2015
Kernel:             2.6.34.6
BootProm:           2.2.0
Control Processor:  e500v2 with 2048 MB of memory

Appl     Primary/Secondary Versions
----------------------------------------
NOS      4.1.3
         4.1.2a
rbridge-id 5
Network Operating System Software
Network Operating System Version: 4.1.2a
Copyright (c) 1995-2014 Brocade Communications Systems, Inc.
Firmware name:      4.1.2a
Build Time:         19:03:59 Sep 26, 2014
Install Time:       07:01:17 Oct 31, 2014
Kernel:             2.6.34.6
BootProm:           2.2.0
Control Processor:  e500v2 with 2048 MB of memory

Appl     Primary/Secondary Versions
----------------------------------------
NOS      4.1.2a
         4.1.2a
```

3. もしいずれかのノードがダウンロードに失敗したら、ダウンロードに失敗したノードに対してもう一度'firmware download logical-chassis rbridge-id'コマンドを実行して、全てのノードを同じファームウェアレベルにしてください。ノードのセカンダリパーティションに新しいファームウェアが適用されていることを確認してください。
4. 各ノードを任意の順番でアクティベートするために、'firmware activate rbridge-id *rbridge-id*'コマンドを実行してください。

NOTE

'firmware activate'コマンドの"*rbridge-id*" オプションで指定された全てのノードは、同時にリブートします。

```
switch# firmware activate rbridge-id 1-2,3
This command will activate the firmware on the following nodes.
Rbridge-id Sanity Result
-------------------------------------
1 Non-disruptive(ISSU)
2 Disruptive
3 Disruptive
It will cause these nodes to reboot at the same time.
Do you want to continue? [y/n]: y
```

6.4.1　ロジカルシャーシクラスタモードでのファームウェアダウンロードの確認

いずれかのノードのダウンロード失敗や Principal ノードのフェイルオーバーが発生すると、ファームウェアダウンロードは中止されます。'firmware download logical-chassis'コマンドを実行した後、以下の手順でコマンドが正常完了したことを確認してください。

1．'show firmwaredownloadstatus rbridge-id'コマンドを実行して、ノードがダウンロードを完了して"Ready to activation"state になっていることを確認してください。
2．'show version rbridge-id'コマンドを実行して、ノードに正しいファームウェアがダウンロードされていることを確認してください。

もし"Ready for activation"state になっていなかったり、正しいファームウェアがダウンロードされていないノードがある場合は、そのノードに対して新しいファームウェアをアクティベートする前にもう一度'firmware download logical-chassis'コマンドを実行してください。

もしあるノードでファームウェアダウンロードが失敗し続ける場合は、失敗したノードにログインして復旧する必要があります。復旧手順は『6.4 ロジカルシャーシクラスタモードでのファームウェアアップグレード』を参照してください。

7 ライセンスの管理

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

NOTE
ライセンスは、各プラットフォーム別に利用できるものが異なります。各プラットフォームに準備されたライセンスをご使用ください。

表 7-1　Network OS のオプション機能のライセンス一覧

ライセンス	説明
VCS_FABRIC	• VCS ファブリックライセンスは、内蔵 DCB スイッチで２４ノードまでの VCS ファブリックを構成することが出来ます。ファブリック内に３ノード以上ある場合、各ノードに VCS ファブリックライセンスをインストールする必要があります。 • もし、VCS ファブリックが２ノード以内ならば、VCS ファブリックライセンスは必要ありません。 • VCS ファブリックライセンス持つスイッチがライセンス持っていないスイッチに接続することはできません。2 ノードの VCS では、両方のスイッチが VCS ライセンス持つ、あるいは両方のスイッチが VCS ライセンスを持っていない状態でなければなりません。 • Network OS v4.1 からは、本ライセンスをインストールすることなく、３ノード以上の VCS ファブリックを構成することが可能です。
FCOE_BASE	• Fibre Channel over Ethernet 機能を有効にするために、Brocade FCoE ライセンスが必要です。単一のスイッチ上で、このライセンスを使用することができますが、FCoE 機能は、そのノードだけに制限されます。マルチホップ FCoE トラフィックをサポートするためには、VCS ファブリックモードを有効にして、各ノードで Brocade FCoE のライセンスをインストールする必要があります。また、2 ノードを超過する VCS ファブリックの場合、FCoE トラフィックがファブリック内のすべてのノードを横断できるように、FCoE のライセンスに加えて、VCS ファブリックライセンスが必要です。 • FCoE ライセンスがない時、FCoE のログインが許可されません。また、

	FCoE トラフィックも、スイッチを通過しません。FCoE のコマンドが実行された時は、"No FCoE license present"のエラーを表示します。
Port_10G_UPGRADE (10Gb 18 Port Activation License)	• 本スイッチは標準で 10Gb 24 ポート分使用可能です。 • 本ライセンスを適用することで 10Gb を 18 ポート追加で利用可能となります。 • 本ライセンスはオプションライセンスです。追加には個別に購入が必要となります。
PORT_40G_UPGRADE (40Gb 2 Port Activation License)	• 適用することで外部 40Gb(QSFP+ポート)を 2 ポート追加で利用可能となります。 • 本ライセンスはオプションライセンスです。追加には個別に購入が必要となります。

7.1 ライセンスの管理

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

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

7.1.1 スイッチライセンスＩＤの表示

スイッチライセンスＩＤは、スイッチでどのライセンスが有効かを特定します。ライセンスキーを有効化する際、スイッチライセンスＩＤが必要です。
スイッチライセンスＩＤを表示するため、特権実行モードで'show license id'コマンドを入力します。

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

7.1.2 ライセンスキーの取得

ライセンスアップグレードオーダーは、トランザクションキーや Brocade software portal へのリンクを含んだメールにより提供されます。デバイスを指定したライセンスファイルは、software portal でスイッチライセンスＩＤと共にトランザクションキーを入力すると生成されます。スイッチライセンスＩＤを保持するために、'show license id'コマンドをご使用下さい。
ライセンスインストールガイドやメールに書かれた手順に従ってライセンスをインストールしてください。ライセンスキーは、大文字小文字を区別します。エラーを避けるために、ライセンスをインストールする場合は、トランザクションキーをコピー＆ペーストしてください。
インストール手順にそって XML ファイルに含まれたライセンスキーをメールで受け取ることが出来ます。

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

7.1.3　ライセンスのインストール

ライセンスをインストールする際、機能によっては、スイッチのリブートが必要となります。
ライセンスをインストールするために、次手順を実行してください。

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

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

表 7-2　ライセンスのインストール後にアクティブにするための要件

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

(1) VCS ファブリックライセンスの追加

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

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

Adding license [*B r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANF
av5W:gWx3hH2:9RsMv3BHfeCRFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#
]
```

7.1.4　ライセンスの表示

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

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

```
VCS Fabric license
Feature name:VCS_FABRIC
```

7.1.5　ライセンスの削除

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

表 7-3　ライセンスの削除後に非アクティブにするための要件

ライセンス	説明
VCS_FABRIC	ライセンスを削除する前に、'chassis disable'が必要です。
PORT_10G_UPGRADE	ライセンスを削除する前に、オンラインとなっている 10Gb ポートが 24 ポート以下となるよう、不使用ポートをディセーブルにすることが必要です。
PORT_40G_UPGRADE	ライセンスを削除する前に、外部 40Gb の２ポートをディセーブルにすることが必要です。

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

ライセンスを削除するために、次の手順を実行してください。

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

NOTE

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

次の例では、VCS ライセンスの表示および削除を示しています。

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

```
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
    VCS Fabric license
    Feature name:VCS_FABRIC

switch# license remove licStr "VCS_FABRIC"

License Removed [VCS_FABRIC]

For license to take effect, it may be necessary to disable/enable ports or switch...
switch#
```

8 SNMP 管理

8.1 SNMP プロトコル概要

Simple Network Management Protocol (SNMP)は、ネットワークデバイスを監視および管理するための標準的な方法です。ネットワーク内のデバイスは、ＳＮＭＰを使用して、プロトコルデータユニット(PDU)と呼ばれるメッセージを送信します。ＳＮＭＰを使ったネットワーク管理は、以下の３つのコンポーネントを必要とします。

- ＳＮＭＰマネージャ
- ＳＮＭＰエージェント
- ＭＩＢ(Management Information Base)

8.1.1 ＳＮＭＰマネージャ

ＳＮＭＰマネージャは、ＳＮＭＰプロトコルを使ってネットワーク内のデバイスと通信できます。一般的に、ＳＮＭＰマネージャは、ネットワークパートナを監視、必要に応じて管理デバイスのパラメータを設定することによりネットワークを管理するネットワーク管理システム(NMS)です。通常は、ＳＮＭＰマネージャはＳＮＭＰエージェントが動作するデバイスにメッセージを送信し、ＳＮＭＰエージェントはリクエストデータを返信します。幾つかのケースでは、管理デバイスから通信を開始し、Ｔｒａｐと呼ばれる非同期イベントを使ってＳＮＭＰマネージャにデータを送信します。

8.1.2 ＳＮＭＰエージェント

ＳＮＭＰエージェントは、ネットワークの管理デバイスで動作するソフトウェアで、デバイスからデータを収集します。各デバイスは、ＳＮＭＰエージェントを実装しています。ＳＮＭＰエージェントはデータを格納し、ＳＮＭＰマネージャからの要求によりデータを送信します。加えて、エージェントはＴｒａｐと呼ばれる特別なＰＤＵを使って、イベントをＳＮＭＰマネージャに非同期に警告します。

8.1.3 ＭＩＢ(Management Information Base)

管理デバイス上のＳＮＭＰエージェントは、ＭＩＢ(Managed Information Base)と呼ばれるデータベースにデバイスのデータを格納しています。ＭＩＢは、階層化データベースで、RFC 2578 [Structure of Management Information Version 2 (SMIv2)]に規定された規格に基づいて構造化されています。

ＭＩＢは、ネットワーク上のデバイスを管理・監視するためのネットワーク管理システムで使用されるオブジェクトのデータベースです。ＭＩＢは、ＳＮＭＰを使用するネットワーク管理システムにより取り出すことが出来ます。ＭＩＢの構造は、デバイスにより許容される管理アクセスの範囲を決定します。ＳＮＭＰを使って、管理アプリケーションはＭＩＢの範囲内で Read/Write 動作が可能です。

8.1.4　　ＳＮＭＰの基本動作

内蔵 DCB スイッチは、次図に示すように、エージェントとＭＩＢを持ちます。エージェントはデバイスの情報にアクセスし、ＳＮＭＰネットワーク管理装置からアクセスできるようにします。

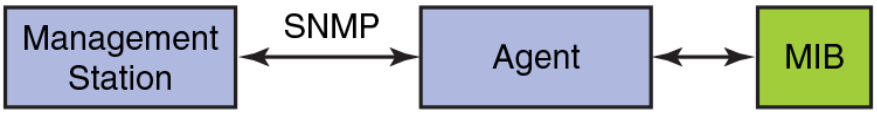

図 8-1　ＳＮＭＰの構造

ＳＮＭＰが有効のとき、管理装置がエージェントに問い合わせる場合、情報を取得(get)，設定(set)出来ます。"get","set","getnext","getresponse"といったＳＮＭＰコマンドは、管理装置から送られます。そして、エージェントは次図に示すように、保持または修正された値を一旦応答します。エージェントは、バイト数とデバイスの内外のパケット数、もしくは、送受信された Broadcast メッセージなどを報告するために変数を使用します。この変数は、管理オブジェクトとして知られています。全ての管理オブジェクトは、ＭＩＢに含まれています。

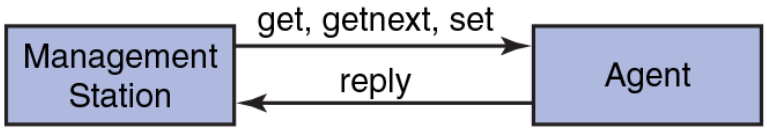

図 8-2　ＳＮＭＰ　Ｇｅｔ/Ｓｅｔ

管理装置は、また、下図に示すように予期しないイベントが発生した場合、スイッチのエージェントからのメッセージを受信することが出来ます。

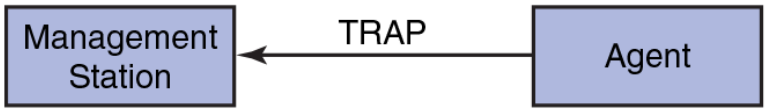

図 8-3　ＳＮＭＰ　Ｔｒａｐ

エージェントは、複数の管理装置からの問合せを受け付けることが出来、最大６つの管理装置に Trap を送信することが出来ます。

NOTE

SNMP オペレーションは、スイッチの CPU パワーを消費します。頻繁なアクセスは、CPU に負荷がかかり、最悪の場合再起動に至る可能性があるため、'show process cpu'コマンドを使用して、CPU 利用率が高騰しないようアクセス頻度に設定してください。特に、'snmpwalk'など連続でアクセスするようなコマンドを事項すると、CPU 利用率は 100%近くになることがありますので、ご使用時は注意してください。

8.1.5　ＭＩＢ(Management Information Base)

ＭＩＢは、デバイス上の監視・管理対象情報のデータベースです。ＭＩＢ構造は、ツリー階層で表現されます。ルートは下記の３つのメインブランチに分岐します。

- International Organization for Standardization (ISO)
- Consultative Committee for International Telegraph and Telephone (CCITT)
- joint ISO/CCITT

これらの分岐は、それらを特定するために短いテキスト文字列と数値(OID)を持っています。テキスト文字列はオブジェクト名を示し、数値はソフトウェがコンパクトでエンコードされた名前表現を生成することを可能としています。

(1) ＭＩＢの構造

各 MIB 変数は、オブジェクト ID(OID)が割り当てられています。OID は、ルートからのパスに沿ったノードの数値ラベルのシーケンスです。例えば、下図に示すように"entity MIB"の OID は下記の通りです。

1.3.6.1.2.1.47

相当する名称は下記の通りです。

iso.org.dod.internet.mgmt.mib-2.entityMIB

その他の分岐は、標準ＭＩＢの一部で、スイッチ上でＳＮＭＰを設定するために関連する部分は、この章の後半で参照されます。

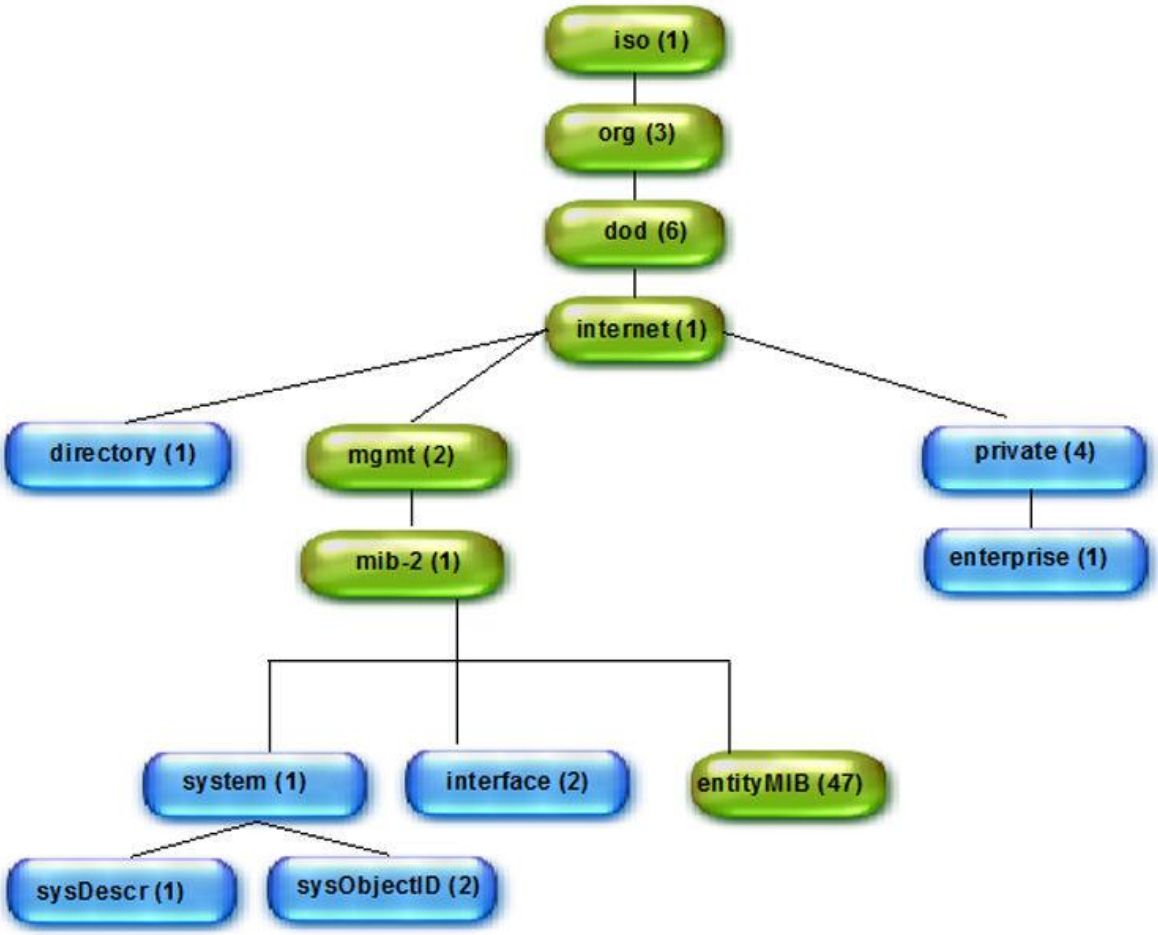

図 8-4　ＭＩＢ　Ｔｒｅｅ

(2)　ＭＩＢ変数へのアクセス

ＭＩＢ変数にアクセスするために、ＭＩＢブラウザが使用できます。

Once loaded, MAX-ACCESS provides access levels between the agent and management station.次表は、アクセスレベルを示します。

表 8-1　ＭＩＢアクセスレベル

アクセスレベル	説　明
not accessible	この変数に対して読み書きできません
read create	表形式のオブジェクトの読み出し、または、修正、または、新しい行として追加が可能です
read only - Public	情報の監視のみ可能です
read-write - Private	読み出し、修正が可能です
accessible-to-notify	Trap を通じてのみ情報の読み出しが可能です

(3) プライベートＭＩＢ

プライベートＭＩＢは、インターネット標準の MIB-II に対して、プライベートに拡張した変数の集合です。プライベートＭＩＢファイルを下記に示します。

- BRCD_NOS_PRODUCTS.mib
- BROCADE-PRODUCTS-MIB.mib
- BROCADE-REG-MIB.mib
- BRCD_TC.mib
- SWBase.mib
- Resource.mib
- System.mib
- FA.mib
- HA.mib
- FOUNDRY-SN-NOTIFICATION.mib

(4) ＭＩＢのロード順序

多くのＭＩＢは、他のＭＩＢで定義された定義を使っています。これらの定義は、ＭＩＢの先頭付近にある"IMPORTS"セクションにリストされています。ＭＩＢをロードする際は、依存関係のあるＭＩＢが正しい順番でロードされることを保証するため、次の表を参照してください。表記載の順序は、ロードすれば正しくロードされる一例を示しています。具体的には、表を例とすると、まず『依存先』に記載されたＭＩＢをロードした後または既にロード済みか確認した後、『ＭＩＢファイル名称』に記載されたプライベートＭＩＢファイルを表の上から順にロードすることで正常にロードすることが出来ます。依存関係を守っていれば、表の順番通りにロードする必要はありません。

NOTE

ＭＩＢファイルをロードする前に、Network OS に対して正しい SNMP バージョンを設定していることを確認してください。Network OS は、SNMPv1,SNMPv2c,SNMPv3 をサポートしています。SNMPv2c の inform request は未サポートです。

表 8-2　プライベートＭＩＢ依存関係

ＭＩＢファイル名称	依存先(事前ロード要)
Brocade-REG-MIB.mib	RFC1155-SMI
Brocade-TC.mib	Brocade-REG-MIB, SNMPv2-TC, SNMPv2-SMI
BRCD_NOS_PRODUCTS.mib	SNMPv2-SMI, Brocade-REG-MIB
BROCADE-PRODUCTS-MIB.mib	SNMPv2-SMI, Brocade-REG-MIB
SWBase.mib	SNMPv2-TC, SNMPv2-SMI, Brocade-REG-MIB
Resource.mib	SNMPv2-TC, SNMPv2-SMI, SWBASE-MIB
System.mib	SNMPv2-TC, Brocade-TC, SWBASE-MIB
FA.mib	RFC1155-SMI, RFC-1212, RFC1213-MIB RFC-1215
HA-mib	SNMPv2-SMI, Brocade-REG-MIB, SW-MIB ENTITY-MIB, SNMPv2-TC
FOUNDRY-SN-NOTIFICATION.mib	SNMPv2-SMI, FOUNDRY-SN-ROOT-MIB IF-MIB, DOT3-OAM-MIB FOUNDRY-SN-SWITCH-GROUP-MIB FOUNDRY-SN-AGENT-MIB FOUNDRY-SN-SWITCH-GROUP-MIB FOUNDRY-SN-SW-L4-SWITCH-GROUP-MIB FOUNDRY-SN-WIRELESS-GROUP-MIB FOUNDRY-SN-OSPF-GROUP-MIB IEEE8021-CFM-MIB

8.2 ＳＮＭＰの設定

8.3 SNMP コミュニティ設定

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

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

次のコミュニティは、read-write 権限です。

- "Secret Code"
- "OrigEquipMfr"

- “private”

次のコミュニティは、read-only です。

- “public”
- “common”
- “ConvergedNetwork”

8.3.1 SNMP コミュニティの追加

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

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

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

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

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

8.3.2 read-only コミュニティのアクセス権の変更

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

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

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

8.3.3 SNMP コミュニティの削除

次の例は、コミュニティ“private”を削除します。

1．'configure terminal'コマンドを入力します。
2．'no snmp-server community string [ro | rw]'を入力します。以下は例です。

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

8.3.4 SNMP コミュニティの表示

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

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

8.4 SNMP サーバ

'snmp-server host'コマンドは、SNMP version 1 / 2c の Trap の送信先 IP アドレス、SNMP バージョン、コミュニティと SNMP サーバのポートを設定します。
コミュニティに関連する SNMP トラップホストを設定するため、ホストを設定する前に、'snmp-server community'コマンドを使って、コミュニティを作成します。
エージェントは、６つのコミュニティとコミュニティに関連づけられた trap recipient と trap recipient の重要度をサポートしています。各コミュニティのトラップ受信のデフォルト値は 0.0.0.0 です。コミュニティ名の長さは、2 から 16 文字です。各コミュニティデフォルト値は、以下の通りです。

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

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

8.4.1 SNMP サーバホストの設定

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

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

次の例は、read-only ユーザーとして、コミュニティ：commaccess を設定し、SNMP version 2c の trap recipient として 10.32.147.6 / ターゲットポート 162 を設定します。

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

8.4.2 SNMP サーバホストの削除

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

8.4.3 SNMP システムグループの設定

SNMP システムグループのシステム連絡先及びロケーションオブジェクトを設定します。

(1) サーバの連絡先の設定

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

1．'configure terminal'コマンドを入力します。
2．'snmp-server contact string'を入力します。
次の例は、デフォルトの連絡先を"Operator 12345"に設定します。テキストにスペースを含む場合は、ダブルクォーテーションで囲みます。

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

(2) サーバの連絡先の削除

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

(3) サーバロケーションの設定

サーバのロケーション情報を設定するには、'snmp-server location'コマンドを使用します。デフォルトのサーバのロケーション情報は、 "End User Premise"です。

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

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

(4) サーバの説明情報の設定

サーバの説明情報を設定するには、'snmp-server sys-descr'コマンドを使用します。デフォルトの説明情報は、"Brocade-VDX-VCS <vcsid>"となっています。使用可能な文字数は、4～255 文字です。

1．'configure terminal'コマンドを入力します。
2．'snmp-server sys-descr'コマンドを入力します。次の例は、デフォルト値を "Brocade-VDX Test Bed" 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 sys-descr "Brocade-VDX Test Bed"
```

3．説明情報を削除するには、'no snmp-server sys-descr'を入力します。

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

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

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

9 ファブリック管理

9.1 TRILL

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

9.2 VCS ファブリックの形成

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

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

次のイベントシーケンスは、VCS ファイブリックの構成手順を示しています。

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

NOTE
もしソフトウェアが"VCS enable"に設定されていなかった場合、スイッチはスタンドアロンモードに移行し、通常の 802.1x イーサネットスイッチとして動作します。

- スイッチで VCS ファブリック有効な状態と判断されると、スイッチソフトウェアは一連の手順を実行します。
  - Brocade Link Discovery Process (BLDP)により、VCS ファブリックが利用可能なスイッチがエッジポートと接続されているかを検出しようとします。更に詳細は、116 ページの『9.2.2 隣接デバイスの検出』を参照下さい。
  - BLDP はリンク状態にある VCS ファブリック環境に隣接のスイッチを組み込もうとします。
- 一連の Fibre Channel fabric formation protocols (RDI, DIA, and FSPF)の手順が実行され、２つの隣接スイッチ間でリンクレベルの関係が構築されます。更に詳細は、116 ページの『9.2.4 ファブリックの形成』を参照下さい。
- マージと結合プロトコルにより、クラスタユニット間のコンフィグレーションがマージされ、ファブリックが形成されます。

9.2.1 RBridge の動作

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

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

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

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

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

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

RBridge は、コーディネータスイッチから特定の RBridge ID をリクエストします。もし、コーディネータスイッチが、この RBridge ID が既に使われていることを検出した場合、次の未使用の RBridge ID を応答します。リクエストした RBridge は、別の RBridge ID を使用することは許されず、ファブリックから自ら分離します。このケースでは、ISL を起動することは出来ません。ISL は、明示的に無効化

された後、重複した RBridge ID を持つ RBridge を取り除くために再度有効化される必要があります。

9.2.2 隣接デバイスの検出

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

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

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

9.2.3 Brocade トランク

Network OS v3.0.0 以降は、ハードウェアベースのリンクアグリゲーショングループ、または LAG などの Brocade トランクをサポートしています。これらの LAG は動的に 2 つの隣接スイッチとの間に形成されます。トランクの形成は FC スイッチ上のトランクの形成を制御するのと同じ FC のトランキングプロトコルによって制御されるので、有効化または無効化を除いてユーザーの介入や設定は必要ありません。設定は、グローバルレベルもしくはインタフェースレベルでトランクを形成するようスイッチのソフトウェアに指示します。手順については、120 ページの『9.4.3 ファブリックトランクの有効化』を参照してください。

NOTE

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

9.2.4 ファブリックの形成

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

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

(1) Principal スイッチの選択

すべての VCS ファブリックが有効なスイッチは、ブートアップ時やファブリックポートを形成した後、それ自体が Principal スイッチであることを宣言し、すべてのファブリックポートでは、このインテントを広告します。インテントには、優先順位とそのスイッチの WWN が含まれています。すべてのスイッチが同時に起動した場合は、デフォルトの優先順位は同じで、すべてのスイッチが、それらの相

互のインテントを比較します。この比較で最も低い WWN を持つスイッチが Principal スイッチになります。WWN は、業界標準のスイッチに割当てられた識別子で、８バイトであることを除いて、MAC と似ています。Principal スイッチの役割は、ファブリックに参加した新しい RBridge が、ファブリックに既に存在するどの RBridge ID とも重複しないことを判断することです。

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

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

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

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

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

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

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

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

9.3 VCS ファブリックの構成管理

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

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

スイッチは、競合があるとファブリックに参加できません。例えば、同じ RBridge ID をもった別のスイッチが存在しファブリック上で動作中である場合です。この場合、同じ CLI 操作で使って新しい RBridge ID を選択してください。
一旦、ファブリックプロトコルにより ID が割当てられると、これらの ID は数値として RBridge ID と等しく、その後は RBridge ID として取り扱われます。
VCS ID や RBridge ID のような VCS ファブリックパラメータを設定したり、VCS ファブリックモードを有効にするため、'vcs'コマンドを使用します。VCS ファブリックパラメータの設定と VCS ファブリックモードの有効化は、同時にも別々にも行うことは可能です。詳細については、表 9-1，表 9-2，表 9-3 を参照してください。
VCS ファブリックの設定を変更後、スイッチは変更を適用し、リブートします。
スイッチの無効化状態は、リブート後まで保持されません。もし、リブート前に無効化されていた場合は、ブートが完了した後、有効化状態で復帰します。

9.3.1 VCS ファブリック設定作業

表 9-1，表 9-2，表 9-3 に VCS ファブリック環境をセットアップするコマンド例を示します。

表 9-1　ロジカルシャーシクラスタモードを有効化するコマンド例

VCS ファブリック設定作業	VCS ファブリックコマンド例
VCS ID をデフォルトの 1、RBridge ID は変更せずロジカルシャーシクラスタモードを有効にする	switch# vcs logical-chassis enable
VCS ID を 225、RBridge ID を 15 に変更しロジカルシャーシクラスタモードを有効にする	switch# vcs vcsid 22 rbridge-id 15 logical-chassis enable
VCS ID を 11 に変更し、RBridge ID は変更せずロジカルシャーシクラスタモードを有効にする	switch# vcs vcsid 11 logical-chassis enable
VCS ID はデフォルトの 1、RBridge ID を 6 としてロジカルシャーシクラスタモードを有効にする	switch# vcs rbridge-id 6 logical-chassis enable

表 9-2　ファブリッククラスタモードを有効化するコマンド例

VCS ファブリック設定作業	VCS ファブリックコマンド例
VCS ID をデフォルトの 1、RBridge ID は変更せずファブリッククラスタモードを有効にする	switch# vcs enable
VCS ID を 55、RBridge ID を 19 に変更しファブリッククラスタモードを有効にする	switch# vcs vcsid 55 rbridge-id 19 enable
VCS ID を 73 に変更し、RBridge ID は変更せずファブリッククラスタモードを有効にする	switch# vcs vcsid 73 enable
VCS ID はデフォルトの 1、RBridge ID を 10 としてファブリッククラスタモードを有効にする	switch# vcs rbridge-id 10 enable

表 9-3　いずれかの VCS モードが既に有効になっている場合のコマンド例

VCS ファブリック設定作業	VCS ファブリックコマンド例
VCS ID を 44 に RBridge ID を 22 変更する	switch# vcs vcsid 44 rbridge-id 22
VCS ID を 34 に変更する	switch# vcs vcsid 34

9.4 ファブリックインタフェースの構成管理

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

9.4.1　ファブリック ISL の有効化

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

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

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

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

9.4.2　ファブリック ISL の無効化

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

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

9.4.3　ファブリックトランクの有効化

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

9.4.4　ファブリックトランクの無効化

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

9.4.5　ブロードキャスト、未学習ユニキャスト、マルチキャスト転送

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

(1) マルチキャスト分配ツリールートの選択

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

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

9.4.6　プライオリティ

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

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

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

(1) プライオリティの変更

1．スイッチに接続し、管理者権限のアカウントでログインします。

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

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

9.4.7　running configuration の表示

'show running-config fabric route mcast'コマンドは、ファブリックルートマルチキャストの構成情報を表示します。スイッチで有効な現在のコンフィグレーションは、running configuration として参照され

ます。スイッチがオンラインの間にコンフィグレーションに行われた全ての変更は、 running configuration に行われます。running configuration は、恒久的ではありません。

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

1．スイッチに接続し、管理者権限のアカウントでログインします。
2．'show running-config fabric route mcast priority'コマンドを入力します。

```
switch# show running-config fabric route mcast rbridge-id 1 priority
fabric route mcast rbridge-id 1
 priority 10
```

- VCS 仮想 IP アドレスの設定

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

```
switch(config)# vcs virtual ip address 10.0.0.23/24
```

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

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

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

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

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

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

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

(1) 仮想 IP アドレスの構成シナリオ
クラスタ内の Principal スイッチには、仮想ＩＰアドレスが割り当てられます。その場合の構成シナリオを表 9-4 に示します。

表 9-4　構成のシナリオ

シナリオ	概要
最初のクラスタ形成	クラスタが最初に形成されている時と仮想 IP アドレスが既に設定されている場合、Principal スイッチは、仮想 IP アドレスが割り当てられています。もし、仮想 IP アドレス設定が存在しないならば、Principal スイッチは、管理ポートの IP アドレスを使用してアクセスすることができます。
仮想 IP の設定	最初にクラスタの仮想 IP アドレスを設定すると、仮想 IP アドレスが Principal スイッチの管理インタフェースにバインドされます。
Principal スイッチのフェイルオーバー	仮想 IP アドレスが管理インタフェースに割り当てられている間に Principal スイッチがセカンダリスイッチになった場合、仮想 IP アドレスは新しい Principal スイッチに再割り当てされます。
Principal スイッチのダウン	クラスタ内の Principal スイッチがダウンした場合、仮想 IP アドレスは、その管理インタフェースから解放されます。仮想 IP アドレスは、Principal スイッチになる次のスイッチに割り当てられます。
Principal スイッチのシャーシ無効化	Principal スイッチで'chassis disable'コマンドが実行されると、仮想 IP アドレスは、その管理インタフェースから解放されます。仮想 IP アドレスは、Principal スイッチになる次のスイッチに割り当てられます。
仮想 IP の削除	コンフィグレーションから仮想 IP アドレスを削除する場合は、仮想 IP アドレスが Principal スイッチの管理インタフェースからアンバインドされます。この場合、Principal スイッチは引き続き管理ポートの IP アドレスを使用してアクセスできます。
些細なマージ	2 つのクラスタが一緒にマージした場合には、より小さい(クラスタ A)のグローバル· コンフィグレーションは、大規模なクラスタ(クラスタ B)で上書きされます。この時間に、仮想 IP アドレスは、クラ

	スタ A の Principal スイッチからアンバインドされます。クラスタ B の仮想 IP アドレスは、新しいマージされたクラスタの Principal スイッチにアクセスするために使用できます。クラスタ B の仮想 IP アドレスが設定されていない場合は、マージされたクラスタに仮想 IP アドレスが設定されません。
クラスタのリブート	クラスタを再起動すると、仮想 IP アドレスは、永続的で、新しい Principal スイッチにバインドされます。
クラスタの単独運転	ISL のリンクが形成している 2 つ以上のクラスタ間でダウンした場合、元のクラスタ内の Principal スイッチは、仮想 IP アドレスを保持します。第２クラスタ内の新しい Principal スイッチは、仮想 IP アドレスが使用中でないことを確認するためにチェックを実行します。使用中である場合、アドレスがスイッチに割り当てられないと意味するエラーが RASlog に記録されます。
スタンドアロンノードの動作	仮想 IP アドレスは、VCS モードでのスタンドアロンノード上に構成することができません。
仮想 MAC アドレス	仮想 MAC アドレスは、仮想 IP アドレスでサポートされません。
管理ポートのプライマリ IPv4 アドレス	仮想 IP アドレスが正常に機能するためには、管理ポートの IPv4 アドレスが割り当てられ、機能する必要があります。

9.4.8　ファブリックの ECMP 負荷分散

ECMP パスのトラフィックは、Vlan ID、MAC DA/SA、L3_ULP、L3 DA/SA、および、L4 Dst/Src の 8 つのフィールドをキーに負荷分散されます。ストリームのいくつかのパターンでは、トラフィックの大部分は一つの ECMP パスにながれこみ、ECMP パスの残りの部分は十分に活用されません。この結果、トラフィックを分散させるために利用可能な ECMP パスが複数あっても、データトラフィックの損失となります。'fabric ecmp load-balance'コマンドを使用して、ファブリック内の ECMP パスの選択方法を設定することができます。このコマンドのオペランドを表 9-5 のリストに示します。

表 9-5　VCS ファブリック設定作業の例

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

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

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

1．RBridgeID コンフィグレーションモードに遷移します。

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

2．'fabric ecmp load-balance'コマンドを実行します。
以下の例では、宛先 MAC アドレスと VID ベースの負荷分散を設定します。

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

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

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

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

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

9.5 VCS ファブリック上での操作

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

表 9-6　VCS ファブリック上での操作

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

NOTE

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

10 Network OS システムモニタ

10.1　システムモニタの概要

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

10.1.1　スイッチヘルス監視

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

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

10.1.2　ハードウェアプラットフォームのデフォルト閾値の設定

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

表 10-1　ハードウェアプラットフォームのデフォルト設定

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

10.1.3　システム設定の閾値

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

NOTE

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

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

2．ダウンの閾値および限界の閾値を設定するには、次のコマンドを入力します。

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

・temp は、温度センサ用の閾値設定を構成します。
・compact-flash はコンパクトフラッシュコンポーネントの閾値を設定します。

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

10.1.4　スイッチヘルスステータスの表示

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

```
switch# show system monitor
```

10.1.5　システムモニタ構成の表示

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

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

10.2　リソース監視

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

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

フォルトは、50 パーセントです。

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

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

表 10-2　CPU およびメモリの閾値の工場出荷時のデフォルト

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

10.2.1　メモリ監視の設定

NOTE
電子メールは、閾値監視のアクションとしてサポートされていません。

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

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

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

システムモニタがアクションをトリガする前に取るリトライ回数(0-100)。

10.2.2　CPU 監視の設定

NOTE
電子メールは、閾値監視のアクションとしてサポートされていません。

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

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

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

10.2.3　閾値監視設定の表示

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

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

10.3　セキュリティ監視

NOTE
電子メールは、閾値監視のアクションとしてサポートされていません。

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

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

セキュリティ監視における、閾値などの監視条件は変更できません。

10.4　インタフェース監視

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

11 ユーザーアカウントの管理

11.1 ユーザーアカウント

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

11.1.1 ローカルスイッチユーザーデータベースのデフォルトアカウント

デフォルトのアカウントとして、工場出荷時 2 つのユーザーアカウントを定義しています。各スイッチの初期インストールおよび設定時にすべてのデフォルトアカウントのパスワードを変更することをお勧めします。
デフォルトユーザーアカウントは "admin"と"user"で、これらのアカウントは、スイッチのローカルユーザデータベース内の"admin"と"user"のロールに関連付けられています。"admin"と "user"のユーザーのみが CLI にアクセスすることができ、アカウントのパスワードを除いて、デフォルトユーザー("admin"と"user")のその他の属性を変更することはできません。
デフォルトでは、すべてのアカウント情報は、スイッチのローカルユーザーデータベースに保管されています。スイッチへのログインユーザーの認証と追跡は、デフォルトでローカルです。

NOTE
デフォルトアカウントを含むユーザーアカウントの最大数は、64 です。デフォルトロールを含むロールの最大数は、64 です。スイッチ毎にサポートされるアクティブな telnet または CLI セッションの最大数は 32 です。

11.1.2 ユーザーアカウントの作成と変更

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

表 11-1　ユーザーアカウントの属性

パラメータ	説明
Name	ユーザー名です。ユーザー名は大文字小文字を識別し、英字で始まり 40 文字以内でなければなりません。使用できる文字は、英字、数字、アンダースコア(_)、ピリオド(.)です。指定されたユーザー名が既に存在する場合は、'username'コマンドは、既存のロールを変更します。
role	ユーザーに割り当てられているロールは、アカウントの RBAC のアクセス権限を定義します。
password	アカウントパスワードは、すべての現在適用中のパスワード規則を満たさなければなりません。詳細については、143 ページの『11.4 パスワードポリシー』を参照してください。
encryption-level	パスワードの暗号化レベル。パスワードを暗号化(7)か、クリアテキスト(0)を選択できます。暗号化レベルを指定しない場合、クリアテキスト(0)がデフォルト設定です。
desc	アカウントのディスクリプション。ディスクリプションは、最長 64 文字まで指定でき、シングルクォテーション(')、ダブルクォーテーション(")、エクスクラメーション(!)、コロン(:)、セミコンマ(;)文字を除く、出力可能な任意の ASCII 文字を含めることができます。 ディスクリプションに空白が含まれている場合、ダブルクォテーション(")でテキストを囲む必要があります。
enable true | false	アカウントが有効か無効かを示します。アカウントが無効にされているユーザーはログインできません。デフォルトのアカウント状態は有効になっています。

11.1.3　ユーザーアカウントの作成

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

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

2．指定されたパラメータで'username'コマンドを入力します。

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

11.1.4　ユーザーアカウント情報の表示

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

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

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

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

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

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

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

11.1.5　既存ユーザーアカウントの変更

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

次の例では、以前に作成した "brcdUser"アカウントにディスクリプションを追加します。

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

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

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

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

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

11.1.6　ユーザーアカウントの無効化

enable パラメータに"false"を設定することにより、ユーザーアカウントを無効化することができます。ユーザーアカウントが無効化された時、無効化されたユーザーのすべてのアクティブなログインセッションが終了します。

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

2．指定されたパラメータで'username'コマンドを入力します。

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

11.1.7　ユーザーアカウントの削除

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

2．'no username'コマンドを入力します。

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

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

11.1.8　ユーザーアカウントのロック解除

ログインリトライの閾値に達すると、ユーザーアカウントはシステムによって自動的にロックされます。アカウントのロックアウトの閾値は、設定可能なパラメータです。詳細については、144 ページの 『11.4.3 アカウントロックアウトポリシー』を参照してください。

NOTE

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

1．現在アクティブなセッションとロックアウトしたユーザーを表示するには、特権実行モードで'show users'コマンドを入力します。

2．ロックされたユーザーアカウントのロックを解除するには、特権実行モードで'unlock username'のコマンドを入力します。

3．ユーザーがロック解除されたことを確認します。'show users'コマンドは、ロックされていないユーザーを表示します。

```
switch# show users
**USER SESSIONS**
RBridge
ID  Username    Host Ip         Device Time Logged In
2   user        10.70.4.105     vty/0  2012-04-30 01:59:35
1   user        10.70.4.105     vty/0  2012-04-30 01:57:41
1   admin       10.70.4.105     vty/2  2012-04-30 01:58:41
1   user        10.70.4.105     vty/3  2012-09-30 02:04:42
**LOCKED USERS**
RBridge
ID      username
1       testUser
switch# unlock username testUser
Result: Unlocking the user account is successful
switch# show users
**USER SESSIONS**
RBridge
ID  Username    Host Ip         Device Time Logged In
2   user        10.70.4.105     vty/0  2012-04-30 01:59:35
1   user        10.70.4.105     vty/0  2012-04-30 01:57:41
1   admin       10.70.4.105     vty/2  2012-04-30 01:58:41
1   user        10.70.4.105     vty/3  2012-09-30 02:04:42
```

```
**LOCKED USERS**
RBridge
ID      username
no locked users
```

11.2　ロールベースアクセス制御

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

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

11.2.1　デフォルトロール

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

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

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

11.2.2　ユーザー定義ロール

デフォルトロールに加えて、Network OS は、ユーザー定義のロール作成をサポートします。ユーザー定義ロールは、特別なルールを追加することによって、洗練された特権の基本セットから始まります。ロールを作成したら、ロールに名前を割り当て、一つ以上のユーザーアカウントへのロールを関連付けることができます。以下のツールは、ユーザー定義されたロールを管理するために利用できます。

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

11.2.3　ユーザー定義ロールの作成

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

表 11-2　ロールの属性

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

ロール作成は、以下の条件のもと実行する必要があります。

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

11.2.4　ロールの作成または変更

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

2．パラメータを指定して、'role'コマンドを入力します。

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

11.2.5　ロールの表示

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

```
switch# show running-config role

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

11.2.6　ロールの削除

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

2．パラメータを指定して'no role'コマンドを入力します。

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

11.3　コマンドアクセスルール

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

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

・ルールのインデックス番号

・ルールを適用するロール

・ルールによって定義されたコマンド

表 11-3 は、ルールの属性の詳細を説明します。

表 11-3　ルールの属性

パラメータ	説明
index	1～512 の範囲内のルールの識別子。
role	ルールが定義されているロール名。
command	アクセスが定義されているコマンド。
operation	オプション。ルールによって付与された一般的なアクセスモードを定義します。アクセスは、読み取り専用(read-only)または読み書き(read-write)にすることができます。デフォルト値は、"read-write "です。
action	オプション。一般的なアクセスモードを制限している修飾子。指定されたアクセスは受け入れる(accept)か、拒絶されます(reject)。デフォルト値は、"reject"です。

11.3.1　複数オプションで指定するコマンド

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

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

NOTE

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

11.3.2　コンフィグレーションコマンドのルール

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

次のルールは、コンフィグレーションコマンドを規定します。

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

11.3.3　運用コマンドのためのルール

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

次のルールは運用コマンドを規定します。

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

11.3.4　インタフェース関連コマンドのためのルール

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

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

次のルールはインタフェース関連コマンドを規定します。

- ロールに、read-write 権限とインタフェースの特定のインスタンスに対する accept action を持つル

ールが関連付けられてある場合、このロールに関連付けられているユーザーは、その属性を変更することができます。

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

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

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

- ロールに、read-only または read-write 権限とインタフェースまたはインタフェースのインスタンスの reject action を持つルールが関連付けられてある場合、このロールに関連付けられているユーザーは、これらのインタフェースまたはインタフェースのインスタンスに関連する clear / show 操作ができません。clear / show 操作をするには、ユーザーのロールは、少なくとも read-only 権限と accept 許可を持たなければなりません。デフォルトでは、すべてのロールは、すべてのインタフェースのために read-only 権限と accept 権限を持っています。

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

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

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

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

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

- インタフェース tengigabitethernet インスタンスのサブモードで'no vlan'および、'no spanning-tree'コマンドを実行するには、ユーザーが'vlan'および'protocol spanning-tree'コマンドの read-write 権限および accept 許可を持つ必要があります。ユーザーが、少なくとも一つのインタフェースに対する read-write 権限および、'vlan'、'spanning-tree'コマンドへの accept 許可を持つならば、ユーザーが持っているデフォルトの許可(read-only 権限、accept 許可)でその他のインタフェースインスタン

スに対して'no vlan'および、'no spanning-tree'の操作を実行できます。

11.3.5　プレースホルダルールの設定

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

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

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

11.3.6　ルールの処理

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

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

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

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

11.3.7　ルールの追加

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

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

1．特権実行モードで、'configure terminal'コマンドを入力してグローバルコンフィグレーションモードに入ります。
2. グローバルコンフィグレーションモードへの read-write アクセスを指定するルールを作成します。

3．'username'コマンドへの read-write アクセスを指定する 2 番目のルールを作成します。指定されたパラメータを使用して、'rule'コマンドを入力します。

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

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

```
switch login: SecAdminUser
Password:******
Welcome to the ConfD CLI
SecAdminUser connected from 127.0.0.1 using console on switch

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

11.3.8　ルールの変更

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

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

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

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

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

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

11.3.9　ルールの削除

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

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

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# no rule 155
```

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

11.3.10 ルールの表示

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

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

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

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

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

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

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

11.3.11 コンフィグレーション例

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

(1) VCS ファブリックセキュリティ管理者アカウントの設定

1．VCS ファブリックセキュリティ管理者のロールを作成します。

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

2．新しく作成されたロールに関連付けるユーザーアカウントを作成します。

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

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

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

SecAdminUser アカウントは、'configuration-level'コマンドのロール、ルール、ユーザー名、AAA、および radius-server への運用アクセスを付与されています。NetworkSecurityAdmin ロールに関連付けられたすべてのアカウントは、ユーザーアカウントの作成および、変更することができ、ロールを管理

してルールを定義することができます。また、ロールは RADIUS サーバを設定可能にし、ログインシーケンスを設定します。

11.4　パスワードポリシー

パスワードポリシーは、グローバルな規制をすべての新しいパスワードに付与することにより、パスワードをより安全にするルールのセットを定義して、実施します。このセクションで説明するパスワードポリシーは、スイッチのローカルユーザーデータベースに適用されます。以下に、設定可能なパスワードポリシーのリストを示します。

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

11.4.1　パスワード強度ポリシー

表 11-4 に設定可能なパスワードポリシーのパラメータを示します。

表 11-4　パスワードポリシーのパラメータ

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

11.4.2　パスワード暗号化ポリシー

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

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

```
switch(config)# service password-encryption
switch(config)# do show running-config service password-encryption
service password-encryption
switch(config)# username testuser role testrole desc "Test User"
encryption-level 0 password hellothere
switch(config)# do show running-config username
username admin password "BwrsDbB+tABWGWpINOVKoQ==¥n" encryptionlevel
7 role admin desc Administrator
username testuser password "cONW1RQ0nTV9Az42/9uCQg==¥n"
encryption-level 7 role testrole desc "Test User"
username user password "BwrsDbB+tABWGWpINOVKoQ==¥n" encryptionlevel
7 role user desc User
```

- パスワード暗号化サービスを無効化すると、クリアテキストに加えられる新しいパスワードでもスイッチ上でクリアテキストとして保存されます。既存の暗号化されたパスワードは暗号化されたままです。
  次の例では、パスワードの暗号化が無効になった後で、testuser のアカウントのパスワードがクリアテキストで保存されています。デフォルトのアカウント、"user"と admin"は暗号化されたままです。

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

11.4.3　アカウントロックアウトポリシー

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

否されます。
明示的に管理アクションでアカウントのロックを解除するまで、アカウントはロックされたままです。ユーザーアカウントを手動でロックすることはできません。ロックされていないアカウントのロックを解除することはできません。
失敗したログイン試行は、ローカルスイッチ上でのみ追跡されます。VCS モードでは、ユーザーアカウントはロックアウトが発生したスイッチだけでロックされ、同じユーザーで、VCS ファブリック内の別のスイッチにログインすることはできます。
アカウントロックアウトポリシーは、admin ロールを持つ root アカウント以外のすべてのユーザーアカウントに適用されます。

11.4.4　サービス妨害の拒否

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

11.4.5　アカウントロックアウト閾値の設定

'password-attributes max-retry maxretry'コマンドでロックアウト閾値を設定することができます。maxretry の値は、ユーザーのアカウントがロックされる前に、誤ったパスワードでログインを試みることができる回数を指定します。失敗ログイン試行回数は、直前のログイン成功からカウントされます。maxretry は 0～16 の値に設定することができます。値が 0 の場合、ロックアウトメカニズムを無効にします(デフォルト)。
次の例では、ロックアウトの閾値を 5 に設定します。

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

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

ユーザーアカウントがロックされている場合、それは 134 ページの『11.1.7 ユーザーアカウントのロック解除』で説明する手順を使用してロックを解除することができます。

11.4.6　パスワードポリシーの管理

既存のパスワードポリシーを定義または変更するために指定されたパラメータで、

'password-attributes'コマンドを使用します。

(1) パスワードポリシーの作成

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

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

2．指定したパラメータで、'password-attributes'コマンドを入力します。

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

(2) デフォルトパスワードポリシーの復元

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

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

2．指定したパラメータで、'password-attributes'コマンドを入力します。

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

(3) パスワード属性の表示

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

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

```
switch# show running-config password-attributes
% No entries found.
```

11.5　セキュリティイベントのロギング

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

12 エッジループ検出の管理

12.1 エッジループ検出の概要

Edge-loop detection(ELD)は、ブロードキャストストームの原因となるレイヤ 2 ループを検出して無効にします。通常、これらのループは設定ミスによって引き起こされます。
ELD は、VCS ファブリッククラスタにて設定でき使用でき、二つ以上の VCS ファブリッククラスタを含む任意のトポロジで、ELD を利用できます。スタンドアロンスイッチも、クラスタに含めることができますが、ループの検出は、VCS ファブリッククラスタ上で働き、スタンドアロンスイッチ上で動作するわけではありません。スタンドアロンスイッチで構成されるネットワークでは、ELD を使用することができません。

具体的には、次のトポロジでレイヤ 2 ループに起因するブロードキャストストームを防止するため、ELD を使用することができます：

- スタンドアロンスイッチに接続した VCS ファブリッククラスタ
- 複数のノードのネットワークに接続した VCS ファブリッククラスタ。
- 他の VCS ファブリッククラスタに接続した VCS ファブリッククラスタ。

図 12-1 は、レイヤ 2 ループの発生する可能性がある VCS ファブリッククラスタとスタンドアロンスイッチ間の誤った構成例を示しています。このケースでは、VCS ファブリッククラスタをスタンドアロンスイッチに接続する 2 つのスイッチ間接続に対して、VCS ファブリッククラスタのエッジデバイス上に VLAG が構成されています。このケースでは、スイッチ間接続の接続先であるスタンドアロンスイッチ上に LAG が作成されていません。ELD は、この潜在的なレイヤ 2 ループを検出し、切断します。

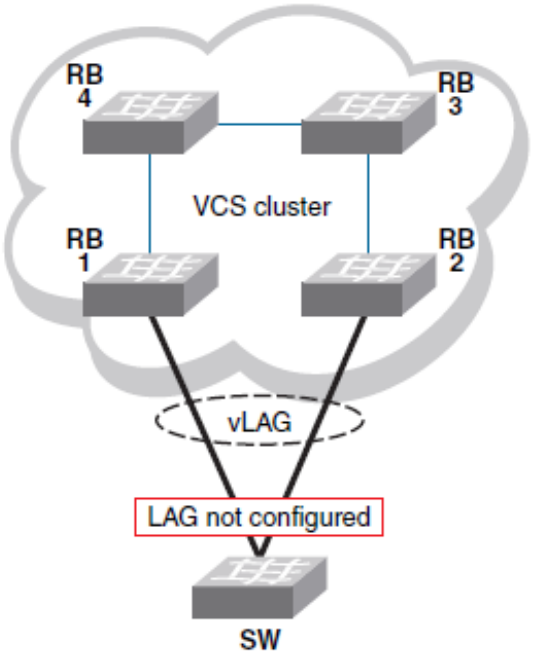

図 12-1　LAG を失ったことが原因のループ

図 12-2 は、ELD がレイヤ 2 ループを検出し、切断できる別の例を示します。このケースでは、レイヤ 2 ループを生み出す構成で複数の VCS ファブリッククラスタが相互接続されています。

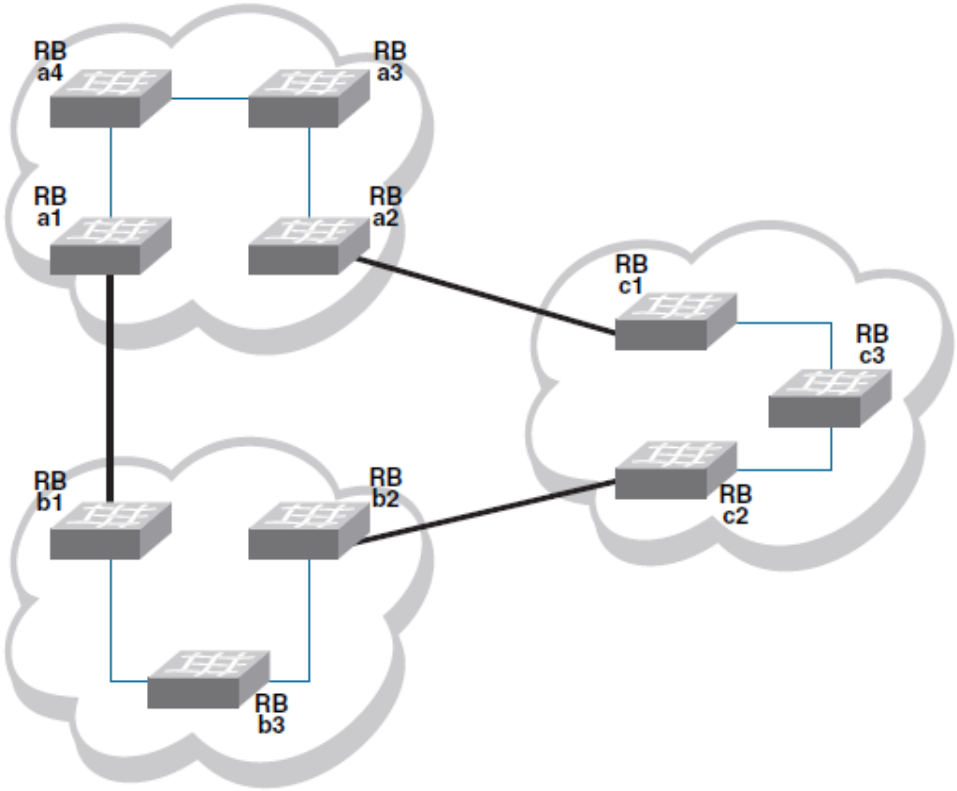

図 12-2　相互接続した VCS ファブリッククラスタが原因となるループ

NOTE

エッジループが発生した場合、VCS ファブリッククラスタ内で共用する MAC アドレステーブルに不整

合が発生する場合があります。ループ発生時は、いずれかひとつの RBridge で'clear mac-address-table dynamic'を必ず実行して MAC アドレステーブルが正常に同期するまでお待ち下さい。

12.2　ELD がループを検出する方法

ELD は、エッジポート上の Multicasting Protocol Data Unit(PDU)パケットによって動作します。ELD が送信する PDU を受けると、デバイスはループを認識します。デバイスは、レイヤ 2 ループが存在することを認識すると、そのポートを無効にし、レイヤ 2 ループを切断することができます。

無効なポートの数を最小限に抑えるために、ELD は、各ポートに優先順位と各々の VCS ファブリッククラスタに固有の受信制限(pdu-rx-limit)を割り当てます。ポートプライオリティは、クラスタの送信または受信エッジポートが無効になっているかどうかを決定します。pdu-rx-limit は、アクションが行われる VCS ファブリック上で決定します。これらの設定がされなければ、レイヤ 2 ループが同時に複数のクラスタ内で検出される可能性があります。その結果、複数のポートが無効になり、VCS ファブリッククラスタ間トラフィックが停止します。

図 12-3 は、149 ページの図 12-2 と同様の相互接続を示していますが、ELD は、各エッジポート上で有効なっておりポートプライオリティと pdu-rx-limit が割り当てられています。

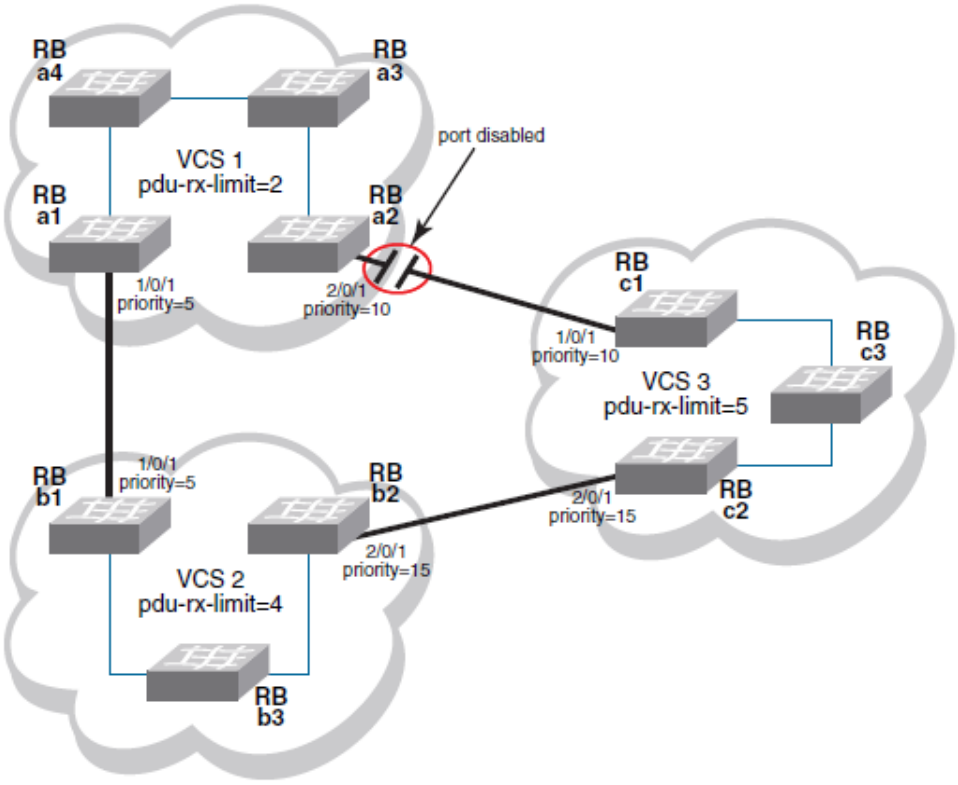

図 12-3　ELD が有効な相互接続の VCS ファブリッククラスタ

すべて ELD 有効エッジポートが同じ速度で PDU を送信すると、VCS1 は最初に pdu-rx-limit に到達します。ポート 2/0/1、ポート 1/0/1 よりも低い優先順位(優先順位の高い番号)を持っているため、無効にすることが選択されています。両方のポートが同じプライオリティの場合、ポート ID が高いポートが無効にされます。
ELD によってシャットダウンされたポートが LAG の一部である場合、LAG のすべてのメンバポートもシャットダウンされます。シャットダウンされたポートが VLAG の一部である場合は、その RBridge 上の VLAG のすべてのメンバポートもシャットダウンされます。
ELD は、ポートを無効にすると、任意の設定ミスが修復されるまで、ポートの通常の動作は、無効のままです。修復が完了すると、ポートを手動で再度有効にする必要があります。

NOTE
ELD がポートを無効にすると、ポートは運用上のステータスは down ですが、管理上のステータスは up です。(ELD による閉塞状況は、'show edge-loop-detection interface'コマンドで確認できます。)ポートが STP またはいくつかの他の L2 プロトコルによって無効にされている場合、ELD はそのポートに対して PDU を処理しません。

12.3 エッジループ検出の設定

エッジループの検出は、グローバルレベルおよびインタフェースレベルで設定を行う必要があります。グローバルレベルの設定に対して、VCS ファブリッククラスタはループが存在していることを判定する前に、任意のポート上で受信する PDU の数を設定する必要があります。この値が、pdu-rx-limit です。また、'hello-interval'コマンドを使用して PDU を送信する間隔を設定しなければなりません。pdu-rx-limit および、hello インターバルタイマの組み合わせは、ELD がレイヤ 2 ループを検出し、切断するのに要する時間を決定します。
インタフェースレベルでは、ポートプライオリティを設定したい各ポートで ELD を有効にする必要があります。また、ELD を有効にする VLAN を指定する必要があります。
ひとつの VCS ファブリッククラスタのみがポートを無効できるように、各 VCS ファブリッククラスタに異なる数値を制限として設定するには、'pdu-rx-limit'コマンドを入力します。隣接した２つの VCS ファブリッククラスタ上のポートが無効となる競合状態を防ぐために 2 増加させた値で設定することをお勧めします。
PDU 間の間隔を設定するには、'hello-interval'コマンドを入力します。この間隔は ELD が構成されているすべての VCS ファブリック· クラスタ上で同じ値に設定する必要があり、そうでなければ、エッジループ検出の結果が予測不能になります。
10 分～24 時間の間で指定した期間の経過後に、ポートを再度有効にするように設定するには、'shutdown-time'コマンドを入力します。この機能の典型的な使い方は、テスト環境のようにネットワークの再構成が一般的な環境においてです。典型的な使い方はデフォルト値のゼロのままでの使用であり、ポートが自動的に再度有効にすることを許可しません。

NOTE
'shutdown-time'への変更は、設定の変更後 ELD によって無効にされたポートに対してのみ有効です。'shutdown-time'の変更前に、ELD によって既に無効になっていたすべてのポートは、変更前の'shutdown-time'の値のままです。これらのポートは、現在実行中のタイマーが切れると、ELD は再度ループを検出し、ポートをシャットダウンした後、新しい'shutdown-time'時間に従い動作します。

ELD が実行されているインタフェースごとに、ELD を有効にするには、'edge-loop-detection vlan'コマンドを入力します。また、ポートプライオリティを指定するには、'edge-loop-detection port-priority'コマンドを入力します。

12.3.1　VCS ファブリッククラスタのためのグローバル ELD パラメータの設定

ELD を構成する VCS ファブリッククラスタの上で、この手順を実行してください。

1．VCS ファブリッククラスタ内の任意のスイッチにログインします。
2．グローバルコンフィグレーションモードで、エッジループ検出コンフィグレーションモードを開始するには、'protocol edge-loop-detection'コマンドを入力します。
3．レイヤ 2 ループを切断する前に受信された PDU の数を設定するには、'pdu-rx-limit *number*'コマンドを入力します。
number オペランドは、1 から 5 の値でなければなりません。デフォルト値は 1 です。
4．PDU 間の間隔を設定するには、'hello-interval number'コマンドを入力します。
number オペランドは、1 ミリ秒の単位を持っています。*number* オペランドの範囲は、100 ミリ秒から 5000 ミリ秒でなければなりません。デフォルト値は 1000 ミリ秒です。
5．シャットダウンポートが再度有効になった後の時間を分単位で設定するには、'shutdown-time *number*'コマンドを入力します。
number オペランドは、10 から 1440(10 分から 24 時間)までの範囲でなければなりません。デフォルト値は、0 でポートが自動的に再有効化されないことを示します。

例：この例では、5 つの PDU の受領の上でループを検出し、切断する VCS ファブリッククラスタを設定します。PDU の間隔は 2000 ミリ秒(2 秒)に設定されているため、任意のループは 10 秒後に中断されます。選ばれたポートは、ループ検出が自動的に再有効化された後、24 時間は無効のままです。

```
switch(config)# protocol edge-loop-detection
switch(config-eld)# pdu-rx-limit 5
switch(config-eld)# hello-interval 2000
switch(config-eld)# shutdown-time 1440
```

12.3.2　ポートでのインターフェースパラメータの設定

ELD で監視したいすべてのポートに対して、この手順を実行します。

1．VCS ファブリッククラスタ内の任意のスイッチにログインします。
2．グローバルコンフィグレーションモードで、エッジループの検出を有効にする RBridge/スロット/ポートを選択するには、interface コマンドを入力します。
3．インターフェースコンフィグレーションモードで、ELD がこのポート上で監視する VLAN を指定

するには、'edge-loop-detection vlan'コマンドを入力します。
VLAN を指定しない場合、コマンドは失敗します。

4．選択した VLAN の指定されたポートの ELD ポート優先度を指定するには、'edge-loop-detection port-priority'コマンドを入力します。しかし、スイッチングを可能にすることは、ポートプライオリティを割り当てるための必須条件ではありません。

NOTE
優先順位の値の範囲は 0 から 255 までです。優先順位 0 のポートは、このポートのシャットダウンが無効になっていることを意味します。デフォルト値のポートプライオリティは 128 です。

この例では、ポート 1/0/7 VLAN 10 およびポート 4/0/6 VLAN 10 の 2 つのポート/ VLAN ペアに ELD ポートプライオリティを設定します。これらのポートの両方が同じループで検出される場合、VCS ファブリッククラスタに対する pdu-rx-limit に到達すると、ELD は、ポート 4/0/6 をシャットダウンします。それが次にプライオリティのより低い(より大きい番号)ポート 1/0/7 を割り当てられているため、ポート 4/0/6 がシャットダウンに選択されます。

```
(config)# interface TenGigabitEthernet 1/0/7
(conf-if-te-1/0/7)# edge-loop-detection vlan 10
(conf-if-te-1/0/7)# edge-loop-detection port-priority 5
(conf-if-te-1/0/7)# top
(config)# interface TenGigabitEthernet 4/0/6
(conf-if-te-4/0/6)# edge-loop-detection vlan 10
(conf-if-te-4/0/6)# edge-loop-detection port-priority 7
```

12.4　エッジループのトラブルシューティング

誤った設定を表示し、修正するために'edge-loop detection'コマンドを使用します。

1．VCS ファブリッククラスタ内の任意のスイッチにログインします。
2．グローバルコンフィグレーションモードで、VCS ファブリッククラスタのエッジループ検知の統計情報を表示するには、'show edge-loop-detection'コマンドを入力します。
コマンド出力は、ELD でディセーブルとなったポートを示しています。
3．手順 2 で検出されたすべての設定の誤りを修正してください。
4．グローバルコンフィグレーションモードで次のいずれかの操作を実行します。
・ELD によって無効にされた一つのポートを有効化します。
- ELD によって無効にされたポートで、’shutdown’コマンドを入力します。
- ELD によって無効にされたポートで、'no shutdown'コマンドを入力します。

NOTE
リモートポートの VCS ID が変更され、エッジポートが ISL ポートになった場合、既に ELD によってシャットダウンされたポートは、ISL ポートとして検出させるためには、'shutdown'コマンド入力後'no shutdown'コマンドを使用する必要があります。

・ELD によって無効にされた全てのポートを有効化するには、'clear edge-loop-detection'コマン

ドを入力します。

13 AMPP の設定

13.1 AMPP 概要

サーバ仮想化インフラは、サーバ側の Virtual Ethernet Bridge (VEB)ポートプロファイルを、VEB ポートを介してネットワークにアクセスする Virtual Machine (VM)が使用するイーサネット MAC アドレスに関連付けています。
VM がある物理サーバから別のサーバにマイグレーションすると、VM に関連付けられたサーバの VEB ポートの自動的なポートプロファイルマイグレーションを提供することで、VEB ポートプロファイルは VM にあわせてマイグレーションします。
サーバ仮想化インフラが十分な制御を提供する環境では、ポートプロファイルが自動的にマイグレーションするアプローチは優れています。そのような環境の例は、ファイアウォールやセキュリティアプライアンスを介して外部ネットワークから分離されたレイヤ 2 ネットワークを使う高性能クラスタになります。
しかしながら、外部のレイヤ 2 スイッチでサポートされるアクセス制御及び QoS とサーバ仮想化インフラの間にはギャップがあります。外部のレイヤ 2 スイッチはサーバの VEB の実装に比べて、高度な制御機能を持っています。
幾つかの環境では、外部のネットワークスイッチで提供される更に高度な制御を必要とします。その例としては、異なる最新のネットワーク制御のもと、同じレイヤ 2 ネットワークの上で各種アプリケーションが動作するような多階層のデータセンタです。この種の環境では、ネットワーク管理者は外部ネットワークスイッチで利用可能な高度なアクセス制御を使うことを好みます。
レイヤ 2 ネットワークは、エンドポイントデバイスが一つのスイッチから別のスイッチに移動するとき、そのデバイスに関連したスイッチのアクセス制御及びトラフィック制御を自動的に移動するメカニズムを持っていません。マイグレーションは、例えばあるシステムのベアメタル OS で動作していて別のシステムに移動する(アプリケーション、ミドルウェア、OS 及び状態を意味する)OS イメージのような、物理的なものかもしれません。または、マイグレーションは、あるシステム上の VMware 上で動作していて、別のシステムの VMware で移動する OS イメージのように、仮想的なものかもしれません。
Brocade Auto Migrating Port Profile (AMPP)機能は、VM が物理サーバ間を移動するとき、ポートプロファイルの関係付けを管理や移動に対応して高度な制御を提供します。

13.1.1 AMPP over vLAG

Virtual Link Aggregation Group (vLAG)は、一つまたは複数の物理スイッチまたはサーバに接続することができる VCS ファブリックとのリンクを示す Brocade 独自の LAG の名前です。冗長性と高い帯域幅のために、vLAG は、VCS ファブリック技術の重要なコンポーネントです。AMPP は、物理ポートと同様に vLAG と標準 LAG でもサポートされています。

vLAG の詳細については、204 ページの『16 リンクアグリゲーションの設定』を参照してください。
次の例の下線付きのテキストは、ポートプロファイルの vLAG 情報であること示しています。

```
switch# show port-profile status
Port-Profile                    PPID      Activated    Associated MAC
Interface
auto-dvPortGroup                1         Yes          None               None
auto-dvPortGroup2               2         Yes          None               None
auto-dvPortGroup3               3         Yes          None               None
auto-dvPortGroup_4_0            4         Yes          0050.567e.98b0     None
auto-dvPortGroup_vlag           5         Yes          0050.5678.eaed     None
auto-for_iscsi                  6         Yes          0050.5673.85f9     None
                                                       0050.5673.fc6d     None
                                                       0050.5674.f772     None
                                                       0050.5675.d6e0     Te
234/0/54
                                                       0050.567a.4288     None
auto-VM_Network                 9         Yes          000c.2915.4bdc     None
                                                       0050.56a0.000d     None
                                                       0050.56a0.000e     None
                                                       0050.56a0.000f     None
                                                       0050.56a0.0010     Po 53
                                                       0050.56a0.0011     Po 53
                                                       0050.56a0.0012     Po 53
                                                       0050.56a0.0013     None
                                                       0050.56a0.0025     None
                                                       0050.56a0.0026     None
                                                       0050.56a0.0027     None
                                                       0050.56a0.0028     None
                                                       0050.56a0.0029     Po 53
                                                       0050.56a0.002a     Po 53
                                                       0050.56a0.002b     Po 53
                                                       0050.56a0.002c     None
                                                       0050.56a0.002d     None
                                                       0050.56a0.002e     None
                                                       0050.56a0.002f     None
                                                       0050.56b3.0001     Po 53
                                                       0050.56b3.0002     Po 53
                                                       0050.56b3.0004     Po 53
                                                       0050.56b3.0005     None
auto-VM_kernel                  10        Yes          0050.5671.4d06     None
                                                       0050.5672.862f     Po 53
                                                       0050.5678.37ea     None
                                                       0050.567a.ddc3     None
auto-VM_NW_1G                   11        Yes          0050.56b3.0000     None
                                                       0050.56b3.0003     Po 82
                                                       0050.56b3.0007     None
                                                       0050.56b3.0008     Po 82
                                                       0050.56b3.0009     Po 82
auto-VMkernel                   12        Yes          0050.567a.fdcf     Po 82
                                                       0050.567c.c2e3     None
auto-VMkernel_VS                13        Yes          0050.567d.16b9     None
                                                       0050.567e.e25b     None
auto-Management+Network         14        Yes          5cf3.fc4d.ca88     None
auto-Virtual+Machine+Network    15        Yes          000c.2941.27e2     None
                                                       000c.2980.335d     None

switch# show port-profile int all
Interface       Port-Profile
Gi 234/0/1      None
Gi 234/0/13     None
Gi 234/0/25     None
Gi 234/0/26     None
Te 234/0/54     auto-for_iscsi
Po 82           auto-VM_NW_1G
                auto-VMkernel
Po 53           auto-VM_Network
```

```
auto-VM_kernel
```

13.1.2　AMPP とスイッチドポートアナライザー

Switched Port Analyzer(SPAN)、またはポートミラーリングは、ネットワークアナライザによる分析のためのネットワークトラフィックを指定します。特定のポートを通過するトラフィックを観測したりスヌーピングしたい場合、人為的にアナライザに接続されたポートにパケットをコピーするため、ポートをミラーリングする必要があります。

AMPP でのポートミラーリングは、プロファイリングポートとしてミラーポートを使うために必要な機能を提供しています。プロファイルポートを宛先ポートとして、またその逆に設定することはできません。SPAN は、プロファイルポートで学習されたトラフィックをミラーリングすることができます。

SPAN の詳細については、275 ページの『22 スイッチドポートアナライザ(SPAN)設定』を参照してください。

13.1.3　スケーラビリティ

表 13-1 は、Network OS でサポートされているスケーラビリティ値を示します。

表 13-1　AMPP スケーラビリティ値

測定基準	スタンドアロンモード	ファブリッククラスタモード	ロジカルシャーシモード
プロファイル数	256	256(v 3.0.0 以前) 750(v 4.1 以降)	750
ポートプロファイル内の VLAN 数	2000	2000	2000
QoS プロファイル	1 cee-map 1 mutation-map	1 cee-map 1 mutation-map	1 cee-map 1 mutation-map
セキュリティプロファイル内の ACLs 数	レイヤ 2 ACL と同じ	レイヤ 2 ACL と同じ	レイヤ 2 ACL と同じ
MAC 関連付け数	8000	8000	8000

表 13-1 の MAC と VLAN スケーリング数は、MAC 関連付けと vlan プロフィールスケーリングに基づいています。さらに、AMPP は、スイッチでサポートされている vLAG と LAG の最大数に従います。従って、v3.0.0 では 256、v4.1 以降は 750 です。

13.2　AMPP ポートプロファイルの構成

図 13-1 に示す通り、デフォルトのポートプロファイルには、LAN および SAN へのアクセスを取得するために VM に必要な全体の構成が含まれています。

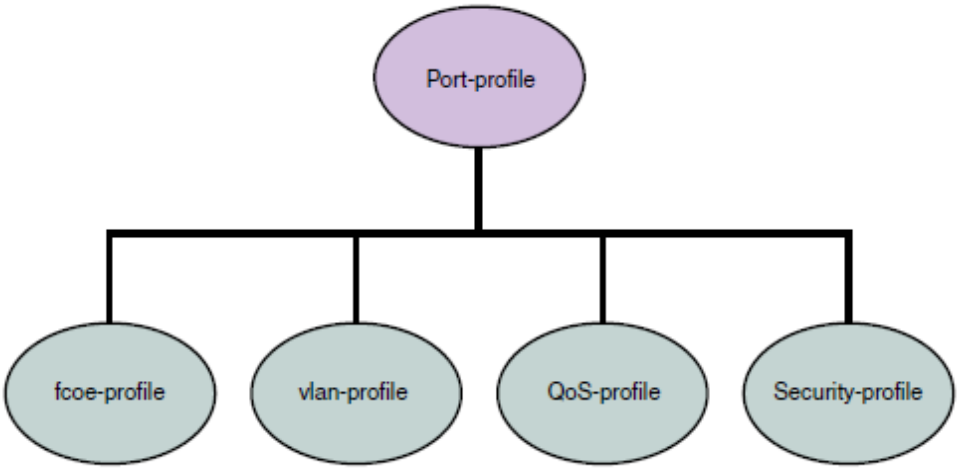

図 13-1　ポートプロファイルの内容

NOTE
ポートプロファイルは、LLDP や SPAN や LAG などの幾つかのインタフェースレベルのコンフィグレーションは含みません。

ポートプロファイルは、自己完結のコンフィグレーションコンテナとして動作します。言い換えれば、もしポートプロファイルが何も設定されていない新しいスイッチに提供された場合、インタフェースのローカル設定を構成し、トラフィックを通し始めることが可能となるということです。ポリシーに対するどのような変更もデータプレーンへ即座に適用されます。
セキュリティプロファイルは、プロファイルまたは PolicyID に基づく ACL に適用されます。したがって、複数のセキュリティプロファイルを同じプロファイル化されたポートに適用することができます。しかし、一旦ポートプロファイルを有効にするとポートプロファイルの編集は出来ません。ポートへプロファイルを適用する場合は、ポートプロファイルの有効化が必須です。

13.2.1　ポートプロファイルの状態

生成中のポートプロファイルは、多数の状態に遷移します。ポートプロファイルの状態は下記の通りです。

- Created - この状態は、ポートプロファイルが作成・修正されたが、完成してない状態を示します。
- Activated - この状態は、ポートプロファイルが有効化されて、MAC とポートプロファイルの関連が有効になっている状態です。もし、作成されたポートプロファイルが完成せず有効化できない場合は、あらゆる競合や依存関係を解決し、ポートプロファイルを再度有効化する必要があります。
- Associated - この状態は、ファブリック内で一つ以上の MAC アドレスがこのポートプロファイルと関連付けられている状態です。
- Applied - この状態は、ポートプロファイルが MAC アドレスと関連付けられた profiled ポートに適用された状態です。どのプロトコルも動作してない状態では、関連付けられた MAC アドレスがプロファイルポートに現れないかを検出するためシステムはパケットを覗き見します。２つの異なるポートプロファイル構成は、ひとつのプロファイルポートに共存できます。しかし、競合があると後

から適用されるポートプロファイルが適用失敗となります。

表 13-2 に、AMPP イベントおよび該当障害の動作について説明します。

表 13-2　AMPP の動作および障害の説明

AMPP イベント	該当する動作と障害内容
Create port-profile	ポートプロファイルが存在しない場合、新たに生成されます。存在していて有効化されてない場合、created となります。
Activate port-profile	ポートプロファイルの構成が完全でなければ、有効化は失敗します。もし、ポートプロファイルが有効化されなければ、どのポートにも適用されません。 すべての依存関係の検証が成功した場合、ポートプロファイルは ACTIVE 状態にあり、関連付けの可能な状態となります。 VLAN プロファイルは、すべてのポートプロファイルのために必須です。
De-activate port-profile	このイベントは全てのプロファイルポートの適用済みポートプロファイルの構成を削除します。 ポートプロファイルに関連付けられた MAC アドレスがあっても無効化されます。
Modify port-profile	ポートプロファイルは有効化される前だけ編集可能です。 ポートプロファイルは、属性に競合があったり、依存関係が不完全ならば、INACTIVE 状態となります。 ポートプロファイルは INACTIVE 状態となると、プロファイルの MAC アドレスへの関連付けはできません。
Associate MAC addresses to a port-profile	MAC アドレスが既にポートプロファイルに関連付けられていると、ポートプロファイルの MAC への関連付けは失敗します。 MAC への関連付けが成功している場合、その MAC があるポートで学習されると、MAC と関連付けられたポートプロファイルが適用されます。
De-associate MAC addresses from a port-profile	マッピングされている場合、特定の MAC アドレスに構成された全てのポリシーは、ポートもしくはスイッチから削除されます。
Deleting a port-profile	ポートプロファイルが有効化状態ならば、IN USE エラーが発生します。AMPP は削除する前にプロファイルを強制的に無効化します。 ポートプロファイルが有効化されている場合、プロファイルを削除すると全ての MAC との関係は削除されます。
Modifying port-profile content when in an associated state	ポートプロファイルが既に有効化されている場合、IN USE エラーが発生します。
Moving the VM MAC and notifying the	ポートプロファイル ID に関連付けられた全てのポリシーが MAC アドレスにマッピングされ、ファブリックの新しいポートに適用されます。

fabric	
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。

13.2.2　新しいポートプロファイルの構成

VM MAC アドレス学習をサポートするため、デフォルトポートプロファイルが使用されます。デフォルトポートプロファイルは、他のユーザー定義の AMPP プロファイルとは異なります。

- ポートプロファイル ID(ppid)を変更することは出来ません。
- VLAN サブプロファイルは修正できません。
- QoS サブプロファイルとセキュリティプロファイルは追加できません。
- デフォルトポートプロファイルは無効化できません。

要求に合わせるために新しいポートプロファイルを作成することを推奨します。新しいポートプロファイルを作成するために、特権実行モードで次の手順を実行してください。

1．物理インタフェースは、ポートプロファイルを作成する前に設定する必要があります。

2．新しいポートプロファイルの名称を作成・設定します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# port-profile vm1-port-profile
switch(config-port-profile-vm1-port-profile)# vlan-profile
switch(config-vlan-profile)# switchport
switch(config-vlan-profile)# switchport mode trunk
switch(config-vlan-profile)# switchport trunk native-vlan 300
switch(config-vlan-profile)# switchport trunk allowed vlan add 300
```

3．VLAN プロファイルコンフィグレーションモードを終了します。

```
switch(config-vlan-profile)# exit
switch(config-port-profile-vm1-port-profile)# exit
```

4．プロファイルを有効化します。

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

5．各ホストに対してプロファイルを MAC アドレスに関連付けます。

```
switch(config)# port-profile vm1-port-profile static 0050.56bf.0001
switch(config)# port-profile vm1-port-profile static 0050.56bf.0002
switch(config)# port-profile vm1-port-profile static 0050.56bf.0003
switch(config)# port-profile vm1-port-profile static 0050.56bf.0004
switch(config)# port-profile vm1-port-profile static 0050.56bf.0005
```

13.2.3　VLAN プロファイルの設定

VLAN プロファイルは、ポートプロファイル全体の VLAN 構成を定義します。それは、tagged と untagged VLAN の両方を含みます。

NOTE

Network OS v3.0.0 は VLAN classifier をサポートしていません。

VLAN プロファイルを設定するために、グローバルコンフィグレーションモードで次の手順を実行してください。

1．AMPP プロファイルは有効な間は修正できません。VLAN プロファイルを修正する前にポートプロファイルを無効化してください。

```
switch(config)# no port-profile vm1-port-profile activate
```

２．VLAN プロファイルコンフィグレーションモードに移行します。

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

３．モードをレイヤ 2 に変更しスイッチング特性をデフォルトに設定します。

```
switch(config-vlan-profile)# switchport
```

４．正しい VLAN に対して VLAN プロファイルモードにアクセスします。

```
switch(config-vlan-profile)# switchport mode access
switch(config-vlan-profile)# switchport access vlan 200
```

５．trunk コンフィグレーションモードに移行します。

```
switch(config-vlan-profile)# switchport mode trunk
```

６．allowed VLAN ID を指定して trunk モードを設定します。

```
switch(config-vlan-profile)# 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(config-vlan-profile)# 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(config-vlan-profile)# exit
switch(config-port-profile-vm1-port-profile)# exit
```

９．プロファイルを有効化します。

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

１０．プロファイルを MAC アドレスに関連付けます。

```
switch(config)# port-profile vm1-port-profile static 0050.56bf.0001
switch(config)# port-profile vm1-port-profile static 0050.56bf.0002
switch(config)# port-profile vm1-port-profile static 0050.56bf.0003
switch(config)# port-profile vm1-port-profile static 0050.56bf.0004
switch(config)# port-profile vm1-port-profile static 0050.56bf.0005
```

１１.変更したいインタフェースのインターフェースコンフィグレーションモードをアクティブにします。次の例は、スロット 0/ポート 0 の 10 ギガビットイーサネットインターフェース用のモードをアクティブにします。

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

１２．物理インタフェース上でポートプロファイルポートを設定します。

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

13.2.4　QoS プロファイルの設定

QoS プロファイルは次の値を定義します。

- 入力の 802.1p プライオリティが内部のキュープライオリティに設定されます。ポートが QoS 非トラストモードの場合、全ての入力のプライオリティはデフォルトのベストエフォートプライオリティにマッピングされます。
- 入力のプライオリティが出力のプライオリティに設定されます。
- 入力プライオリティのマッピングが絶対優先または WRR トラフィッククラスに設定されます。
- 絶対優先または WRR トラフィッククラスでのフロー制御を有効化

QoS プロファイルは、CEE QoS とイーサネット QoS の２つの特色を持ちます。QoS プロファイルは CEE QoS かイーサネット QoS のいずれかを含みます。サーバ側のポートは、通常、コンバージドトラフィックを運んでいます。

QoS プロファイルを設定するため、グローバルコンフィグレーションモードで次の手順を実行します。

１．AMPP プロファイルは有効な間は修正できません。VLAN プロファイルを修正する前にポートプ

ロファイルを無効化します。

```
switch(config)# no port-profile vm1-port-profile activate
```

2．QoS プロファイルモードに移行します。

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

3．CEE マップを適用します。(ファブリッククラスタモード/ロジカルシャーシクラスタモードの場合)

```
switch(config-qos-profile)# cee default
```

4．デフォルト CoS 値を設定します。

```
switch(config-qos-profile)# qos cos 6
```

5．CoS に対する QoS トラスト属性を設定します。(スタンドアロンモードの場合)

```
switch(config-qos-profile)# qos trust cos
```

6．プロファイルへのマップを適用します。以下のいずれかを行います。(スタンドアロンモードの場合)

- 存在する CoS-to-CoS ミューテイションマップを適用する

```
switch(config-qos-profile)# qos cos-mutation vm1-cos2cos-map
```

- 存在する CoS-to-Traffic クラスマップを適用する。

```
switch(config-qos-profile)# qos cos-traffic-class vm1-cos2traffic-map
```

7．以下のいずれかの Pause 機能を有効にします。(スタンドアロンモードの場合)

- PFC なし

```
switch(config-qos-profile)# qos flowcontrol tx on rx on
```

- 各 CoS 値に対する PFC 付

```
switch(config-qos-profile)# qos flowcontrol pfc 1 tx on rx on
switch(config-qos-profile)# qos flowcontrol pfc 2 tx on rx on
```

8．QoS プロファイルモードを終了します。

```
switch(config-qos-profile)# exit
```

9．プロファイルを有効化します。

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

１０．プロファイルを MAC アドレスに関連付けます。

```
switch(config)# port-profile vm1-port-profile static 0050.56bf.0001
switch(config)# port-profile vm1-port-profile static 0050.56bf.0002
switch(config)# port-profile vm1-port-profile static 0050.56bf.0003
switch(config)# port-profile vm1-port-profile static 0050.56bf.0004
switch(config)# port-profile vm1-port-profile static 0050.56bf.0005
```

１１.変更したいインタフェースのインターフェースコンフィグレーションモードをアクティブにします。次の例は、スロット 0/ポート 0 の 10 ギガビットイーサネットインターフェース用のモードをアクティブにします。

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

１２．物理インタフェース上でポートプロファイルポートを設定します。

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

13.2.5　セキュリティプロファイルの設定

セキュリティプロファイルは、サーバが接続されたポートに必要な全てのセキュリティルールを定義します。典型的なセキュリティプロファイルは MAC ベースの標準または拡張 ACL の属性値を含みます。セキュリティプロファイルは、プロファイルまたは PolicyID に基づく ACL に適用されます。したがって、複数のセキュリティプロファイルを同じプロファイル対象のポートに適用することができます。

セキュリティプロファイルを設定するため、グローバルコンフィグレーションモードで次の手順を実行します。

1．AMPP プロファイルは有効な間は修正できません。セキュリティプロファイルを修正する前にポートプロファイルを無効化します。

```
switch(config)# no port-profile vm1-port-profile activate
```

2．セキュリティポートプロファイルコンフィグレーションモードに移行します。

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

3．ACL セキュリティ属性を修正します。

詳細は 227 ページの『19 アクセスコントロールリスト(ACL)の設定』を参照下さい。

4．セキュリティプロファイルに ACL を適用します。

```
switch(config-security-profile)# mac access-group vm1-acl in
```

5．セキュリティプロファイルコンフィグレーションモードを終了します。

```
switch(config-security-profile)# exit
switch(config-port-profile-vm1-port-profile)# exit
```

6．プロファイルを有効化します。

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

7．各ホストの MAC アドレスにプロファイルを関連付けます。

```
switch(config)# port-profile vm1-port-profile static 0050.56bf.0001
switch(config)# port-profile vm1-port-profile static 0050.56bf.0002
switch(config)# port-profile vm1-port-profile static 0050.56bf.0003
switch(config)# port-profile vm1-port-profile static 0050.56bf.0004
switch(config)# port-profile vm1-port-profile static 0050.56bf.0005
```

8. 変更したいインタフェースのインターフェースコンフィグレーションモードをアクティブにします。次の例は、スロット 0/ポート 0 の 10 ギガビットイーサネットインターフェース用のモードをアクティブにします。

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

9．物理インタフェース上でポートプロファイルポートを設定します。

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

13.2.6　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グレーションモードで次の手順を実行します。

1. 変更したいインタフェースのインターフェースコンフィグレーションモードをアクティブにします。次の例は、スロット 0/ポート 0 の 10 ギガビットイーサネットインターフェース用のモードをアクティブにします。

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

2．物理インタフェース上でポートプロファイルポートの設定を削除します。

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

13.2.7　ポートプロファイルの削除

ポートプロファイルを削除するために特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
switch(config)#
```

2．ポートプロファイルを非アクティブにします。

```
switch(config)# no port-profile vm1-port-profile activate
```

3．カスタムプロファイルを削除するためポートプロファイルコマンドの"no"付を使います。デフォルトポートプロファイルは削除できません。

```
switch(config)# no port-profile vm1-port-profile
```

13.2.8　サブプロファイルの削除

サブプロファイルを削除するには、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#
```

2．ポートプロファイルを非アクティブにします。

```
switch(config)# no port-profile vm1-port-profile activate
```

3．ポートプロファイルモードに移行します。

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

4．VLAN サブプロファイルを削除するには：

```
switch(config-port-profile-vm1-port-profile)# no vlan-profile
```

5．セキュリティサブプロファイルを削除するには：

```
switch(config-port-profile-vm1-port-profile)# no security-profile
```

6．　QoS サブプロファイルを削除するには：

```
switch(config-port-profile-vm1-port-profile)# no qos-profile
```

13.3　AMPP プロファイルの確認

AMPP プロファイルを確認するには、特権実行モードで次の手順を実行します。

1．現在の MAC の詳細を表示するため、'show'コマンドを使います。

```
switch# show mac-address-table port-profile
Legend: Untagged(U), Tagged (T), Not Forwardable(NF) and Conflict(C)
VlanId   Mac-address       Type      State       Port-Profile      Ports
1        0050.5679.5351   Dynamic    Active      Profiled(U)       Te 111/0/10
1        0050.567b.7030   Dynamic    Active      Profiled(U)       Te 111/0/12
1        005a.8402.0000   Dynamic    Active      Profiled(T)       Te 111/0/24
1        005a.8402.0001   Dynamic    Active      Profiled(NF)      Te 111/0/24
1        005a.8402.0002   Dynamic    Active      Not Profiled      Te 111/0/24
1        005a.8402.0003   Dynamic    Active      Not Profiled      Te 111/0/24
1        005a.8402.0004   Dynamic    Active      Not Profiled      Te 111/0/24
1        005a.8402.0005   Dynamic    Active      Profiled(NF)      Te 111/0/24
1        005a.8402.0006   Dynamic    Active      Not Profiled      Te 111/0/24
1        005a.8402.0007   Dynamic    Active      Profiled(T)       Te 111/0/24
1        005b.8402.0001   Dynamic    Active      Profiled(T)       Te 111/0/24
1        005c.8402.0001   Dynamic    Active      Profiled(T)       Te 111/0/24
100      005a.8402.0000   Dynamic    Active      Profiled          Te 111/0/24
100      005a.8402.0001   Dynamic    Active      Profiled(NF)      Te 111/0/24
100      005a.8402.0003   Dynamic    Active      Not Profiled      Te 111/0/24
100      005a.8402.0005   Dynamic    Active      Profiled(NF)      Te 111/0/24
100      005a.8402.0007   Dynamic    Active      Profiled          Te 111/0/24
Total MAC addresses : 17
```

2．全ての利用可能なポートプロファイル設定を表示するため、'show running-config'を使います。

```
switch# show running-config port-profile
port-profile default
 vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
 !
```

```
!
port-profile vm_kernel
 vlan-profile
  switchport
  switchport mode access
  switchport access vlan 1
```

3．現在のポートプロファイル設定を表示するため、'show port-profile'コマンドを使います。

```
switch# show port-profile
port-profile default
ppid 0
 vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
  port-profile vm_kernel
  ppid 1
 vlan-profile
  switchport
  switchport mode access
  switchport access vlan 1
```

4．現在の全ての AMPP プロファイルの状態を表示するために、'show port-profile status'コマンドを使います。

```
switch# show port-profile status applied
Port-Profile            PPID        Activated    Associated MAC   Interface
auto-for_iscsi          6           Yes          0050.5675.d6e0   Te 9/0/54
auto-VM_Network         9           Yes          0050.56b3.0001   Te 9/0/53
                                                 0050.56b3.0002   Te 9/0/53
                                                 0050.56b3.0004   Te 9/0/53
                                                 0050.56b3.0014   Te 9/0/53
switch# show port-profile status activated
Port-Profile            PPID        Activated    Associated MAC   Interface
auto-dvPortGroup        1           Yes          None             None
auto-dvPortGroup2       2           Yes          None             None
auto-dvPortGroup3       3           Yes          None             None
auto-dvPortGroup_4_0    4           Yes          0050.567e.98b0   None
auto-dvPortGroup_vlag   5           Yes          0050.5678.eaed   None
auto-for_iscsi          6           Yes          0050.5673.85f9   None
switch# show port-profile status associated
Port-Profile            PPID        Activated    Associated MAC   Interface
auto-dvPortGroup_4_0    4           Yes          0050.567e.98b0   None
auto-dvPortGroup_vlag   5           Yes          0050.5678.eaed   None
auto-for_iscsi          6           Yes          0050.5673.85f9   None
```

5．プロファイルおよび適用インタフェース情報を表示するために、'show port-profile interface all'コマンドを使用します。

```
switch# show port-profile interface all
Port-profile            Interface
auto-VM_Network         Te 9/0/53
auto-for_iscsi          Te 9/0/54
```

14 VLAN の設定

14.1 VLAN 概要

IEEE 802.1Q Virtual LANs (VLANs)は物理ネットワーク上に複数の仮想ネットワークを重ねる機能を提供します。VLAN は仮想ネットワーク間のネットワークトラフィックを隔離し、管理及びブロードキャストドメインのサイズを小さくすることが可能です。
VLAN は物理的な位置に依存しないことが要求される共通の要件を持ったエンドステーションを含みます。エンドステーションが物理的に同一 LAN セグメントに無かったとしても、一つの VLAN にグループ化することが出来ます。VLAN は一般的に IP サブネットワークと関連付けられ、個々の IP サブネットの全てのエンドステーションは、同一 VLAN に属します。VLAN 間のトラフィックは、ルーティングされなければなりません。VLAN の構成要素は、インタフェース毎に設定できます。

14.2 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 が割り当てられていない場合、native VLAN の全ての送出フレームは、タグ無です。
  - native VLAN に設定された VLAN タグと等しいタグを持ったフレームは、native VLAN で処理されます。
  - 入出力に対して、native VLAN でないタグ付フレームは、ユーザーが指定した VLAN に従って処理されます。これは、trunk モードと呼ばれています。

NOTE
入力の VLAN フィルタは、デフォルトで全てのレイヤ 2 インタフェースで有効です。これは、VLAN がユーザー設定に依存して受信ポートでフィルタされることを保証しています。

図 14-1 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。

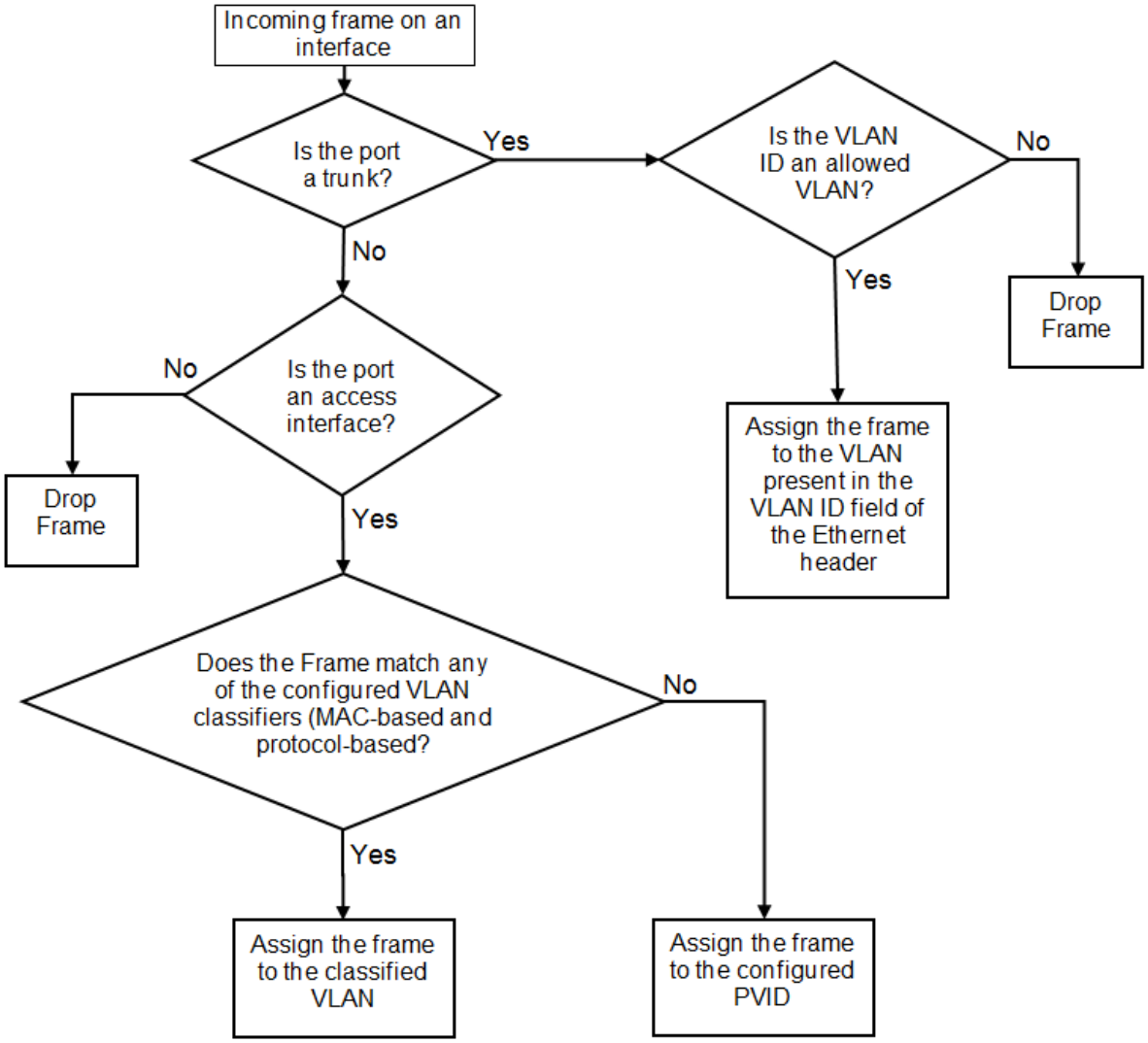

図 14-1　入力の VLAN フィルタ

入力の VLAN フィルタに関して、理解しておくべき重要な要件があります。

- 入力の VLAN フィルタはポートの VLAN メンバに依存します。
- ポートの VLAN メンバは Network OS の CLI から構成されます。
- 動的 VLAN 登録はサポートしていません。
- VLAN フィルタリングを入出力ポートの両方で行います。
- LAG インタフェースのような論理的なレイヤ 2 インタフェースでの VLAN フィルタはポートインタフェースと同様です。
- VLAN FDB(filtering database)は、入力フレームの転送先を決定します。

補助的に、VLAN FDB について知っておくべき重要な要件があります。

- VLAN FDB は MAC アドレスと VLAN ID に基づき到着フレームの転送先を決定するのを補助する情報を含みます。FDB は、静的定義とスイッチにより学習する動的定義の両方を含みます。

- 学習により FDB エントリを動的に更新する機能をサポートしています。(ポートの状態が許可されていた場合。)
- 動的 FDB エントリは、マルチキャストグループアドレスに対しては生成されません。
- 動的 FDB エントリは、ハードウェアに設定されたエージングタイムに基づき、消えていきます。エージングタイムは、60 から 1000000 秒の間で設定できます。デフォルトは 300 秒です。
- VLAN ID を指定して、静的に MAC アドレスを登録することが出来ます。静的エントリは消えません。
- 静的 FDB エントリは、存在している動的に学習された FDB エントリを上書きし、エントリを消してしまう学習を無効にします。

NOTE

スイッチでのフレーム操作の詳細については、33 ページの『1.5 レイヤ 2 イーサネットの概要レイヤ 2 イーサネットの概要』を参照下さい。

14.3 VLAN 設定のガイドラインと制限

VLAN を設定する場合は、これらの VLAN 設定のガイドラインと制約に従ってください。

- アクティブなトポロジにおいて、独立した VLAN 学習(IVL)機能により、VLAN 単位に MAC アドレスが学習されます。
- MAC アドレス ACL は、いつも静的 MAC アドレスエントリを上書きします。このケースでは、MAC アドレスは転送アドレスであり、FDB エントリは ACL によって上書きされます。
- 本スイッチは、イーサネット DIX フレームと 802.2LLC SNAP encapsulated フレームのみをサポートしています。
- 802.1q トランクリンクの両端で同じネイティブ VLAN を設定する必要があります。そうしないと、ループおよび VLAN リークをブリッジングループの原因となることがあります。
- VCS ファブリッククラスタ内のすべてのスイッチは、同じ VLAN 番号を使用して設定する必要があります。
- 1 行で入力できる文字数は、コマンドを含めて 250 文字となっています。このため、'switchport trunk allowed vlan'で定義できる VLAN ID は、この文字数制限を越えて定義できません。

14.4 VLAN のデフォルト設定

表 14-1 は VLAN のデフォルト設定を示しています。

表 14-1　VLAN デフォルト設定

パラメータ	デフォルト設定
デフォルト VLAN	VLAN1
MTU サイズ	2,500bytes

14.5　VLAN の構成と管理

この節では、VLAN を設定・管理する様々な手順を解説しています。

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。

14.5.1　インタフェースポートの有効化・無効化

NOTE
DCB インタフェースは、スタンドアロンモードでは、デフォルトで無効になりますが、VCS ファブリックモードでは、デフォルトで有効になります。

NOTE
DCB インタフェースは、イーサネットリンクスピードのオートネゴシエーションをサポートしていません。DCB インタフェースは、10 ギガビットイーサネットおよびギガビットイーサネットをサポートしています。

インタフェースポートを有効化・無効化するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．インタフェースタイプとスロット/ポートを指定するために、'interface'コマンドを入力します。VCS モードでは、"gigabitethernet *rbridge-id/slot/port"*オペランドのみを使用します。これらのポートのためのプロンプトは、switch(config-if-gi-22/0/1)#のフォーマットになります。
```
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
```

14.5.2　インタフェースポートの MTU 設定

NOTE
ファブリック全体は、単一のスイッチのような働きをします。そのため、MTU はエッジポートにのみ適用できて、ISL 上ではありません。

MTU(maximum transmission unit)を設定するため、インタフェースポート上で、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．インタフェースタイプとスロット/ポートを指定するために、'interface'コマンドを入力します。
```
switch(config)# interface tengigabitethernet 0/1
```
3．インタフェースポートを有効化するため、'no shutdown'コマンドを実行します。
4．インタフェースポートの MTU を指定するため、'mtu'コマンドを実行します。
```
switch(conf-if-te-0/1)# mtu 4200
```

14.5.3　VLAN の作成

VLAN はコンフィグレーションの観点から、インタフェースとして取り扱われます。
デフォルトでは、全てのポートは VLAN1(VLAN ID = 1)に割り当てられます。vlan_ID の値は 1 から 3963 が利用できます。VLAN ID 3964 から 4094 はシステムで予約しています。また、VLAN1002(VLAN ID=1002)は、VCS モードではシステムで予約されていますが、Network OS 4.x 以降、スタンドアロンモードでもシステムで予約されており、使用できません。

NOTE
Network OS 3.0.0 では、'reserved vlan'コマンドをサポートしていません。

VLAN インタフェースを作成するには、特権実行モードから、次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．VLAN インタフェースに番号を割り当てるため、'interface vlan'コマンドを実行します。
```
switch(config)# interface vlan 1010
```

14.5.4　VLAN での STP の有効化

インタフェースポートの全ては、一旦 VLAN に構成されます。一つのコマンドで、VLAN の全てのメンバに対して Spanning Tree Protocol (STP)を有効にすることが出来ます。
VLAN の STP を有効にするため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．VLAN の STP のタイプを選択するため、'protocol spanning tree'コマンドを実行します。
```
switch(config)# protocol spanning-tree pvst
switch(config-pvst)# exit
```
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 1010
```

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(config-Vlan-1010)# no spanning-tree shutdown
```

14.5.5　VLAN の STP の無効化

全てのインタフェースポートは、一旦 VLAN に設定されます。一つのコマンドで、VLAN の全てのメンバの STP を無効化できます。

VLAN の STP を無効化するため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．VLAN インタフェース番号を選択するため、'interface'コマンドを実行します。

```
switch(config)# interface vlan 55
```

3．VLAN55 のスパニングツリーを無効化するため、'spanning-tree shutdown'コマンドを実行します。

```
switch(config-Vlan-55)# spanning-tree shutdown
```

14.5.6　レイヤ 2 スイッチポートとしてのインタフェースポートの構成

レイヤ 2 スイッチポートとしてインタフェースを構成するため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。

VCS モードでは、"tengigabitethernet *rbridge-id*/*slot*/*port*"オペランドのみを使用します。これらのポートのためのプロンプトは、switch(config-if-te-22/0/1)# のフォーマットになります。

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

3．DCB インタフェースを有効化するため、'no shutdown'コマンドを実行します。

4．レイヤ 2 スイッチポートとして構成するため、'switchport'コマンドを入力します。

5．DCB インタフェースの状態を確認するため、'do show'コマンドを入力します。

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

6．DCB インタフェース実行コンフィグレーションの状態を表示するため、'do show'コマンドを実行します。

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

14.5.7　アクセスインタフェースとしてのインタフェースポートの構成

各 DCB インタフェースポートは、フレームが untagged か tagged かに基づき受信します。アクセスモードは、untagged と priority-tagged フレームのみ受け付けます。

アクセスインタフェースとしてインタフェースを構成するため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行

します。
```
switch(config)# interface tengigabitethernet 0/1
```
3．DCB インタフェースを有効化するため、'no shutdown'コマンドを実行します。
4．レイヤ 2 スイッチポートとしてインタフェースを設定するため、'switchport'コマンドを入力します。
```
switch(conf-if-te-0/1)# switchport
switch(conf-if-te-0/1)# switchport access vlan 20
```

14.5.8　トランクインタフェースとしてのインタフェースポートの設定

各 DCB インタフェースポートは、フレームが untagged か tagged かに基づき受信します。トランクモードは、VLAN-tagged フレームのみ受け付けます。
トランクインタフェースとしてインタフェースを構成するため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。
```
switch(config)# interface tengigabitethernet 0/19
```
3．DCB インタフェースを有効化するため、'no shutdown'コマンドを実行します。
4．DCB インタフェースをトランクモードとするため、'switchport'コマンドを実行します。
```
switch(conf-if-te-0/19)# switchport
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
```

14.5.9　トランクインタフェースの VLAN の無効化

トランクインタフェースの VLAN を無効化するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。
```
switch(config)# interface tengigabitethernet 0/10
```
3．DCB インタフェースを有効化するため、'no shutdown'コマンドを実行します。

4．DCB インタフェースをトランクモードとするため、'switchport'コマンドを実行します。

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

5．トランクポートから VLAN 範囲を削除するには、もう一度、'switchport'コマンドを入力します。

```
switch(conf-if-te-0/10)# switchport trunk allowed vlan remove 30
```

14.6　プロトコルベース VLAN の分類ルールの設定

プロトコルや MAC アドレスに基づく選択された VLAN への分類されたフレームに対して特別なルールを定義するため、VLAN classifier ルールを構成できます。ルールの組は VLAN classifier グループに分類されます。(174 ページの『14.6.4 VLAN classifier グループと付加ルールの作成』を参照下さい。)
VLAN classifier ルール(1 から 256)は、これらのカテゴリの一つにある構成可能なルールの組です。

- 802.1Q protocol-based classifier ルール
- ソース MAC address-based classifier ルール
- Encapsulated Ethernet classifier ルール

NOTE
複数の VLAN classifier は、別のルールからユニークとなるよう結果として VLAN ID を提供するインタフェース単位に適用されます。

802.1Q protocol-based VLAN は、untagged フレームか優先度タグ付のフレームにのみ適用されます。
Ethernet-II と 802.2 SNAP encapsulated frames の両方は、次のプロトコルタイプをサポートしています。

- Ethernet hexadecimal (0x0000 から 0xffff)
- Address Resolution Protocol (ARP)
- IP version 6 (IPv6)

NOTE
利用可能な全ての VLAN classifier のオプションの完全な情報として、『Network OS Command Reference』を参照下さい。

14.6.1　VLAN classifier ルールの生成

ARP protocol-based VLAN classifier ルールを生成するため、特権実行モードから次の手順で実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．protocol-based VLAN classifier ルール構成するため、'vlan classifier rule'コマンドを入力します。

```
switch(config)# vlan classifier rule 1 proto ARP encap ethv2
```

14.6.2　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.7f1d
```

14.6.3　VLAN classifier ルールの削除

VLAN classifier groups (1 から 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
```

14.6.4　VLAN classifier グループと付加ルールの作成

VLAN classifier グループ(1 から 16)は、いくつでも VLAN classifier ルールを含めることが出来ます。
VLAN classifier グループを構成し VLAN classifier ルールを追加するため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．VLAN classifier group を作成してルールを追加します。

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

14.6.5　インタフェースポートの VLAN classifier グループの有効化

VLAN classifier グループとインタフェースポートを結びつけるために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを入力します。

VCS モードでは、"tengigabitethernet rbridge-id/slot/port"オペランドのみを使用します。これらのポートのためのプロンプトは、switch(config-if-gi-22/0/1)#のフォーマットになります。

```
switch(config)# interface tengigabitethernet 0/10
```

3．DCB インタフェースを有効化する'switchport'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。

14.6.6　VLAN 情報の表示

VLAN 情報を表示するため、特権実行モードから次のコマンドを入力します。

1．指定したインタフェースの構成情報と状態を表示するため、'show interface'コマンドを入力します。

```
switch# show interface tengigabitethernet 0/10 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
```

14.7　MAC アドレステーブルの設定

各 DCB ポートは MAC アドレステーブルを持っています。MAC アドレステーブルは、フラッディングをさけるためユニキャストとマルチキャストを格納しています。内蔵 DCB スイッチはハードウェアでエージングタイマを持っています。もし、MAC アドレスが残留すると、指定した時間後無効化され、MAC アドレステーブルテーブルから削除されます。レイヤ 2 イーサネット環境において、スイッチがどのように MAC アドレスを操作するかの詳細については、33 ページの『1.5 レイヤ 2 イーサネットの概要』を参照下さい。

14.7.1　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、適切な値を入力します。

```
switch(config)# mac-address-table aging-time 600
```

14.7.2　MAC アドレステーブルへの静的アドレス登録

MAC アドレステーブルに静的アドレスを登録するため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．下記の例では、VLAN100 で受信するパケットに対して、静的アドレス 0011.2222.3333 を MAC アドレステーブルに登録します。

```
switch(config)# mac-address-table static 0011.2222.3333 forward
tengigabitethernet 0/1 vlan 100
```

14.8　ネイティブＶＬＡＮ

ネイティブ VLAN は、トランクインタフェースにおいて untagged フレームを送受信する VLAN です。DCB スイッチでは、トランクインタフェースを設定すると、自動的にネイティブ VLAN が有効になります。デフォルトでは、VLAN１(デフォルト VLAN)がネイティブ VLAN です。
一方、ネイティブ VLAN で tagged フレームを扱うことも出来ます。この場合、untagged フレームを受信すると破棄します。次の表に、ネイティブ VLAN 設定に関する各オプションと、DCB スイッチでのフレーム送受信時の動作を示します。

表 14-2　ネイティブ VLAN 動作仕様

グローバル設定		no vlan dot1q tag native		vlan dot1q tag native	
インタフェース設定		no switchport trunk tag native-vlan	switchport trunk tag native-vlan	no switchport trunk tag native-vlan	switchport trunk tag native-vlan
ネイティブ VLAN で扱うフレームの送信		untagged	untagged	untagged	tagged
到着フレーム	untagged	ネイティブ VLAN で受信	ネイティブ VLAN で受信	ネイティブ VLAN で受信	破棄
	tagged	ネイティブ VLAN で受信	ネイティブ VLAN で受信	ネイティブ VLAN で受信	ネイティブ VLAN で受信

14.8.1　ネイティブ VLAN の設定

ネイティブ VLAN は、スイッチ単位で設定するグローバル設定と、ポート個別に設定するインタフェース設定の２種類の設定方法があります。この設定の組合せにより、送受信時の動作が決定します。詳細は、表 14-2 を参照ください。

(1) ネイティブ VLAN グローバル設定

ネイティブ VLAN をグローバルに設定する場合は、次の手順に従ってください。

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．ネイティブ VLAN で、untagged フレームを取り扱うか、tagged フレームを取り扱うかで適切なコマンドを入力します。次の例は、untagged フレームを取り扱う場合の例です。

```
switch(config)# no vlan dot1q tag native
```

(2) ネイティブ VLAN インタフェース設定

ネイティブ VLAN を各インタフェースに設定する場合は、次の手順に従ってください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。

```
switch(config)# interface tengigabitethernet 0/19
```

3．DCB インタフェースを有効化するため、'no shutdown'コマンドを実行します。

4．DCB インタフェースをトランクモードとするため、'switchport'コマンドを実行します。

```
switch(conf-if-te-0/19)# switchport
switch(conf-if-te-0/19)# switchport mode trunk
```

5．ネイティブ VLAN で、untagged フレームを取り扱うか、tagged フレームを取り扱うかで適切なコマンドを入力します。次の例は、tagged フレームを取り扱う場合の例です。なお、上記ステップの'switchport mode trunk'を設定することで、自動的に'switchport trunk tag native-vlan'は設定されます。

```
switch(conf-if-te-0/19)# no switchport trunk tag native-vlan
```

14.8.2　ネイティブ VLAN の変更

ネイティブ VLAN は、デフォルトでは VLAN 1 (デフォルト VLAN)ですが、次の手順により任意の VLAN ID に変更することが出来ます。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。

```
switch(config)# interface tengigabitethernet 0/19
```

3．DCB インタフェースを有効化するため、'no shutdown'コマンドを実行します。

4．DCB インタフェースをトランクモードとするため、'switchport'コマンドを実行します。

```
switch(conf-if-te-0/19)# switchport
switch(conf-if-te-0/19)# switchport mode trunk
```

5．ネイティブ VLAN の VLAN ID を変更するため、'switchport trunk native-vlan *vlan_id* を実行します。

```
switch(conf-if-te-0/19)# switchport trunk native-vlan 100
```

14.8.3　ネイティブ VLAN の無効化

DCB スイッチでは、ネイティブ VLAN を設定により無効化することが出来ません。しかし、次の設定手順により、トランク設定の VLAN で取り扱うことが可能となり、実質ネイティブ VLAN を無効化することが出来ます。

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．ネイティブ VLAN で、tagged フレームを取り扱うため'vlan dot1q tag native'を入力します。

```
switch(config)# vlan dot1q tag native
```

3．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。

```
switch(config)# interface tengigabitethernet 0/19
```

4．DCB インタフェースを有効化するため、'no shutdown'コマンドを実行します。

5．DCB インタフェースをトランクモードとするため、'switchport'コマンドを実行します。

```
switch(conf-if-te-0/19)# switchport
switch(conf-if-te-0/19)# switchport mode trunk
```

6．インタフェースを通して、送受信する VLAN ID を指定します。次の例は、VLAN ID に 30 を設定しています。

```
switch(conf-if-te-0/19)# switchport trunk allowed vlan add 30
```

7．ネイティブ VLAN の VLAN ID を変更するため、'switchport trunk native-vlan *vlan_id* を実行します。先のステップで設定した VLAN ID と同じＩＤを指定します。

```
switch(conf-if-te-0/19)# switchport trunk native-vlan 30
```

15 スパニングツリーの設定

15.1 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、リンク障害によりループが発生する場合があります。

NOTE
Network OS 3.x 以前では、VCS モードで全ての 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+、RPVST+をサポートします。

スパニングツリーが実行中、ネットワークにあるいずれかの LAN からその他の LAN に単一の経路で到達できるよう、ネットワークスイッチは実際のネットワークトポロジをスパニングツリートポロジへ変更します。ネットワークスイッチは、ネットワークトポロジに変更がある度に新しいスパニングツリートポロジを再計算します。

NOTE
スタンドアロンモードで動作しているすべての内蔵 DCB スイッチは、VLAN のループの問題を回避するために xSTP を必要に応じて設定しておく必要があります。

各々の LAN に対して、LAN に接続されたスイッチはルートスイッチに最も近いスイッチである指定スイッチを選択します。指定スイッチは、LAN からまた LAN へ全てのトラフィックを転送する役割を持ちます。LAN に接続された指定スイッチのポートは、指定ポートと呼ばれます。スイッチは、そのポートのどれがスパニングツリートポロジの一部かを決定します。ポートがルートポートか指定ポートならばスパニングツリートポロジに含まれます。
STP を使うと、データトラフィックはスパニングツリートポロジの一部であるポートでのみ転送されます。スパニングツリートポロジの一部ではないポートは、自動的に blocking(無効化)状態に変更されます。それらのポートは、スパニングツリートポロジが壊れ、新しい経路として自動的に有効化されるまで、blocking 状態は維持されます。
STP で動作する全てのレイヤ 2 インタフェースに対する STP インタフェースの状態は下記の通りです。

- Blocking - インタフェースはフレーム転送しません。
- Listening - インタフェースはフレーム転送するポートの一部としてスパニングツリーにより特定されます。これは、Blocking 状態からの遷移状態です。
- Learning-インタフェースは、フレーム転送する準備をします。

- Forwarding - インタフェースはフレーム転送します。
- Disabled - shutdow 設定か未接続かそのポートではスパニングツリーが動作していないために、インタフェースはスパニングツリーに参加していません。

スパニングツリーに参加しているポートは以下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 機能は、STP の構成によく使用されるオプション機能です。
- Root guard - 詳細は 199 ページの『15.6.21 (4)guard root の設定』を参照下さい。
- PortFast BPDU guard と BPDU filter - 詳細は、201 ページの『15.6.21 (8)port fast(STP)の有効化』を参照下さい。

15.2 設定時の注意事項および制約事項

スパニングツリーの設定を行う時は、次のコンフィグレーションの注意事項および制約事項に従ってください。
- xSTP の種類を変更する場合、現在、有効にしている xSTP を無効にする必要があります。
- パラレルリンクの両側に接続されているすべてのデバイス上で xSTP を有効にしてください。そうでない場合、パケットドロップやパケットフラッディングが発生する可能性があります。
- LAG は、通常のリンクとして扱われており、デフォルトで STP が有効になっています。
- 32 個の MSTP インスタンスと一つの MSTP リージョンを持つことができます。
- MSTP インスタンスにマッピングする前に、VLAN を作成してください。
- MSTP force-version オプションは、サポートしていません。
- 誤設定のスパニングツリーが稼働しているローカルエリアネットワークが一つ以上のループを持っている場合、スパニングツリーBPDU(Bridge Protocol Deta Unit)のトラフィックストームが発生する可能性があります。特定の状況でスパニングツリーBPDU を含むトラフィックストームに長期間さらされた時、内蔵 DCB スイッチは、再起動することがあります。
- さらに、誤設定のスパニングツリーが稼働しているローカルエリアネットワークが一つ以上のループを持っている場合、スパニングツリーBPDU のトラフィックストームが発生する可能性があります。エッジループ検出プロトコルは、スパニングツリーBPDU などの制御パケットを伴うトラフィックストーム中でループを排除することはできません。
- ネットワーク内の冗長パスでロードバランシングが機能するためには、すべての VLAN－インスタンスマッピング割り当てが一致している必要があります。そうしないと、すべてのトラフィックが一つのリンク上を流れます。
- 'global protocol spanning-tree mstp'コマンドを用いて MSTP を有効にする時、RSTP は自動的に有効

にされます。

- 同一の MSTP リージョン内に 2 台以上のスイッチが存在するためには、同じ VLAN－インスタンスマッピング、同じコンフィグレーションリビジョン番号、同じ名前を持つ必要があります。

15.3　RSTP 概要

NOTE

RSTP は、STP と互換性と相互接続性をもつように設計されています。しかし、STP が動作しているスイッチと相互接続する場合、RSTP の高速コンバージェンスの利点はなくなります。

IEEE 802.1w 高速スパニングツリー(RSTP)規格は、802.1D STP 規格の発展したものです。RSTP は、スイッチやポートや LAN の障害時に高速再コンバージェンスが可能になります。そして、エッジポートや新しいルートポートや point-to-point で接続されたポートの再構築が可能となります。
RSTP が動作する全てのレイヤ 2 インタフェースの状態は次の通りです。

- Learning - インタフェースはフレーム転送に参加するための準備をします。
- Forwarding - インタフェースはフレーム転送します。
- Discarding - インタフェースはフレームを破棄します。802.1D の disabled, blocking, listening 状態が RSTP の discarding 状態に集約されたことに注意してください。discarding 状態のポートは、有効なトポロジに参加せず、MAC アドレス学習も行いません。

表 15-1 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 15-1　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状態のポートの役割もまた違っています。RSTP はポートの状態とトポロジ内で果たすポートの役割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となり、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対して代替ポートとして動作します。

ルートポートと指定ポートだげが、有効なトポロジの一部となります。代替・バックアップポートは

トポロジに組み込まれません。
ネットワークが安定していると、ルートポートと指定ポートは Forwarding 状態であり、代替ポートとバックアップポートは、Discarding 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 Forwarding 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、184 ページの『15.6 スパニングツリーの構成と管理』を参照下さい。

15.4 MSTP 概要

IEEE802.1s Multiple STP(MSTP)は、単一の物理トポロジ上で多数のループフリーなトポロジの作成を可能とします。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でき、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。

多数のスイッチが複数のスパニングツリーインスタンスに参加するため、同一の MSTP 構成に一貫して構成されなければなりません。同一 MSTP 構成を持って接続されたスイッチのグループは、MSTP リージョンと呼ばれます。

NOTE
32 の MSTP インスタンスと一つの MSTP リージョンをサポートしています。

MSTP はリージョンを使ってスイッチドメインを管理する階層構造を導入しています。共通 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 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。複数のスパニングツリーインスタンスは、MSTP リージョン内で動作し、そのインスタンスにマッピングされている VLAN に対して有効なトポロジを決定する RSTP インスタンスです。全てのリージョンは、リージョン内の全てのスイッチを含むシングルスパニングツリーを形成した common internal spanning tree(CIST)を持っています。CIST インスタンスと MSTP インスタンスの違いは、CIST インスタンスは MSTP リージョンを跨って動作し、リージョンを跨ってループフリーなトポロジを形成しますが、MSTP インスタンスは、一つのリージョン内のみで動作します。CIST インスタンスは、リージョンを跨るスイッチが RSTP をサポートしているなら、RSTP を使って動作します。しかし、幾つかのスイッチが 802.1D STP を使っているなら、CIST

インスタンスは、802.1D に戻ります。各リージョンは、他のリージョンに対して単一の STP か RSTP ブリッジとして論理的に見えます。

15.5　PVST+と Rapid PVST+の概要

一般的に、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、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、全てのブリッジに接続するスパニングツリーはリアルタイムに形成されます。冗長ポートはブロッキング状態(non-forwarding)になります。それらは、必要な時に有効化されます。
ブリッジトポロジに対するスパニングツリーを構築するため、ブリッジは制御フレーム(BPDU)を交換しなければなりません。プロトコルは、BPDU の意味と必要となるステートマシンを定義しています。最初のスパニングツリープロトコル(STP)は IEEE 802.1d 規格の一部になりました。
しかし、STP のコンバージェンス時間はリンク障害時 50 秒です。これは、すぐに受け入れられなくなってきました。STP の主なフレームワークみを維持したまま、ラピッドスパニングツリー(RSTP)の一部として、コンバージェンスを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。
Per-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 Pre-VLAN Spanning Tree+ (RPVST+)と呼ばれます。RPVST+は、スイッチ上の各 VLAN に対するスパニングツリーインスタンスの一つを持ちます。
しかし PVST+は、ネットワーク上に多くの VLAN があると、多くの CPU パワーを消費するので、スケーラブルではありません。両極端な機能である PVTP+と RPVST+の合理的な妥協点は、Multiple Spanning Tree(MSTP)になります。MSTP 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複数インスタンスを動作させることができます。そして、各インスタンスに VLAN の集合を割り当てます。

NOTE
Network OS は、PVST+と RPVST+のみをサポートします。 PVST と RPVST プロトコルは、Cisco 独自のものであり、サポートしていません。

PVST+や RPVST+を構成するために、'protocol spanning-tree pvst'と'protocol spanning-tree rpvst'コマンドを使用します。詳細は、『Network OS Command Reference』を参照下さい。
例えば、下記の手順は VLAN10 に対する PVST+を設定します。

```
switch(config)# protocol spanning-tree pvst
```

```
switch(config-pvst)# bridge-priority 4096
switch(config-pvst)# forward-delay 20
switch(config-pvst)# hello-time 2
switch(config-pvst)# max-age 7
```

15.5.1　PVST+と RPVST+のガイドラインと制限

PVST+と RPVST+を構成するとき、次の事項を考慮してください。

- スタンドアロンモードで STP/RSTP/MSTP を動作させる場合、ネイティブ VLAN のタギングを無効化することが必要です。そうでなければ、PVST+/RPVST+が収束しないで、ネイティブ VLAN 上のループをつくります。タグ付けされたネイティブ VLAN データトラフィックは無視され、ネイティブ VLAN のタグなしデータは転送されます。
- ファブリッククラスタモードのエッジポートでは、ネイティブ VLAN のタギングを無効化が必要です。そうでなければ、PVST+/RPVST+が収束しないで、ネイティブ VLAN 上のループをつくります。タグ付けされたネイティブ VLAN データトラフィックは無視され、ネイティブ VLAN のタグなしデータは転送されます。
- PVST+モードをインタフェースで有効にせずに、VLAN の下で RSTP が有効になっているスイッチ X が接続しているタグ付きポートに同じ VLAN が設定されている場合でも、タグ付きのポートで BPDU は廃棄されます。

15.6　スパニングツリーの構成と管理

本章をご覧になる前に、『15.5.1 PVST+と RPVST+のガイドラインと制限』を参照してください。

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。

15.6.1　デフォルトのスパニングツリー設定

各スパニングツリーのデフォルト設定値を示します。

NOTE
ここで示すデフォルト設定値は、ファームウェアのデフォルト設定にコンフィグレーションを初期化した場合の値であり、工場出荷時の設定とは異なります。工場出荷時の設定は、モジュールもしくは装置付属添付品(添付 CD またはシステム装置内蔵)のコンフィグ情報を参照下さい。

表 15-2 に、STP 構成のデフォルト値を示します。

表 15-2　STP デフォルト構成パラメータ

パラメータ	デフォルト設定
Spanning-tree mode	STP、 RSTP、MSTP が無効(デフォルト)
Bridge priority	32768
Bridge forward delay	15 秒
Bridge maximum aging time	20 秒
Error disable timeout timer	無効
Error disable timeout interval	300 秒
Port-channel path cost	スタンダード
Bridge hello time	2 秒

表 15-3 に、MSPT のみを設定した場合のデフォルト値を示します。

表 15-3　MSTP デフォルト構成パラメータ

パラメータ	デフォルト設定
Cisco interoperability	無効
Switch priority (VLAN を MSTP インスタンスにマッピング時)	32768
Maximum hops	20 hops
Revision number	0

表 15-4 に、10GbE DCB インタフェースのデフォルト値を示します。

表 15-4　10GbE DCB インタフェースデフォルト構成パラメータ

パラメータ	デフォルト設定
Spanning tree	インタフェース上で無効
Automatic edge detection	無効
Path cost	2000
Edge port	無効
Guard root	無効
Hello time	2 秒
Link type	Point-to-point
Port fast	無効
Port priority	128
DCB interface root port	DCB インタフェースがルートポートになることを許可
DCB interface BPDU restriction	制限は無効

15.6.2　STP の設定

STP の設定手順は次の通りです。

1．グローバルコンフィグレーションモードに移行します。

2．'protocol spanning-tree'グローバルコマンドを使って、PVST+を有効化します。詳細は、189 ページの『15.6.5 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、190 ページの『15.6.8 (1)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(config-stp)# bridge-priority 28672
```

4．オプション：'spanning-tree portfast'コマンドを使って、スイッチのポートに PortFast 機能を有効化します。詳細は、201 ページの『15.6.21 (8)port fast(STP)の有効化』を参照下さい。

NOTE

PortFast 機能は、ワークステーションや PC が接続されたポートにのみ有効化される必要があります。ワークステーションや PC が接続された全てのポートにこれらのコマンドを繰り返してください。スイッチが接続されたポートには PortFast 機能を設定してはいけません。

NOTE

トランキングおよび非トランキングモードで、ポート上で Port Fast を有効にすると、一時的なブリッジループを引き起こす可能性があります。

```
switch(config)# interface tengigabitethernet 0/10
switch(conf-if-te-0/10)# spanning-tree portfast
switch(conf-if-te-0/10)# exit
switch(config)# interface tengigabitethernet 0/11
switch(conf-if-te-0/11)# spanning-tree portfast
switch(conf-if-te-0/11)# exit
```

ワークステーションや PC が接続された全てのポートにこれらのコマンドを繰り返してください。

5．オプション：非ブロケード社製スイッチとの相互接続のため、次の'spanning-tree bpdu-mac'コマンドを使ってスイッチと接続したインタフェースを構成する必要があります。

```
switch(config)# interface tengigabitethernet 0/12
switch(conf-if-te-0/12)# spanning-tree bpdu-mac 0100.0ccc.cccd
```

6．次のポートを forwarding モードに設定します。

- ルートスイッチの全てのポート
- ルートポート
- 指定ポート

7．オプション：'spanning-tree guard root'コマンドを使って guard root 機能を設定します。guard root 機能は、ネットワーク中にルートブリッジの位置を強制的に設定する方法です。詳細は、199 ページの『15.6.21 (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、184 ページの『15.6 スパニングツリーの構成と管理』を参照下さい。

15.6.3 RSTP の設定

基本的な RSTP の設定手順は次の通りです。

1．グローバルコンフィグレーションモードに移行します。
2．'protocol spanning-tree'グローバルコマンドを使って、RSTP を有効化します。詳細は、189 ページの『15.6.5 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、190 ページの『15.6.8 (1) 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(config-rstp)# bridge-priority 28672
```
4．'bridge forward delay'を設定します。詳細は、190 ページの『15.6.8 (2)ブリッジ転送遅延時間の指定』を参照してください。
```
switch(config-rstp)# forward-delay 20
```
5．'bridge maximum aging time'を指定します。詳細は、191 ページの『15.6.8 (3)bridge maximum aging time の指定』を参照下さい。
```
switch(config-rstp)# max-age 25
```
6．'error disable timeout timer'を有効にします。詳細は、192 ページの『15.6.9 (1)error disable timeout timer の有効化』を参照下さい。
```
switch(config-rstp)# error-disable-timeout enable
```
7．'error-disable-timeout interval'を設定します。詳細は、193 ページの『15.6.9 (2)error disable timeout interval の指定』を参照下さい。
```
switch(config-rstp)# error-disable-timeout interval 60
```
8．'port-channel path cost'を設定します。詳細は、193 ページの『15.6.10 port-channel path cost の指定』を参照下さい。
```
switch(config-rstp)# port-channel path-cost custom
```
9．'bridge hello time'を設定します。詳細は、192 ページの『15.6.8 (4)bridge hello time の設定』を参照下さい。
```
switch(config-rstp)# hello-time 5
```
10．オプション：'spanning-tree edgeport'コマンドを使って、スイッチのポートに EdgePort 機能を有効化します。詳細は、198 ページの『15.6.21 (3)エッジポートとしてポート(インターフェース)の有効化』を参照下さい。

NOTE
EdgePort 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設定してください。基本的

に、スイッチが接続されたポートには EdgePort 機能を設定してはいけません。

NOTE
トランキングおよび非トランキングモードでポート上の EdgePort を有効にすると、一時的なブリッジループを引き起こす可能性があります。

```
switch(config)# interface tengigabitethernet 0/10
switch(conf-if-te-0/10)# spanning-tree edgeport
switch(conf-if-te-0/10)# exit
switch(config)# interface tengigabitethernet 0/11
switch(conf-if-te-0/11)# spanning-tree edgeport
switch(conf-if-te-0/11)# exit
switch(config)#
```

ワークステーションや PC が接続された全てのポートにこれらのコマンドを繰り返してください。

１１．次のポートを forwarding モードに設定します。

- ルートスイッチの全てのポート
- ルートポート
- 指定ポート

詳細は、201 ページの『15.6.21 (9)ポートプライオリティの指定』を参照下さい。

１２．オプション：'spanning-tree guard root'コマンドを使って guard root 機能を設定します。guard root 機能は、ネットワーク中にルートブリッジの位置を強制的に設定する方法です。詳細は、199 ページの『15.6.21 (4)guard root の設定』を参照下さい。

隣接スイッチやブリッジに接続している他の全てのポートは、自動的に blocking モードになります。これは、ワークステーションや PC と接続しているポートに適用しません。これらのポートは forwarding モードとなります。

１３．特権実行モードに戻ります。

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

１４．running-config file を startup-config file に格納するため、'copy'コマンドを実行します。

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

15.6.4　MSTP の構成

基本的な MSTP の設定手順は次の通りです。

１．グローバルコンフィグレーションモードに移行します。

２．'protocol spanning-tree'グローバルコマンドを使って MSTP を有効にする。詳細は、189 ページの『15.6.5 STP, RSTP, MSTP, PVST の有効化』を参照下さい。

```
switch(config)# protocol spanning-tree mstp
```

３．'region'コマンドを使ってリージョン名称を指定します。更に詳細は、195 ページの『15.6.16 MSTP リージョン名称の指定』を参照下さい。

```
switch(config-mstp)# region brocade1
```

４．'revison'コマンドを使って、レビジョン番号を指定します。更に詳細は、196 ページの『15.6.17 MSTP 構成のレビジョン番号の指定』を参照下さい。

```
switch(config-mstp)# revision 1
```

５．'instance'コマンドを使って、VLAN を MSTP インスタンスに割り当てます。更に詳細は、194 ページの『15.6.14 VLAN の MSTP インスタンスへのマッピング』を参照下さい。

```
switch(config-mstp)# instance 1 vlan 2, 3
switch(config-mstp)# instance 2 vlan 4-6
```

```
switch(config-mstp)# instance 1 priority 4096
```

6．'max-hops'コマンドを使って、インタフェース上にループを防止するために BPDU の最大ホップ数を指定します。更に詳細は、195 ページの『15.6.15 BPDU(MSTP)最大 hop 数の指定』を参照下さい。

```
switch(config-mstp)# max-hops 25
```

7．特権実行モードに戻ります。

```
switch(config-mstp)# end
```

8．running-config file を startup-config file に格納するため、'copy'コマンドを実行します。

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

MSTP に関する更に詳細な情報は、184 ページの『15.6 スパニングツリーの構成と管理』を参照下さい。

15.6.5　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を必要としません。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+, RPVST+を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree rstp
```

15.6.6　STP, RSTP, MSTP, PVST 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+, RPVST+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
```

15.6.7　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+, RPVST+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(config)# protocol spanning-tree rstp
switch(config-mstp)# shutdown
```

15.6.8　ブリッジパラメータの指定

(1) ブリッジプライオリティの指定

STP,RSTP,MSTP のいずれのモードでも、スイッチのプライオリティを指定するには、'bridge-priority' コマンドを使います。ルートスイッチを決定した後、ルートスイッチとして指定するスイッチに適切な値を設定します。もし、スイッチが他の全てのスイッチより低いブリッジプライオリティを持っているなら、他のスイッチはそのスイッチをルートスイッチとして自動的に選択します。

ルートスイッチは、システムの中心に位置づけ、継続不可能なスイッチ構成に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、ネットワーク上の全ての判断は、ルートスイッチの観点から決定されます。

Bridge Protocol Data Units(BPDU)は、スイッチ間で交換される情報を伝達します。ネットワーク上の全てのスイッチの電源が投入されると、ルートスイッチを選択するプロセスが開始されます。各スイッチは、VLAN 毎に直接接続されたスイッチに BPDU を送信します。各スイッチはスイッチが送信した BPDU と受信した BPDU を比較します。ルートスイッチの選択プロセスでは、もしスイッチ２が広告する root ID より低い番号となる root ID をスイッチ１が広告するならば、スイッチ２は root ID を広告するのを停止し、スイッチ１の root ID を受け入れます。最も低いプライオリティをもったスイッチがルートスイッチとなります。

さらに、特定の VLAN のためのブリッジプライオリティを指定することもできます。VLAN パラメータが提供されていない場合、プライオリティの値は、すべての VLAN ごとのインスタンスに対してグローバルに適用されます。しかし、明示的に設定している VLAN では、VLAN 単位の設定は、グローバル設定よりも優先されます。

NOTE

VLAN の値は、1 から 3962 以内で、3963 から 4094 までは、リザーブされています。

ブリッジプライオリティを指定するために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．STP, RSTP, MSTP, PVST+, RPVST+を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree rstp
```

3．ブリッジプライオリティを指定します。範囲は 0 から 61400 までで、値は 4096 単位でのみ設定できます。デフォルトは、32678 です。

```
switch(config-stp)# bridge-priority 20480
```

4．オプション：特定の VLAN のブリッジプライオリティを指定します。

```
switch(config)# protocol spanning-tree rpvst
switch(config-rpvst)# vlan 10 bridge-priority 20480
```

(2) ブリッジ転送遅延時間の指定

STP,RSTP,MSTP のいずれのモードでも、全てのスパニングツリーインスタンスで forwarding 状態とな

るまでの listening 及び learning 状態をどのくらい維持するかを指定するためにこのコマンドを使います。範囲は、4 から 30 秒です。デフォルト 15 秒です。次の関係が維持される必要があります。

```
2*(forward_delay - 1)>=max_age>=2*(hello_time + 1)
```

さらに、特定の VLAN のための転送遅延を指定することもできます。VLAN パラメータが提供されていない場合、プライオリティの値は、すべての VLAN 毎のインスタンスに対してグローバルに適用されます。しかし、明示的に設定している VLAN では、VLAN 単位の設定がグローバル設定よりも優先されます。

VLAN の値は、1 から 3962 以内で、3963 から 4094 までは、リザーブされています。

ブリッジ転送遅延を指定するために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．STP, RSTP, MSTP, PVST+, RPVST+を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree stp
```

3．ブリッジ転送遅延を指定します。

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

4．オプション：特定の VLAN のためのブリッジ転送遅延を指定します。

```
switch(config)# protocol spanning-tree pvst
switch(config-pvst)# vlan 10 forward-delay 20
```

(3) bridge maximum aging time の指定

STP,RSTP,MSTP のいずれのモードでも、インターフェースに Bridge Protocol Data Unit (BPDU)構成情報を格納する前に経過する最大時間を制御するために、このコマンドを使用します。"maximum aging time"を設定する場合、max-age は hello-time より大きくなければなりません。この範囲は、6 から 40 秒で、デフォルトは、20 秒です。次の関係を維持しなければなりません。

```
2*(forward_delay - 1)>=max_age>=2*(hello_time + 1)
```

さらに、特定の VLAN に対して maximum age を指定することもできます。VLAN パラメータが提供されていない場合、プライオリティの値は、すべての VLAN インスタンスに対してグローバルに適用されます。しかし、明示的に設定している VLAN では、VLAN 単位の設定がグローバル設定よりも優先されます。

VLAN の値は、1 から 3962 以内で、3963 から 4094 までは、リザーブされています。

"bridge maximum aging time"を指定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．STP, RSTP, MSTP, PVST+, RPVST+を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree stp
```

3．bridge maximum aging time を指定します。

```
switch(config-stp)# max-age 25
```

4．オプション：特定の VLAN のための bridge maximum aging time を指定します。

```
switch(config)# protocol spanning-tree pvst
switch(config-pvst)# vlan 10 max-age 25
```

(4) 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 秒です。デフォルトは 2 秒です。

'hello-time'を設定する場合、'max-age'設定が'hello-time'設定より大きくなければなりません。次の関係が維持される必要があります。

```
2*(forward_delay - 1)>=max_age>=2*(hello_time + 1)
```

さらに、特定の VLAN に対して'hello-time'を指定することもできます。VLAN パラメータが提供されていない場合、プライオリティの値は、すべての VLAN インスタンスに対してグローバルに適用されます。しかし、明示的に設定している VLAN では、VLAN 単位の設定がグローバル設定よりも優先されます。VLAN の値は、1 から 3962 以内で、3963 から 4094 までは、リザーブされています。

"bridge hello time"を設定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．STP, RSTP, MSTP, PVST+, RPVST+を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree stp
```

3．インタフェースで'hello BPDU'の送信間隔を秒単位で指定します。

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

4．オプション：特定の VLAN のための"hello BPDU"の送信間隔を秒単位で指定します。

```
switch(config)# protocol spanning-tree pvst
switch(config-pvst)# vlan 10 hello-time 5
```

5．特権実行モードに戻ります。

```
switch(config-pvst)# 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
```

15.6.9　ＳＴＰタイマの設定

(1) error disable timeout timer の有効化

STP,RSTP,MSTP のいずれのモードでも、ポートを無効状態にするまでのタイマーを有効にするため、このコマンドを使用します。'STP BPDU guard'によりポートが無効にされている時、ポートを手動で有効にしなければ、ポートは無効のままです。このコマンドにより、ポートを無効状態から有効化することができます。'error disable timeout interval'設定の詳細については、193 ページの『15.6.9 (2) error disable timeout interval の指定』を参照下さい。

'error disable timeout timer'を設定するため、特権実行モードで次の手順を実行します。デフォルトでは、タイムアウト機能は無効です。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．STP, RSTP, MSTP, PVST+, RPVST+を有効にするため、'protocol'コマンドを入力してください。

```
witch(config)# protocol spanning-tree stp
```

3．'error disable timeout timer'を有効化します。

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

(2) error disable timeout interval の指定

STP,RSTP,MSTP のいずれのモードでも、インタフェースの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には、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．STP, RSTP, MSTP, PVST+, RPVST+を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree 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(config-stp)# error-disable-timeout interval 60
```

15.6.10 port-channel path cost の指定

STP,RSTP,MSTP のいずれのモードでも、port-channel path cost を指定するためにこのコマンドを使用します。デフォルトのコストは、"standard"です。パスコストのオプションは次の通りです。

- custom - port-channel の帯域に沿ってパスコストを変更する場合指定します。
- standard - port-channel の帯域に沿ってパスコストを変更しない場合指定します。

'port-channel path cost'を指定するために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．STP, RSTP, MSTP, PVST+, RPVST+を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree stp
```

3．'port-channel path cost'を指定します。

```
switch(config-stp)# port-channel path-cost custom
```

4．特権実行モードに戻ります。

```
switch(configig-stp)# 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
```

15.6.11 transmit hold count (RSTP、MSTP、RPVST+)の設定

RSTP と MSTP モードで、'transmit hold count'を使って BPDU のバーストサイズを設定することができます。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 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． RSTP, MSTP, RPVST+を有効にするため、'protocol'コマンドを入力してください。
```
switch(config)# protocol spanning-tree rstp
```
3．'transmit hold count'を指定します。
```
switch(config-rstp)# transmit-holdcount 5
```
4．特権実行モードに戻ります。
```
switch(config-rstp)# 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
```

15.6.12 Cisco 相互接続性(MSTP)の設定

MSTP モードで、いくつかの Cisco スイッチとの相互接続の機能を有効にしたり無効にしたりするために、'cisco-interoperability'コマンドを使います。もし、Cisco 相互接続性がネットワークでいずれかのスイッチに必要となった場合、そしてネットワーク上の全てのスイッチに互換性が必要となった場合、このコマンドを使って有効化します。デフォルトでは Cisco 相互接続性は無効となっています。

NOTE

このコマンドは、幾つかの旧式の Cisco スイッチの MSTP BPDU にある"version 3 length"が、現在の規格に適合しないために必要となります。

ある旧式の Cisco スイッチとの相互接続性を有効化するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．MSTP を有効にするため、'protocol'コマンドを入力してください。
```
switch(config)# protocol spanning-tree mstp
```
3．Cisco 相互接続性を有効にします。
```
switch(config-mstp)# cisco-interoperability enable
```

15.6.13 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-mstp)# protocol spanning-tree mstp
```
3．Cisco 相互接続性を無効にします。
```
switch(config-mstp)# cisco-interoperability disable
```

15.6.14 VLAN の MSTP インスタンスへのマッピング

MSTP モードで、VLAN を MSTP インスタンスへマッピングするために、'instance'コマンドを使用します。インスタンスに VLAN の設定をグループ化することができます。このコマンドは VLAN が生成された後にのみ使用することができます。VLAN インスタンスマッピングは、基礎となる VLAN が削除されるとコンフィグレーションから削除されます。

VLAN を MSTP インスタンスにマッピングするために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．MSTP を有効にするため、'protocol'コマンドを入力してください。
```
switch(config)# protocol spanning-tree mstp
```
3．VLAN を MSTP インスタンスにマッピングします。
```
switch(config-mstp)# instance 5 vlan 300
```
4．特権実行モードに戻ります。
```
switch(config-mstp)# 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
```

15.6.15 BPDU(MSTP)最大 hop 数の指定

MSTP モードで、MSTP リージョンでの BPDU の最大 hop 数を設定するためにこのコマンドを使用します。BPDU の最大 hop 数を指定することは、インタフェースでのループ発生を回避することになります。hop 数を変更すると、全てのスパニングツリーインスタンスに影響です。範囲は、1 から 40 です。デフォルトは 20 です。

MSTP リージョンでの BPDU 最大 hop 数を設定するため、特権実行モードで次の手順を実行します。
1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．MSTP を有効にするため、'protocol'コマンドを入力してください。
```
switch(config)# protocol spanning-tree mstp
```
3．MSTP 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(config-mstp)# max-hops 20
```
4．特権実行モードに戻ります。
```
switch(configig-mstp)# 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
```

15.6.16 MSTP リージョン名称の指定

MSTP モードで、MSTP リージョン名称を割り当てるためこのコマンドを使用します。リージョン名称は、最大 32 文字で大文字小文字を識別します。

MSTP リージョン名を設定するため、特権実行モードで次の手順を実行します。
1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．MSTP を有効にするため、'protocol'コマンドを入力してください。
```
switch(config)# protocol spanning-tree mstp
```
3．MSTP リージョン名称を設定するため、'region'コマンドを入力します。
```
switch(config-mstp)# region Sydney
```
4．特権実行モードに戻ります。
```
switch(config-mstp)# 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
```

15.6.17 MSTP 構成のレビジョン番号の指定

MSTP モードで、MSTP 構成のレビジョン番号を指定するためこのコマンドを使用します。範囲は、0 から 255 です。デフォルトは 0 です。

MSTP 構成のレビジョン番号を指定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．MSTP を有効にするため、'protocol'コマンドを入力してください。

```
switch(config)# protocol spanning-tree mstp
```

3．MSTP 構成のレビジョン番号を指定するため、'revision'コマンドを入力します。

```
switch(config-mstp)# revision 17
```

4．特権実行モードに戻ります。

```
switch(config-mstp)# 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
```

15.6.18 スパニングツリーカウンタのクリア

特権実行モードで、全てのまたは指定したインタフェースのスパニングツリーカウンターをクリアするためこのコマンドを使用します。

スパニングツリーカウンタをクリアするため、特権実行モードで次の手順を実行します。

1．全てのインタフェースの全てのスパニングツリーカウンターをクリアするために、'clear'コマンドを使います。

```
switch# clear spanning-tree counter
```

2．指定した port-channel や DCB ポートインタフェースに関連したスパニングツリーカウンターをクリアするために、'clear'コマンドを使います。

```
switch# clear spanning-tree counter interface tengigabitethernet 0/1
```

15.6.19 スパニングツリー検出プロトコルのクリア

特権実行モードで、全てのインタフェースや特定のインタフェースにおいて、隣接スイッチと強制的に再ネゴシエーションを行うようプロトコルマイグレーションプロセスをリスタートします。

プロトコルマイグレーションプロセスをリスタートするために、特権実行モードで次の手順を実行します。

1．全てのインタフェースの全てのスパニングツリー検出プロトコルをクリアするために、'clear'コマンドを使います。

```
switch# clear spanning-tree detected-protocols
```

2．指定した port-channel や DCB ポートインタフェースに関連したスパニングツリー検出プロトコルをクリアするために、'clear'コマンドを使います。

```
switch# clear spanning-tree detected-protocols interface tengigabitethernet 0/1
```

15.6.20 STP 関連情報の表示

STP, RSTP, MSTP, PVST+, RPVST+関連の全ての情報を表示するために、特権実行モードで'show spanning tree brief'コマンドを入力します。

NOTE

'root guard'が働いた場合、'show spanning-tree brief'コマンド出力は、ポート状態を ERR と表示します。

15.6.21 DCB インタフェースポート毎の STP, RSTP, MSTP の設定

この章では、10 ギガビットイーサネットの DCB インタフェースポート毎に STP, RSTP, MSTP を有効、設定するためのコマンドを詳細に説明します。

NOTE

NOS v3.0.0 以前のバージョンは、VCS モードで、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+, RPVST+をサポートしています。

(1) 自動エッジ検出機能の有効化

DCB インタフェースで、エッジポートを自動的に有効にするために、このコマンドを使用します。ポートは、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。

自動エッジ検出機能を有効化するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。

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

3．DCB インタフェースを有効化するため、'no shutdown'コマンドを入力します。

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

4．DCB インタフェースに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
```

NOTE

NOS v3.0.0 では、自動エッジ検出機能(“spanning-tree autoedge”オプション)は、未サポートです。ポートの接続先ネットワークに、ループがないことが確実な場合は、“spanning-tree edgeport” オプションを設定してください。

(2) パスコストの設定

DCB 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、このコマンドを使用します。より小さいパスコストにより、インタフェースが root となる可能性が高くなります。範囲は、1 から 200000000 です。デフォルトのパスコストは、10G インタフェースのための 2000 です。さらに、特定の VLAN のためのスパニングツリーコストを指定することもできます。VLAN パラメータが提供されていない場合、プライオリティの値は、すべての VLAN インスタンスに対してグローバルに適用されます。しかし、明示的に設定している VLAN では、VLAN 単位の設定がグローバル設定よりも優先されます。

VLAN の値は、1 から 3962 以内で、3963 から 4094 までは、リザーブされています。

インタフェースにスパニングツリー計算のためのパスコストを設定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。

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

2．DCB インタフェースを有効化するため、'no shutdown'コマンドを入力します。

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

3．DCB インタフェースでのスパニングツリー計算のためのパスコストを設定するため'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)# spanning-tree cost 10000
```

4．オプション：特定の VLAN のためのパスコストを設定するには、'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)#spanning-tree vlan 10 cost 10000
```

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
```

(3) エッジポートとしてポート(インターフェース)の有効化

DCB インタフェースに、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には、次のガイドラインに従ってください。

- BPDU を受信しなければエッジポートとなります。
- エッジポートで BPDU を受信すれば、通常のスパニングツリーポートとなり、エッジポートとはなりません。
- ネットワークでループを生成することが無いエンドステーションと直接接続しているポートなので、エッジポートは直接 Forwarding 状態となり、Listening/Learning 状態をスキップします。
- このコマンドは、RSTP と MSTP でサポートされます。STP に対しては、'spanning-tree portfast'コマンドを使用してください。(201 ページの『15.6.21 (8)port fast(STP)の有効化』を参照下さい。)

DCB インタフェースをエッジポートに指定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。
```
switch(config)# interface tengigabitethernet 0/1
```
3．DCB インタフェースを有効化するため、'no shutdown'コマンドを入力します。
```
switch(conf-if-te-0/1)# no shutdown
```
4．DCB インタフェースをエッジポートに指定するため'spanning-tree'コマンドを入力します。
```
switch(conf-if-te-0/1)# spanning-tree edgeport
```

(4) guard root の設定

DCB インタフェースで、スイッチに guard root を有効化するため、このコマンドを使用します。guard root は、ネットワーク上にルートブリッジを強制的に配置する方法を提供します。インタフェースに設定された guard root で、スイッチはいずれ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を許容されるかを制限することができます。ルートポートは、ルートスイッチへの最短パスを提供します。デフォルトでは、guard root は無効です。

guard root は、悪意のある攻撃や、ルートブリッジにするつもりの無いブリッジデバイスがルートブリッジになるような意図しない誤設定からルートブリッジを保護します。これは、データパスでは致命的なボトルネックとなります。guard root は、有効化されたポートが指定ポートであることを保証します。もし、guard root が設定されたポートが、高優先度の BPDU を受信すると、Discarding 状態となります。

さらに、特定の VLAN のための guard root を指定することもできます。VLAN パラメータが提供されていない場合、プライオリティの値は、すべての VLAN ごとのインスタンスに対してグローバルに適用されます。しかし、明示的に設定している VLAN では、VLAN 単位の設定がグローバル設定よりも優先されます。

VLAN の値は、1 から 3962 以内で、3963 から 4094 までは、リザーブされています。

DCB インタフェースに guard root を設定するために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。
```
switch(config)# interface tengigabitethernet 0/1
```
3．DCB インタフェースを有効化するため、'no shutdown'コマンドを入力します。
```
switch(conf-if-te-0/1)# no shutdown
```
4．DCB インタフェースに guard root を有効にするため、'spanning-tree'コマンドを入力します。
```
switch(conf-if-te-0/1)# spanning-tree guard root
```
5．VLAN のための guard root を有効にするため、'spanning-tree'コマンドを入力します。
```
switch(conf-if-te-0/1)# spanning-tree vlan 10 guard root
```

(5) MSTP hello time の設定

DCB インタフェースで、ルートスイッチからの BPDU の送信間隔を設定するため、このコマンドを使用します。hello-time の変更は、全てのスパニングツリーインスタンスに影響します。'max-age'は、

'hello-time'より大きくなければなりません。(191 ページの『15.6.8 (3)bridge maximum aging time の指定』を参照ください。)範囲は、1 から 10 秒です。デフォルトは、2 秒です。

DCB インタフェースに MSTP hello time を設定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。
```
switch(config)# interface tengigabitethernet 0/1
```
3．DCB インタフェースを有効化するため、'no shutdown'コマンドを入力します。
```
switch(conf-if-te-0/1)# no shutdown
```
4．DCB インタフェースに hello time を設定するため'spanning-tree'コマンドを入力します。
```
switch(conf-if-te-0/1)# spanning-tree hello-time 5
```
5．特権実行モードに戻ります。
```
switch(conf-if-te-0/1)# end
```
6．running-config file を startup-config file に格納するため、'copy'コマンドを実行します。
```
switch# copy running-config startup-config
```

(6) MSTP インスタンスの制限の指定

DCB インタフェースで、MSTP インスタンスの制限を指定するため、このコマンドを使用します。

DCB インタフェースに MSTP インスタンスの制限を指定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。
```
switch(config)# interface tengigabitethernet 0/1
```
3．DCB インタフェースを有効化するため、'no shutdown'コマンドを入力します。
```
switch(conf-if-te-0/1)# no shutdown
```
4．DCB インタフェースに制限を設定するため、'spanning-tree'コマンドを入力します。
```
switch(conf-if-te-0/1)# spanning-tree instance 5 restricted-tcn
```
5．特権実行モードに戻ります。
```
switch(conf-if-te-0/1)# end
```
6．running-config file を startup-config file に格納するため、'copy'コマンドを実行します。
```
switch# copy running-config startup-config
```

(7) リンクタイプの指定

DCB インタフェースに、リンクタイプを指定するためこのコマンドを使用します。"point-to-point"を指定すると、高速スパニングツリーが Forwarding 状態に遷移することを有効化します。"shared"を指定すると、高速スパニングツリーの遷移を無効にします。

DCB インタフェースにリンクタイプを指定するために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力し

ます。

2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。

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

3．DCB インタフェースのリンクタイプを有効にするため、'no shutdown'コマンドを入力します。

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

4．DCB インタフェースに制限を設定するため'spanning-tree'コマンドを入力します。

```
switch(conf-if-te-0/1)# spanning-tree link-type shared
```

(8) port fast(STP)の有効化

DCB インタフェースで、高速に Forwarding 状態に遷移することを可能とする"port fast"を有効化するため、このコマンドを使用します。"port fast"は、標準の forward time を待つことなく、インタフェースを即座に Forwarding 状態にします。

NOTE

もし、"portfast bpdu-guard"オプションがインタフェースで有効になっており BPDU を受信した場合、インタフェースは無効化され"ERR_DISABLE"状態にします。

NOTE

トランキングおよび非トランキングモードでは、ポート上で Port Fast を有効にすると、一時的なブリッジループを引き起こす可能性があります。

MSTP と RSTP には'spanning-tree edgeport'コマンドを使用下さい。(198 ページの『15.6.21 (3) エッジポートとしてポート(インターフェース)の有効化』を参照下さい。)

インタフェースで、STP の"port fast"を有効にするため、特権モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。

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

3．DCB インタフェースを有効に設定するため、'no shutdown'コマンドを入力します。

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

4．DCB インタフェースの"port fast"を有効にするため'spanning-tree'コマンドを入力します。

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

(9) ポートプライオリティの指定

DCB インタフェースに、ポートプライオリティを指定するために、このコマンドを使用します。範囲は、0 から 240 で、16 単位で指定します。デフォルトは 128 です。

さらに、特定の VLAN のためのスパニングツリープライオリティを指定することもできます。VLAN パラメータが提供されていない場合、プライオリティの値は、すべての VLAN ごとのインスタンスに対してグローバルに適用されます。しかし、明示的に設定している VLAN では、VLAN 単位の設定がグローバル設定よりも優先されます。

VLAN の値は、1 から 3962 以内で、3963 から 4094 までは、リザーブされています。

DCB インタフェースにポートプライオリティを設定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定して、'interface'コマンドを入力します。
```
switch(config)# interface tengigabitethernet 0/1
```
3．DCB インタフェースを有効にするため、'no shutdown'コマンドを入力します。
```
switch(conf-if-te-0/1)# no shutdown
```
4．DCB インタフェースにポートプライオリティ設定するため、'spanning-tree'コマンドを入力します。
```
switch(conf-if-te-0/1)# spanning-tree priority 32
```

(10)ルートポート遷移の抑止
DCB インタフェースで、ポートのルートポートへの遷移を抑止するためこのコマンドを使用します。デフォルトは、DCB インタフェースがルートポートに遷移できます。

ポートがルートポートに遷移することを抑止するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。
```
switch(config)# interface tengigabitethernet 0/1
```
3．DCB インタフェースを有効にするため、'no shutdown'コマンドを入力します。
```
switch(conf-if-te-0/1)# no shutdown
```
4．ポートがルートポートに遷移することを抑止するため'spanning-tree'コマンドを入力します。
```
switch(conf-if-te-0/1)# spanning-tree restricted-role
```

(11)トポロジチェンジ通知の抑止
DCB インタフェースで、トポロジチェンジ通知 BPDU の送信を抑止するためにこのコマンドを使用します。デフォルトでは、抑止しません。

トポロジチェンジ通知 BPDU の送信を抑止するために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。
```
switch(config)# interface tengigabitethernet 0/1
```
3．DCB インタフェースを有効にするため、'no shutdown'コマンドを入力します。
```
switch(conf-if-te-0/1)# no shutdown
```
4．トポロジチェンジ通知 BPDU の送信を抑止するため'spanning-tree'コマンドを入力します。
```
switch(conf-if-te-0/1)#spanning-tree restricted-tcn
```

(12) スパニングツリーの有効化

DCB インタフェースで、スパニングツリーを有効化するために、このコマンドを使います。デフォルトでは、スパニングツリーは有効です。

スパニングツリーを有効化するため特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。
```
switch(config)# interface tengigabitethernet 0/1
```
3．DCB イインタフェースを有効にするため、'no shutdown'コマンドを入力します。
```
switch(conf-if-te-0/1)# no shutdown
```
4．スパニングツリーを有効化するため'spanning-tree'コマンドを入力します。
```
switch(conf-if-te-0/1)# no spanning-tree shutdown
```

(13) スパニングツリーの無効化

DCB インタフェースで、スパニングツリーを無効化するために、このコマンドを使います。デフォルトでは、スパニングツリーは有効です。

スパニングツリーを無効化するため特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定して'interface'コマンドを入力します。
```
switch(config)# interface tengigabitethernet 0/1
```
3．DCB イインタフェースを有効にするため、'no shutdown'コマンドを入力します。
```
switch(conf-if-te-0/1)# no shutdown
```
4．スパニングツリーを無効化するため'spanning-tree'コマンドを入力します。
```
switch(conf-if-te-0/1)# spanning-tree shutdown
```

NOTE

インタフェースでスパニングツリーが無効化された状態で、インタフェース自身も shutdown 定義されている場合、’`show spanning-tree interface`’での protocol 表示が正しくない場合があります。

---

16 リンクアグリゲーションの設定

16.1 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ても、他のリンクはアップしたまま通信が途絶えません。
リンクを LAG に設定するため、物理リンクは同じスピードでなければならず、全てのリンクは同じ隣接デバイスと接続される必要があります。リンクアグリゲーションは、手動で LAG を構成したり、IEEE802.3ad の Link Aggregation Control Protocol (LACP)を使って動的に構成する方法があります。
複数の入力ソースからのトラフィックが同じ出力ポートにキューイングされると、入力ソースが単一の物理リンクか、または、複数のメンバーリンクを持つトランクであるかにかかわらず、すべての入力ソースに同じ重みが与えられます。

NOTE
LAG と LAG インタフェースはポートチャネル(port-channel)とも呼びます。

リンクアグリゲーションの利点を下記にまとめます。

- 帯域の増加(論理帯域は要求に応じて動的に変化します。)
- アベイラビリティの向上
- 負荷分割
- 高速な構成設定と再構成

本スイッチは、次のトランクタイプをサポートしています。

- 静的な標準 LAG
- LACP を使用した動的な標準ベースの LAG
- 静的な Brocade 独自 LAG
- LACP 拡張機能を使用した Brocade 独自の動的な LAG

16.1.1 リンクアグリゲーショングループの設定

内蔵 DCB スイッチでは標準 LAG として 16 リンクまでの LAG を最大 24 まで設定できます。各 LAG はアグリゲータと関連付けられています。アグリゲータはイーサネットフレームの収集と分配機能を管理します。
各ポートでのリンクアグリゲーションは次の制御を行います。

- ポートアグリゲーションを制御するための構成情報の維持
- LAG で接続した他のデバイスとの構成情報の交換

- ポートが LAG に参加・離脱した場合のアグリゲータへの追加と切り離し
- アグリゲータのフレーム収集と分配機能の有効化・無効化

内蔵 DCB スイッチでの各リンクは、一つの LAG に関連付けることがはできますが、二つ以上の LAG とは関連付けられません。LAG へのリンクの追加・削除は静的、動的、LACP を介して制御できます。各 LAG は次のコンポーネントから構成されます。

- LAG に含まれる個々のリンクの MAC アドレスとは異なる MAC アドレス
- 隣接デバイスとの接続を識別するための各リンクに対するインタフェース番号
- 各リンクに対する管理キー。同じ管理キーを持つリンクだけが同一 LAG に結合されます。LACP を使って構成された各リンク上では、LACP が自動的に port-channnel 識別番号と同じ管理キーを構成します。

16.1.2　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内の物理リンクの属性を自動的に調整するための IEEE802.3ad で規定される標準のプロトコルです。LACPはリンクがLAGに結合できるかどうかを自動的に決定します。もし、リンクが LAG に結合できる場合は、LACP はリンクを LAG にまとめます。LAG の全てのリンクは同一の管理特性を持ちます。LACP は２つのモードで動作します。

- パッシブモード
  LACP は、パートナーシステムからの Link Aggregation Control Protocol Data Unit (LACPDU)に応答しますが、LACPDU の交換はしません。
- アクティブモード
  LACP は、パートナーシステムからの LACPDU 送信に係らず LACPDU を交換します。

16.1.3　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。

16.1.4　静的リンクアグリゲーション

静的リンクアグリゲーションでは、リンクはパートナーシステム間で LACPDU を交換することなく LAG にリンクが追加されます。静的リンクでのフレームの収集・分配はリンクの動作状態や管理状態により決定されます。

NOTE
ポートチャネルを shutdown して reload など装置の再起動をしないで下さい。物理リンクとの状態不整合となり、通信エラーとなります。閉塞する場合は、ポートチャネルのメンバの物理リンクを shutdown してください。

16.1.5　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ますが、トラフィックを分散する方法が異なります。それには、アグリゲートされる前にリンクメンバーで追加されるルールを合わせておかなければなません。

- 最も重要なルールは、リンクメンバ間のファイバ長に大きな差が無いことであり、すべてのメンバーは同じ port-group の一部であることである。(内蔵 DCB スイッチではアップリンクポートとサーバ接続ポートは同一 port-group ではありません。)
- 最大で port-group 当たり 4 つの Brocade LAG を生成することが出来ます。

16.1.6　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に関連しています。収集と分配プロセスは次が保証されなければなりません。

- 制御用 PDU の挿入と監視
- 制御用通信の特定リンクへの制限
- 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

16.2　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 ファブリックが複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 の全てのノードで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。

16.2.1　vLAG の構成

Network OS は、ポートチャネルでの通信速度を 1 Gbps または 10 Gbps に設定するため、speed オプションをサポートしています。デフォルトは 10 Gbps です。ポートチャネルが 1 Gbps である場合、そのスピードは、ポートチャネルを有効にする前に設定する必要があります。そうでない場合、スピード不一致のため LAG/vLAG は構成されません。
'speed'コマンドについては、『Network OS Command Reference』を参照してください。

NOTE
DCB 機能は、vLAG ではサポートされていません。

---

vLAG 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、204 ページの『16.1.1 リンクアグリゲーショングループの設定』を参照下さい。VCS ファブリックが多数のスイッチ間で LAG 構成が定義されていることを検出すると、LAG は自動的に vLAG になります。

```
switch(config)# interface port-channel 27
```

2．特権実行モードに戻るため、'end'コマンドを使います。

```
switch(config-Port-channel-27)# end
```

3．ポートチャネルの詳細を確認するために'show'コマンドを使います。

```
switch# show port-channel detail
LACP Aggregator: Po 27 (vLAG)
 Aggregator type: Standard
 Ignore-split is enabled
  Member rbridges:
    rbridge-id: 1 (1)
    rbridge-id: 231 (4)
  Actor System ID - 0x8000,01-e0-52-00-00-01
  Admin Key: 0027 - Oper Key 0027
  Receive link count: 4 - Transmit link count: 4
  Individual: 0 - Ready: 1
  Partner System ID - 0x8000,00-05-33-a4-e3-33
  Partner Oper Key 0027
 Member ports on rbridge-id 231:
   Link: Te 231/0/2 (0xE718010001) sync: 1
   Link: Te 231/0/3 (0xE718018002) sync: 1   *
   Link: Te 231/0/6 (0xE718030005) sync: 1
   Link: Te 231/0/7 (0xE718038006) sync: 1
```

4．ポートチャネルインタフェースの詳細を確認するため'show'コマンドを使います。

```
switch# show port port-channel tengigabitethernet 1/0/3
 LACP link info: te231/0/3 - 0xE718018002
 Actor System ID: 0x8000,01-e0-52-00-00-01
 Partner System ID: 0x8000,00-05-33-a4-e3-33
 Actor port priority: 0x8000 (32768)
 Admin key: 0x001b (27) Oper key: 0x001b (27)
 Receive machine state : Current
 Periodic Transmission machine state : Slow periodic
 Mux machine state : Collecting/Distributing
 Admin state: ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
```

```
Oper state: ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Partner oper state: ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Partner oper port: 2
Selected: :1
Defaulted State Action: No Default-Up
```

16.2.2　vLAG 分割を無視する設定

'vlag ignore-split'コマンドは、LACP ベース vLAG 用です。本コマンドは、LACP ベースの v LAG ごとに設定できます。vLAG が二つ以上のノードにまたがるシナリオでは、vLAG のノードのいずれかがダウン状態になる場合にパケット損失の程度を最小限に抑えることができ、vLAG フェイルオーバーによるダウンタイムを低減することができます。

ノード間の接続がファブリック分割のために失われた場合(vLAG メンバの一つがダウン状態になるのとは対照的に)、マルチキャスト/ブロードキャストパケットの重複があります。個々のリンクが一点故障とならないよう、ファブリック内の冗長性を構築することをお勧めします。

図 16-1 は、RB2、RB3、RB4 の 3 つのリンクを持った二重の vLAG 構成を示します。Host-1 が Host-2 または Host3 と通信している最中に RB2、RB3、RB4 のいずれかが再起動すると、瞬間的なトラフィックの中断が発生することがあります。

NOTE

'ignore-split が有効な場合、サーバからのトラフィック送出が早いと VLAG ノードの再起動により 1 秒以上通信が途絶える可能性があります。

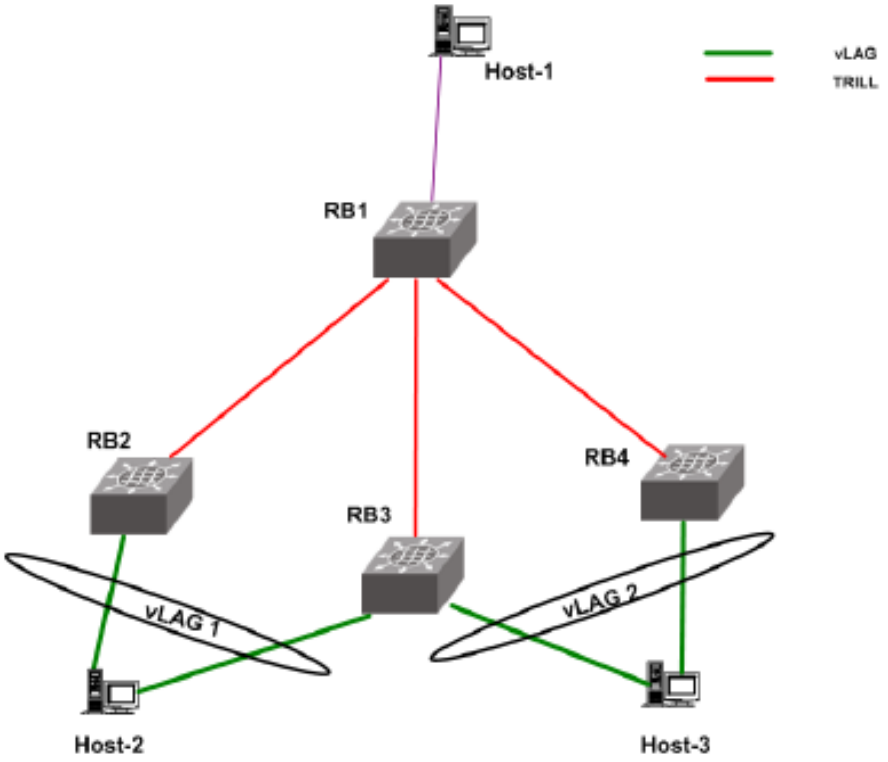

図 16-1　ignore split の VLAG 設定

vLAG フェイルオーバーダウンタイムを減らすために、vLAG でリンク(この場合は RB2、RB3、及び RB4)

の全てに ignore split を設定する必要があります。
'vLAG ignore split'を設定するには、グローバルコンフィグレーションモードで次の手順を実行します。

1．RB2 にログインします。
2．ポートチャネル１にアクセスします。
```
switch(config)# interface port-channel 1
```
3．'vLAG ignore split'を有効にします。
```
switch(config-Port-channel-1)# vlag ignore-split
```
4．RB3 にログインします。
5．ポートチャネル１にアクセスします。
```
switch(config)# interface port-channel 1
```
6．'vLAG ignore split'を有効にします。
```
switch(config-Port-channel-1)# vlag ignore-split
```
7．ポートチャネル２にアクセスします。
```
switch(config)# interface port-channel 2
```
8．'vLAG ignore split'を有効にします。
```
switch(config-Port-channel-2)# vlag ignore-split
```
9．RB4 にログインします。
１０．ポートチャネル２にアクセスします。
```
switch(config)# interface port-channel 2
```
１１．'vLAG ignore split'を有効にします。
```
switch(config-Port-channel-2)# vlag ignore-split
```

16.2.3　リモート RBridge 上のロードバランスの設定

vLAG にトラフィックを転送する際、vLAG のメンバーを持つリモート RBridge で、ロードバランシング機能を設定することができます。vLAG を構成するパスにトラフィックを分散するには、RB2,RB3,RB4 に'lag-load-balancing'を設定します。利用できる条件特性を、表 16-1 に示します。

表 16-1　ロードバランス条件

パラメータ	詳細条件
dst-mac-vid	宛先 MAC アドレスと VID ベースのロードバランシング
dst-mac-vid	送信元 MAC アドレスと VID ベースのロードバランシング
src-dst-mac-vid	送信元および宛先 MAC アドレスと VID ベースのロードバランシング
src-dst-ip	発信元と宛先の IP アドレスベースのロードバランシング
src-dst-ip-mac-vid	送信元と宛先の IP アドレス、MAC アドレスおよび VID ベースのロードバランシング。
src-dst-ip-port	発信元と宛先の IP アドレスと TCP / UDP ポートベースのロードバランシング
src-dst-ip-mac-vid-port	送信元と宛先の IP アドレス、MAC アドレス、VID および TCP / UDP ポートベースのロードバランシング。

さらに、クラスタ内に存在する異なる vLAG には、異なる条件を設定することができます。この条件は、

各 RBridge と各 vLAG 単位に有効にできるので、異なる vLAG のトラフィック毎に異なる load-balance 条件を設定することができます。'show running-config rbridge-id <rbridgeID>'コマンドは、コンフィグレーション情報を表示します。

次の例では、"宛先 MAC アドレスと VID ベースのロードバランシング"の条件を設定します。

```
switch(config)# rbridge-id 2
switch(config-rbridge-id-2)# fabric port-channel 20 load-balance dst-mac-vid
switch(config-rbridge-id-2)# end
switch# show running-config rbridge-id 2
rbridge-id 2
interface-nodespecific ns-vlan 10
interface-nodespecific ns-ethernet 100
fabric vlag 10 load-balance src-dst-mac-vid
fabric vlag 20 load-balance dst-mac-vid
no protocol vrrp
switch# show fabric port-channel load-balance 10
Fabric Vlag Load-Balance Information
------------------------------
Rbridge-Id : 2
Vlag : 10
Load-Balance Flavor : Source and Destination MAC address and VID based load
balancing
switch# show fabric port-channel all
Fabric Vlag Load-Balance Information
------------------------------
Rbridge-Id           :  2
Vlag                  : 10
```

16.3　LACP 設定のガイドラインと制限

この章では、別途明確に示されているものを除いて、標準ベースの LAG 構成に適用されます。LACP を構成する場合は、これら LACP 構成のガイドラインと制限に従ってください。

- 内蔵 DCB スイッチの全てのポートは全二重でのみ動作します。
- "switchport"インタフェースとして定義されたインタフェースは LAG に結合できません。しかし、LAG は“switchport”として定義してください。
- vLAG では、LACP をご使用下さい。

16.4　デフォルト LACP 構成情報

表 16-2 はデフォルトの LACP 構成情報を一覧しています。

表 16-2　デフォルト LACP 構成パラメータ

パラメータ	デフォルト設定
システムプライオリティ	32768
ポートプライオリティ	32768
タイムアウト	Long(標準 LAG)または short(Brocade　LAG)

16.5　LACP の構成と管理

この章では、Link Aggregation Control Protocol (LACP)の設定方法について説明しています。

NOTE
コンフィグレーションを格納するため、'copy running-config startup-config'コマンドを入力してください。

16.5.1　ポートの LACP 有効化

既存の LAG にインタフェースを追加するために、新しいインタフェースに対して同じ LAG グループ番号を使ってこの手続きを繰り返してください。
インタフェースの LACP を有効化するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。
```
switch(config)# interface tengigabitethernet 0/1
```
3．DCB インタフェースを有効化するため、'no shutdown'コマンドを入力します。
```
switch(conf-if-te-0/1)# no shutdown
```
4．DCB インタフェースに対する LACP を設定するため、'channel-group'コマンドを入力します。
```
switch(conf-if)# channel-group 4 mode active type standard
```

16.5.2　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 アドレスとともにシステムプライオリティを使用し、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
```

16.5.3　DCB インタフェースの LACP タイムアウト時間の設定

LACP タイムアウトは、隣接デバイスからの LACP 応答がタイムアウトするまでの待ち時間を設定します。short 指定の場合は 3 秒、long の場合は 90 秒です。デフォルトは long です。
インタフェースの LACP タイムアウト時間を指定するため、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．DCB インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。

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

3．DCB インタフェースを有効化するため、'no shutdown'コマンドを入力します。

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

4．DCB インタフェースのタイムアウト時間を指定します。

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

16.5.4　LAG の LACP 統計情報のクリア

LACP 統計情報カウンタをクリアするため、LAG グループ番号を指定して'clear'コマンドを入力します。

特定の LAG の LACP カウンタをクリアする例

```
switch# clear lacp 42 counters
```

16.5.5　全 LAG グループの LACP 統計情報のクリア

全 LAG グループの LACP 統計情報カウンタをクリアするため、'clear'コマンドを入力します。

LACP カウンタのクリアする例

```
switch# clear lacp counters
```

16.5.6　LACP 情報の表示

LACP 統計情報と構成情報を表示するため'show'コマンドを使います。『Network OS Command Reference』を参照してください。

16.6　LACP トラブルシューティング

LACP 構成でのトラブルシュートのため、次のトラブルシュートのヒントをお使い下さい。

IEEE802.3ad 準拠の動的トラングを設定したがリンクが LAG に組み込まれない場合：

- 両装置での接続ポートのトランクタイプが標準となっているか設定を確認する。
- 両装置での接続ポートが両方ともパッシブモードとなっていないか設定を確認する。いずれか一方がアクティブでなければなりません。
- 'no shutdown'コマンドをリンクの両端のインターフェース上で実行し、port-channel インタフェースが administrative up 状態にあることを確認します。
- port-channel がギガビットインターフェースを使用している場合、speed パラメータを 1000 に設定されていることを確認してください。
- LAG のポートが同一の隣接スイッチに接続されているか確認してください。
- スイッチのシステム ID がユニークかを確認してください。'show lacp sys-id'を入力することで確認できます。
- 両装置で PDU に関するエラーなく LACPDU が送受信されているか確認します。'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。

Brocade ベースのダイナミックトランクがリンク上に設定されている場合、リンクが LAG に参加することはできません：

- リンクの両端のトランクタイプが Brocade として構成されることを確認してください。
- リンクの両端をパッシブモードで構成されていないことを確認してください。いずれか一方がアクティブでなければなりません。
- 'no shutdown'コマンドをリンクの両端のインターフェース上で実行し、port-channel インタフェースが administrative up 状態にあることを確認します。
- LAG のポートが同一の隣接スイッチに接続されているか確認してください。
- スイッチのシステム ID がユニークかを確認してください。'show lacp sys-id'を入力することで確認できます。
- 両装置で PDU に関するエラーなく LACPDU が送受信されているか確認します。'show lacp counters number'を実行し、受信と送信の統計情報を確認します。統計情報は増加し続けているはずで、ゼロか一定値ではないはずです。もし PUD の受信が増えない場合は、隣接スイッチで'show interface <link-name>'コマンドを入力して、CRC エラーを確認します。もし、PDU の送信が増加しない場合は、'show interface <link-name>'コマンドを入力して、リンクの動作状態を確認し、状態が"up"となっているか確認します。
- リンクのファイバーの長さは 7 マイクロ秒のデスキュー値を持っていることを確認してください。そうでない場合は、リンクが LAG に参加することができず、次の RASLOG メッセージが発生します。

  ```
  Deskew calculation failed for link <link-name>.
  ```

  リンクがこの問題が発生した場合は、'show port-channel'コマンドを実行すると、次のメッセージが表示されます。

  ```
  Mux machine state : Deskew not OK.
  ```

Brocade ベースのスタティックトランクがリンクの上に構成されている場合、リンクが LAG に参加することはできません：

- リンクの両端が、トランクタイプの Brocade として設定され、モードが"ON"であることを確認してください。
- 'no shutdown'コマンドをリンクの両端のインターフェース上で実行し、port-channel インタフェースが administrative up 状態にあることを確認します。

標準ベースのスタティックトランクがリンクで構成されている場合、リンクが LAG に参加することはできません：

- リンクの両端が、トランクタイプの標準として設定され、モードが"ON"であることを確認してください。
- 'no shutdown'コマンドをリンクの両端のインターフェース上で実行し、port-channel インタフェースが administrative up 状態にあることを確認します。

17 NIC 冗長(track)の設定

17.1 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(minimum-links)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。
本機能は、BS500/BS2000 搭載の内蔵 DCB スイッチでサポートされています。

17.2 NIC 冗長(track)の構成

17.2.1 ポート監視の有効化と設定(物理ポート)

インタフェースの監視機能を有効化するために、特権実行モードから次の手順を実行してください。

1. グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2. 障害発生時閉塞するインタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。
   ```
   switch(config)#interface tengigabitethernet 0/9
   ```
3. インタフェースを有効化するため、'no shutdown'コマンドを入力します。
4. インタフェースに対する track 機能を有効化するため、'track'コマンドを入力します。
   ```
   switch(conf-if-te-0/9)#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-te-0/9)#track interface ethernet 0/1
   ```

NOTE
一つの閉塞対象インタフェースに対して複数インタフェースを監視している場合、いずれかのインタフェースで障害が発生している最中に reload を実行しないで下さい。もし、reload が必要な場合は、閉塞対象インタフェースに関連付けられている監視対象の全てのインタフェースに接続されたケーブルを、一旦抜いてから reload を実行してください。

17.2.2　ポート監視の有効化と設定(LAG)

インタフェースの監視機能を有効化するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．障害発生時閉塞するインタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。

```
switch(config)#interface tengigabitethernet 0/9
```

3．インタフェースを有効化するため、'no shutdown'コマンドを入力します。

4．インタフェースに対する track 機能を有効化するため、'track'コマンドを入力します。

```
switch(conf-if-te-0/9)#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-te-0/9)#track interface port-channel 10
```

17.2.3　ポート監視の無効化

インタフェースの監視機能を削除するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．インタフェースのタイプとスロット/ポート番号を指定するため、'interface'コマンドを実行します。

```
switch(config)#interface tengigabitethernet 0/9
```

3．インタフェースを有効化するため、'no shutdown'コマンドを入力します。

4．インタフェースに対する track 機能を削除するため、'no track'コマンドを入力します。

```
switch(conf-if-te-0/9)#no track enable
```

18 LLDP の設定

18.1 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。

18.2 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 TLV 拡張を付加しています。４つの TLV セットは次の通りです。

- 基本管理 TLV セット：このセットはレイヤ 2 トポロジをマップするための情報を提供し、次の TLV を含みます。
  - Chassis ID TLV - ポートを装備するスイッチやルータの ID を提供。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。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。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。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 TLV。
  - 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示す。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 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します。不整合が検出されるとトラップやイベントが 一度報告されます。オプション TLV です。このセットは次の TLV を含みます。
  - Port VLANID TLV - VLAN ポートで受信される untagged もしくは優先 tag データに関連したポート VLAN ID(PVID)を示す。
  - PPVLAN ID TLV - VLAN ポートで受信される untagged もしくは優先 tag データに関連したポート及びプロトコルベース VLAN ID(PPVID)を示す。TLV は、ポートがポート及びプロトコルベース VLAN(PPVLANs)をサポートしているかどうか、また、一つもしくはそれ以上の PPVLANs が有効かどうかを示す"flags"フィールドをサポート。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。
  - 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。LLDPDU の VLAN name TLV の数は、ポートで有効な VLAN の数に依存。
  - 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 です。このセットは次の TLV を含みます。
  - 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。
  - Maximum Ethernet frame size TLV - デバイスの MAC 及び PHY で実装されている利用可能な最大フレームサイズを示す。

NOTE

内蔵 DCB スイッチは、MDI TLV をサポートしていません。当該情報を含んだフレームはエラーフレームとしてカウントします。

18.3 DCBX 概要

ストレージトラフィックは、DCB により提供されるロスレス通信を要求します。Data Center Bridging(DCB) Capability Exchange Protocol (DCBX)は、より効果的なスケジューリングやリンクトラフィックに対する優先フロー制御を実現するために隣接装置と DCB 関連パラメータを交換します。
DCBX は２つのリンク間でパラメータを交換するために LLDP を使用します。DCBX は、情報交換のために LLDP の基盤上に構築されています。DCBX 交換パラメータは、組織的に規定された TLV にパッケージされます。DCBX プロトコルはリンクの他方から通知を要求します。これにより、LLDP は送受信両方有効にされます。DCBX は、制御用 TLV と機能 TLV の両方をチェックするバージョン番号を必要とします。
DCBX は次の通り、他のプロトコル及び機能と相互作用します。

- LLDP-LLDP は、RSTP や LACP のような別のレイヤ 2 プロトコルと並行して実行されます。DCBX は、リンクパートナー間でサポートされる機能を伝えるために、LLDP 基盤上に構築されています。DCBX プロトコルと特徴 TLV は LLDP 規格の上流規格として扱われる。
- QoS マネジメント - DCBX のリンクパートナーと交換されるケイパビリティは、ハードウェアスケジューリングや優先フロー制御を制御できるようハードウェアをセットアップするため QoS マネジメントエンティティに受け渡されます。

DCBX の QoS 規格は２つの機能に分割されます。

- Enhanced Transmission Selection

- Priority Flow Control

18.3.1 Enhanced Transmission Selection

コンバージドネットワークでは、異なるトラフィックタイプが個別にネットワーク帯域に影響を与えます。Enhanced Transmission Selection (ETS)の目的は、コンバージドトラフィックの異なる優先設定に基づき帯域を割り当てることです。例えば、プロセス間通信(IPC)トラフィックは、必要なだけ帯域を使用することが出来、帯域のチェックは行わず、LAN や SAN のトラフィックが残りの帯域を共用するなどです。表 18-1 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 18-1 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 18-1　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

18.3.2 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、ユーザー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。

18.4 LLDP の設定に関する注意事項および制約事項

LLDP を設定する時には、LLDP の設定に関する注意事項および制約事項に従ってください。

- Brocade の LLDP の実装では、標準の LLDP 情報に加えて、Brocade 固有の TLV 交換をサポートしています。
- 必須 TLV は、常に広告されます。
- LLDP のリンクレベルのパラメータの交換は他のレイヤ 2 プロトコルに対して透過的です。LLDP のリンクレベルのパラメータは、LLDP によって他の関連するプロトコルへ報告されます。

NOTE
DCBX 構成は、単純に DCBX 関連の TLV を広告されるように構成することが必要です。詳細な情報は、220 ページの『18.5 LLDP の構成と管理』を参照してください。

18.5　LLDP の構成と管理

この章では、LLDP の設定方法について説明しています。

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。

18.5.1　デフォルト LLDP 設定情報

表 18-2 にデフォルト LLDP 設定情報を示します。

表 18-2　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

18.5.2　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いかぎり、全てのインタフェースで LLDP を有効にします。LLDP はデフォルトで有効となっています。
LLDP を全体で有効化するために、特権実行モードで次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．LLDP 構成モードに移行します。

```
switch(config)# protocol lldp
```

18.5.3　装置全体の LLDP の無効化・リセット

'no protocol lldp'コマンドは、'protocol lldp'コマンドを使用して行われたすべての構成設定をデフォルト設定に戻します。LLDP はデフォルトで有効となっています。

LLDP を全体でリセットするために、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．LLDP をリセットします。

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

LLDP を全体で無効化にするために、グローバルコンフィグレーションモードから次の手順を実行します。

1．protocol コンフィグレーションモードに移行するため、'protocol lldp'コマンドを入力します。

```
switch(config)# protocol lldp
```

2．LLDP を無効化します。

```
switch(conf-lldp)# disable
```

18.5.4　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ことにより、全てのインタフェースに非デフォルトパラメータ値を設定できます。

(1) ハードウェアのシステム名称の指定

LLDP の装置でのシステム名称は、スイッチの識別に役立ちます。デフォルトでは、SNMP の MIB で指定される"host-name"が使われます。

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 Hitachi_Alpha
```

(2) 装置の LLDP システムディスクリプションの指定

NOTE

ディスクリプションに OS バージョンか MIB で定義する情報を使うことを推奨します。また、システム名とディスクリプションの一部として#$！@などの特殊文字を使用しないでください。

装置の LLDP システムディスクリプションを指定するために、特権実行モードで次の手順を実行してください。システムディスクリプションは、隣接スイッチから参照できます。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．LLDP 構成モードに移行します。
```
switch(config)# protocol lldp
```
3．装置のシステムディスクリプションを指定します。
```
switch(conf-lldp)# system-description IT_1.6.2_LLDP_01
```

(3) LLDP のユーザーディスクリプションの指定

LLDPユーザー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 のユーザーディスクリプションを指定します。
```
switch(conf-lldp)# description Hitachi-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)# 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 フレームの送信間隔を設定します。
```
switch(conf-lldp)# hello 45
```

(6) 受信の保持時間の設定

受信デバイス情報の保持時間を設定するため、特権実行モードで次の手順を実行してください。これは、隣接情報を無効とするまでに見逃すことができる連続するLLDP helloパケットの数を指定します。デフォルトは４です。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．LLDP 構成モードに移行します。

```
switch(config)# protocol lldp
```

3．受信の保持時間を設定します。

```
switch(conf-lldp)# multiplier 6
```

(7) オプション LLDP TLV の広告

オプションの LLDP TLV を広告するために、特権実行モードで次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．LLDP 構成モードに移行します。

```
switch(config)# protocol lldp
```

3．オプションの LLDP TLV を広告するよう設定します。

```
switch(conf-lldp)# advertise optional-tlv management-address port-description
system-capabilities system-name system-description
```

(8) LLDP DCBX 関連 TLV の広告設定

デフォルトでは、スタンドアロンモードのスイッチでは、"dcbx-tlv"のみを広告します。

VCS ファブリックモードのスイッチでは、以下の TLV がデフォルトで広告されます。

- dcbx-tlv
- dcbx-fcoe-app-tlv
- dcbx-fcoe-logical-link-tlv

DCBX 関連 TLV を広告するために、特権実行モードで次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．LLDP 構成モードに移行します。

```
switch(config)# protocol lldp
```

3．下記のコマンドを使用して、DCBX 関連 TLV を広告します。

- switch(conf-lldp)# advertise dcbx-fcoe-app-tlv
- switch(conf-lldp)# advertise dcbx-fcoe-logical-link-tlv
- switch(conf-lldp)# advertise dcbx-tlv
- switch(conf-lldp)# advertise dot1-tlv
- switch(conf-lldp)# advertise dot3-tlv

(9) iSCSI 優先度の設定

iSCSI 優先度の設定は、DCBX iSCSI TLV で広告される優先度を設定します。

iSCSI TLV は、接続されている CEE 機能が有効となっているサーバ及びターゲットへの iSCSI トラフィックの構成パラメータを広告するだけです。スイッチでは、広告されたパラメータが iSCSI サーバやタ

ーゲットでの使用を確認も強制もしません。
iSCSI 優先度を設定するために、特権実行モードで次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．LLDP 構成モードに移行します。
```
switch(config)# protocol lldp
```
3．iSCSI 優先度を設定します。
```
switch(conf-lldp)# iscsi-priority 4
```

NOTE
デフォルトの iSCSI 優先度は 4 で、別の値に iSCSI の優先度を変更しない限り表示されません。

4．TLV を広告します。
```
switch (conf-lldp)# advertise dcbx-isci-app-tlv
```

(10) LLDP プロファイルの設定
スイッチ上で最大 64 のプロファイルを設定できます。'no profile'コマンドを使用して、プロファイル全体を削除できます。
LLDP プロファイルを設定するために、特権実行モードで次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．LLDP 構成モードに移行します。
```
switch(config)# protocol lldp
```
3．プロファイル名称を設定します。
```
switch(conf-lldp)# profile UK_LLDP_IT
```
4．プロファイルのディスクリプションを指定します。
```
switch(conf-lldp-profile-UK_LLDP_IT)# description standard_profile_by_Jane
```
5．LLDP フレームの送受信を有効化します。
```
switch(conf-lldp-profile-UK_LLDP_IT)# no mode
```
6．LLDP 更新情報の送信間隔を設定します。
```
switch(conf-lldp-profile-UK_LLDP_IT)# hello 10
```
7．受信に対する保持時間を設定します。
```
switch(conf-lldp-profile-UK_LLDP_IT)# multiplier 2
```
8．オプション LLDP TLV を広告します。
```
switch(conf-lldp)# advertise optional-tlv management-address port-description
system-capabilities system-name system-description
```
9．LLDP DCBX 関連 TLV を広告します。
```
switch(conf-lldp-profile-UK_LLDP_IT)# advertise dot1-tlv
switch(conf-lldp-profile-UK_LLDP_IT)# advertise dot3-tlv
switch(conf-lldp-profile-UK_LLDP_IT)# advertise advertise dcbx-tlv
switch(conf-lldp-profile-UK_LLDP_IT)# advertise dcbx-fcoe-logical-link-tlv
switch(conf-lldp-profile-UK_LLDP_IT)# advertise dcbx-fcoe-app-tlv
switch(conf-lldp-profile-UK_LLDP_IT)# advertise dcbx-iscsi-app-tlv
```

NOTE
"dot1.tlv"と"dot3.tlv"は広告しないことを推奨します。この構成は、機能的な問題を引き起こす可能性があります。

１０．特権実行モードに戻ります。

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

１１．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

(11) iSCSI プロファイルの設定

インタフェース個別に適用する iSCSI プロファイルを設定することが出来ます。しかし、優先ビットはインタフェース毎に手動で設定しなければなりません。'no profile name'コマンドでプロファイル全体を削除することが出来ます。

iSCSI プロファイルを設定するために、特権実行モードから次の手順を実行してください。

１．cee-map が既に作成されていない場合、cee-map を設定します。

CEE-map コマンドの設定については、『Network OS Command Reference』を参照してください。

```
switch(config)# cee-map default
switch(config-cee-map-default)# priority-group-table 2 weight 30 pfc off
switch(config-cee-map-default)# priority-group-table 3 weight 20 pfc on
switch(config-cee-map-default)# priority-group-table 1 weight 50 pfc off
switch(config-cee-map-default)# priority-table 1 1 1 1 2 3 1 15.0
switch(config-cee-map-default)# priority-group-table 2 weight 30 pfc on
```

'priority-table'コマンドの構文：

```
priority-table PGID0 PGID1 PGID2 PGID3 PGID4 PGID5 PGID6 PGID7
```

PGID 値の範囲は、DWRR 優先グループのための 0 から 7 と完全優先グループのための 15.0 から 15.7 です。PGID 値と CoS 値は共通で、PGID0 を指定すると、CoS=0 の全てのパケットに対する優先グループ ID を設定し、GPID1 を指定すると、CoS=1 の全てのパケットに対する優先グループ ID を設定します。このように、PGID7 までの値を指定すると、CoS=7 までの全てのパケットに対する優先グループを設定します。

CEE マップ構成のプライオリティテーブルは、PGID 15.0 を CoS7 専用とすることが必要です。この制限のため、PGID15.0 がプライオリティテーブル構成の最後のパラメータとして構成されることを確認してください。

"priority-table 1 2 2 2 2 2 2 15.0"構文の説明は、次のとおりです。

これは、CoS=1、CoS=2、CoS=3、CoS=4、CoS=5、CoS=6 を DWRR 優先度グループ ID:2 に、CoS= 0 を優先度グループ ID:1 に、CoS=7 を完全優先グループに割当てたことを示します。

これは CEE プライオリティーをプライオリティグループテーブルに割り当てる一つの方法で、それは 8 つ入力 CoS をそれぞれのプライオリティグループにマップできます。

VCS モードでは、トラフィッククラスは、すべて絶対優先(802.1Q デフォルト)または絶対優先と DWRR トラフィッククラスの組み合わせです。

２．LLDP 構成モードに移行します。

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

3．iSCSI のための LLDP プロファイルを作成します。
```
switch(conf-lldp)# profile iscsi_config
```
4．iSCSI TLV を広告します。
```
switch(conf-lldp-profile-iscsi_config)# advertise dcbx-iscsi-app-tlv
```
5．指定したインタフェースの構成モードに移行します。
```
switch (conf-lldp-profile-iscsi_config)# interface te 0/1
```
6．インタフェースに CEE プロビジョニングマップを適用します。
```
switch(conf-if-te-0/1)# cee default
```
7．iSCSI 用に生成した LLDP プロファイルを適用します。
```
switch(conf-if-te-0/1)# lldp profile iscsi_config
```
8．インタフェースに対する iSCSI 優先ビットを設定します。
```
switch(conf-if-te-0/1)# lldp iscsi-priority 4
```
9．追加するインタフェースに対して手順 5 から 8 を繰り返します。

18.5.5　LLDP のインタフェースレベルコマンドオプションの設定

インタフェースに割り当てられるのは、一つの LLDP プロファイルだけです。もし、インタフェースレベルの lldp profile を使わないなら、グローバルコンフィグレーションが使われます。もし、グローバルコンフィグレーションが無い場合、装置のデフォルト値が使用されます。
LLDP のインタフェースレベルコマンドのオプションを設定するため、特権実行モードで次の手順を実行してください。

1．DCB インタフェースタイプとスロット番号を指定して、'interface'コマンドを入力します。
```
switch(config)# interface tengigabitethernet 0/10
```
2．インタフェースに LLDP プロファイルを適用します。
```
switch(conf-if-te-0/10)# lldp profile network_standard
```
3．特権実行モードに戻ります。
```
switch(conf-if-te-0/10)# end
```
4．running-config を startup-config へ格納するため、'copy'コマンドを入力します。
```
switch# copy running-config startup-config
```

18.5.6　LLDP 関連情報の消去

LLDP 関連情報を消去するため、特権実行モードで次の手順を実行してください。

1．LLDP 隣接情報をクリアするため、'clear'コマンドを使います。
```
switch# clear lldp neighbors interface tengigabitethernet 0/1
```
2．LLDP 統計情報をクリアするため、'clear'コマンドを使います。
```
switch# clear lldp statistics interface tengigabitethernet 0/1
```

18.5.7　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
```

19 アクセスコントロールリスト(ACL)の設定

19.1 ACL 概要

NOTE
Network OS では、イングレス(入力)レイヤ 2 MAC アクセス制御リスト(ACL)およびレイヤ 3 IP アクセス制御リストの両方がサポートされています。 Network OS v4.0.0 の導入に伴い、extended IP ACL は IPv6 をサポートし、マネジメントプレーンから IPv6 を用いてスイッチまたはクラスタにアクセスすることが可能となります。一方、マネジメントプレーン ACL はこのような使用方法はサポートしていません。

ACL はハードウェアに対するトラフィックをフィルタし、ACL が適用されたインタフェースを経由して受信するフレームを許可したり拒否したりします。Network OS でサポートされているレイヤ 2 の以下のインターフェースに ACL を適用することができます。

- 物理(10 ギガビットイーサネットとギガビットイーサネット)
- VLAN
- ポートチャネル(静的 LAG と動的 LAG)
- レイヤ 3 バーチャルインタフェース(Network OS v3.0.0 以降)

各々の ACL は、イーサネットフレームに対して適用できる“許可(permit)”及び“拒否(deny)”の statement(ルール)の組み合わせにより構成されます。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。

19.1.1 ACL の利点

ACL を用いることによる主な利点は以下の通りです。

- 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ーをブロックする
- 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(Standard 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のみ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(Extended ACL)
  受信フレームの送信元及び受信元 MAC アドレスからトラフィックを許可及び拒否します。

MAC ACL は次のインタフェースタイプをサポートしています。
- 物理インタフェース
- 論理インタフェース(LAG)
- VLAN

IP ACL は次のインタフェースタイプをサポートしています。
- 論理インタフェース(LAG)
- VLAN

19.1.2　IP ACL

IP ACL は、スイッチへのアクセスを制御します。スイッチからの出力やアウトバンド管理トラフィックの制御に関しては、IP ACL の管理対象外となります。IP ACL は、IPv4 と IPv6 をサポートし、同時に制御可能です。
IP ACL は、パケットフィルタリングファイアウォールとして、インターフェースに適用されるルールのセットです。各ルールは、送信元および宛先 IP アドレス、プロトコルまたはポートの組み合わせにより、トラフィックを拒否または許可するかどうかを定義しています。
各 ACL は、一意の名前を持っている必要がありますが、定義する ACL の数には制限はありません。ACL は、IPv4/v6 のどちらかの一方にのみ対応するルールを含むことができます。IP のバージョン毎に、一つの ACL を一度にインターフェース上で有効にすることができます。言い換えれば、パケットフィルタリング用に IPv4 用の ACL が一つと、IPv6 用の ACL が一つをインタフェースに有効にすることができます。
トラフィックをフィルタリングするために、インターフェースに適用した ACL の各ルールは、シーケンス番号の昇順でチェックされます。一つのアクセスリストに対して最大 2,048 個のルールを追加することができます。ACL がインターフェースに適用される時、ACL に 256 以上のルールがある場合、最も小さいものから 256 個のルールが適用されます。ACL が全くルールも含まずインターフェースに適用される場合、レイヤ 2 ACL とレイヤ 3 ACL で挙動が異なります。
レイヤ 2 ACL の場合、ルールが定義されていない ACL があるインタフェースに適用された場合、何も実行されず、すべての入力トラフィックがインターフェースを通過するように許可されます。一方、レイヤ 3 ACL または IP ACL の場合、ルールが定義されていないとアクセスは拒否されます。
一旦 IP ACL ルールが作成されると、そのオプションは何も変更することができません。

スイッチのデフォルト設定では、2 つの ACL から構成されます。一つは IPv4 ACL で、もう一方は IPv6 ACL がインターフェースに適用されます。

IP アクセスリスト(IP ACL)は以下の 2 種類があります。

- 標準(Standard)
  送信元 IP アドレスだけに対するルールを含みます。ルールは、そのソース IP アドレスのすべてのポートに適用できます。
- 拡張(Extended)
  IP プロトコル、送信元 IP、送信先 IP、送信元ポートと送信先ポートの組合せに対するルールを含みます。

NOTE
IP ACL が VE インタフェースに適用されている場合、その VE インターフェースの “shutdown” / “no shutdown” の状態に関係なく、経由されるトラフィックまたは VLAN スイッチされるトラフィックは適用された ACL によりフィルタされます。

19.1.3　IP ACL パラメータ

表 19-1 に IP アクセスコントロールリスト(ACL)のパラメータとその定義を示します。

NOTE
内蔵 DCB スイッチ上の Network OS v3.0 以降では、拡張 IP ACL ルールに対してサポートされているパラメータは eq パラメータのみとなります。

表 19-1　IP ACL パラメータ

ACL／ルールタイプ	IP ACL パラメータ	IP ACL パラメータ定義
標準 IP ACL	name	標準 IP アクセスコントロールリストの名前。名前は英数字で、63 を超える文字を含めることはできません。アンダースコア(_)及びハイフン(-)も先頭に用いることを除き使用可です。
標準 IP ACL ルール	seq	ルールのシーケンス番号。番号は 0 から 4294967290 までででなければなりません。シーケンス番号が割り当てられていないルールに対しては番号 1 が自動的に割り当てられます。一度関連付けられた番号を変更するには 'resequence' コマンドを実行することで変更可能です。
	permit/deny	ルールで指定された組み合わせに対して、トラフィックを許可または拒否するかどうかを指定します。
	any/host	入力トラフィックをフィルタリングする必要があるホストの IP アドレス。
拡張 IP ACL	name	拡張 IP アクセスコントロールリストの名前。名前は英数字で、63 を超える文字を含めることはできません。アンダースコア(_)及びハイフン(-)も先頭に用いることを除き使用可です。
拡張 IP ACL ルール	seq	ルールのシーケンス番号。番号は 0 から 65535 までででなければなりません。シーケンス番号が割り当てわれていないルールに対しては番号 1 が自動的に割り当てられます。一度関連付けられた番号変更するには 'resequence' コマンド実行することで変更可能です。
	permit/deny	ルールで指定された組み合わせに対して、トラフィックを許可または拒否するかどうかを指定します。
	protocol	フィルタリング対象の IP パケットのタイプを示します。
	any/host	着信トラフィックをフィルタリングする必要があるホストの IP アドレス。
	any	出力または発信トラフィックの制御がブロックされているホストの IP アドレス。出力と発信トラフィックがブロックされるため、宛先アドレスは常に "any"(また、ホストの仮想 IP アドレスもカバーしています)。
	port-number	フィルタが適用されるため、送信元または宛先ポートを示します。これは UDP と TCP の両方に適用されます。番号は 0 から 65535 までです。
	range	ACL ルールを介してフィルタされている必要があり、複数の宛先ポートがある場合は、開始ポートと終了ポートを指定する範囲のパラメータを使用します。
	eq	ACL ルールを介してフィルタしなければならない唯一の宛先ポートがある場合、eq パラメータを使用します。
	dscp value	受信したパケットの dscp 値に対して、指定された値を比較します。有効な値の範囲は 0 から 63 までです。
	ack, fin, rst, sync, urg, psh	TCP フラグの任意の組み合わせを指定することができます。
	Log	フィルタに一致するパケットは CPU に送信され、対応するログエントリが生成されます。オプションのログパラメータは、ログメカニズムを有効にします。このオプションは、許可と拒否でのみ使用可能です。
	hard drop	エコー要求(ping)のような制御フレーム、データフレームを破棄します。

19.1.4　デフォルト ACL 設定

スイッチ上に適用されているポリシーが一つも無い場合、これらのデフォルトの ACL ルールが Network OS で有効です。

- seq 0 は、tcp any any eq 22 を許可します。
- seq 1 は、tcp any any eq 23 を許可します。
- seq 2 は、tcp any any eq 897 を許可します。
- seq 3 は、tcp any any eq 898 を許可します。
- seq 4 は、tcp any any eq 111 を許可します。
- seq 5 は、tcp any any eq 80 を許可します。
- seq 6 は、tcp any any eq 443 を許可します。
- seq 7 は、udp any any eq 161 を許可します。
- seq 8 は、udp any any eq 111 を許可します。
- seq 9 は、tcp any any eq 123 を許可します。
- seq 10 は、tcp any any の範囲 600 から 65535 を許可します。
- seq 11 は、udp any any の範囲 600 から 65535 を許可します。

19.2　ACL の構成と管理

本節では Network OS 上で動作するアクセスコントロールリスト(ACL)の動作について説明します。

19.2.1　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限に従ってください。

- ACL ではルールの順番が重要です。最初のルールがトラフィックにマッチすると、以降の処理はフレームに適用されません。
- 標準 ACL と拡張 ACL は同じ名称にできません。
- マネジメントインタフェースに対して UDP プロトコルを許可、または拒否する ACL を適用することにより、TCP プロトコルに対する暗黙の拒否が成立します。例外として、ping 要求は通過することができます。
- 特定の UDP ポートに対する許可、または拒否する ACL を適用することにより、その他の全ての UDP ポートに対する暗黙の拒否が成立します。
- 特定の TCP ポートに対する許可、または拒否する ACL を適用することにより、その他の全ての TCP ポートに対する暗黙の拒否が成立します。
- レイヤ 2 ACL には ACL のルールリストの最後に追加されるデフォルト許可ルールがあります。この暗黙のルールは、ACL に関連付けられている順序リスト内の設定されたルールのいずれにも一致しない、すべてのレイヤ 2 ストリームを許可します。
- "permit any"というデフォルトのアクションが L2 ACL の最後に追加されます。このデフォルトルールはユーザーには公開されず、暗黙のルールとして動作します。
- 一方、レイヤ 3 ACL では、デフォルトで拒否 "deny" ルールが L3 ACL の最後に追加されます。
- "deny any"というデフォルトのアクションが L3 ACL の最後に追加されます。このデフォルトルール

はユーザーには公開されず、暗黙のルールとして動作します。

- "permit" または "deny" ACL の代わりに hard-drop ACL を適用すると、ドロップされるパケットを有効化し、パケットトラップエントリを優先します。しかし、hard-drop ACL よりも前に定義されるルールで発生した許可エントリは優先されません。
- 任意のインタフェースに適用されている ACL は削除できません。
- route-map 中の ACL は OSPF (Open Shortest Path First) 及び BGP (Border Gateway Protocal) プロトコルでは使用されません。
- すでに存在している ACL に対して新規の Option パラメータを追加することはできません。Option パラメータを追加したい場合は一度ルールを削除し、追加パラメータを含むルールを新規作成する必要があります。

BS500 及び BS2000 向けの内蔵 DCB スイッチは以下の機能をサポートしていません。

- Egress ACL
- MAC マスク(FFFF.FFFF.FFFF を除く)
- 可変 LSB を有する不連続な IP アドレスマスク
- TCP または UDP ポートレンジに対する "eq" (equal)を除くオペレータ
- TCP flag の内、PUSH および URG

例として、 0.0.255.255 のワイルドカードマスクはサポートしますが、一方で 255.0.0.0, 0.255.0.255 といった不連続な IP アドレスマスクは非サポートです。CIDR フォーマットにより表記された IP アドレスとマスク表記に関してのみサポートされます。

19.2.2 標準 MAC ACL の作成とルールの追加

標準 MAC ACL の作成およびルール追加を実施する際は以下の項目に留意する必要があります。

- MAC ACL 入のルールに割り当てられたシーケンス番号を変更するには 'resequence' コマンドを使用できます。236 ページの『19.2.8 MAC ACL のシーケンス番号の並び替え』を参照して下さい。
- レイヤ 2 インターフェースに適用されるまで、MAC ACL が有効になりません。234 ページの『19.2.4 DCB インターフェースへの MAC ACL の適用』および 234 ページの『19.2.5 VLAN インタフェースへの MAC ACL 適用』を参照してください。
- Network OS v2.x などの以前のバージョンでは "[]¥.@#+*()={}"といった特定の文字列を ACL の名前に用いることが可能でした。一方、Network OS v3.0.0 よりこれら特殊な文字列を ACL の名称に用いることは禁止となり、記号としてはアンダースコア(_)及びハイフン(-)のみ使用可能です。Network OS v2.x から v3.x 以降へのアップデートの際、アップデートファイルに含まれるスクリプトにより自動的にこれら無効な文字列は削除されます。結果として、アップデート後の ACL 名がユニークで無くなる可能性があります。これを避けるため、アップデートの際、各々の ACL に ID が付与されます。(例：MAC ACL の場合は -m<acl_num>が、IP ACL の場合は –i<acl_num>が自動付与されます。)
- ACL が特定のホストまたは特定のレンジを "deny" するよう設定されている場合(例：'seq 2 deny host 10.9.106.120')でも、内蔵 DCB スイッチは hard-drop オプションが追加されている(例：'seq 20 hard-drop icmp any any')場合を除き、ping コマンドに応答します。

MAC ACL の作成とルールを追加するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．標準 MAC ACL の作成し、ACL コンフィグレーションモードに移行します。
この例では、標準の MAC ACL の名前は "test_01"としています。

```
switch(config)# mac access-list standard test_01
switch(conf-macl-std)#
```

3．送信元 MAC アドレスでトラフィックを廃棄するよう MAC ACL にルールを追加するため、'deny'コマンドを入力します。

```
switch(conf-macl-std)# deny 0022.3333.4444 ffff.ffff.ffff 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 ffff.ffff.ffff 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 ffff.ffff.ffff count
switch(conf-macl-std)# seq 1000 permit 0022.1111.2222 ffff.ffff.ffff count
```

6．特権実行モードに戻ります。

```
switch(conf-macl-std)# end
```

7．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

19.2.3　拡張 MAC ACL の作成とルールの追加

拡張 MAC ACL の作成およびルール追加を実施する際は以下の項目に留意する必要があります。

- MAC ACL 入のルールに割り当てられたシーケンス番号を変更するには 'resequence' コマンドを使用できます。236 ページの『19.2.8 MAC ACL のシーケンス番号の並び替え』を参照して下さい。
- MAC ACL の名称は最大 64 文字です。レイヤ 2 インターフェースに適用されるまで、MAC ACL が有効になりません。234 ページの『19.2.4 DCB インターフェースへの MAC ACL の適用』および 234 ページの『19.2.5 VLAN インタフェースへの MAC ACL 適用』を参照してください。
- Network OS v2.x などの以前のバージョンでは “[]¥.@#+*()={}”といった特定の文字列を ACL の名前に用いることが可能でした。一方、Network OS v3.0.0 よりこれら特殊な文字列を ACL の名称に用いることは禁止となり、記号としてはアンダースコア(_)及びハイフン(-)のみ使用可能です。Network OS v2.x から v3.x 以降へのアップデートの際、アップデートファイルに含まれるスクリプトにより自動的にこれら無効な文字列は削除されます。結果として、アップデート後の ACL 名がユニークで無くなる可能性があります。これを避けるため、アップデートの際、各々の ACL に ID が付与されます。(例：MAC ACL の場合は -m<acl_num>が、IP ACL の場合は –i<acl_num>が自動付与されます。)
- ACL が特定のホストまたは特定のレンジを “deny” するよう設定されている場合(例：'seq 2 deny host 10.9.106.120')でも、内蔵 DCB スイッチは hard-drop オプションが追加されている(例：'seq 20 hard-drop icmp any any')場合を除き、ping コマンドに応答します。

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 ffff.ffff.ffff 0022.3333.5555
ffff.ffff.ffff
```
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 ffff.ffff.ffff 0022.3333.5555
ffff.ffff.ffff
```
5．特権実行モードに戻ります。
```
switch(conf-macl-ext)# 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
```

19.2.4　DCB インターフェースへの MAC ACL の適用

適用する ACL が存在し、この DCB のインターフェースに必要な方法でトラフィックをフィルタリングするように設定されていることを確認します。ACL は、明示的に'access-group'コマンドを使用してインターフェースに適用されるまで機能しません。ACL を明示的に DCB インタフェースに適用することで、DCB インタフェースで受信されるフレームはフィルタされます。

NOTE
ACL がインターフェースにアクセスグループとして適用する前に、DCB インターフェースをレイヤ 2 スイッチポートとして設定する必要があります。

DCB インターフェースに MAC ACL を適用するには、特権実行モードから次の手順を実行してください。
1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．DCB インターフェースタイプとスロット/ポート番号を指定するには、'interface'コマンドを入力します。
```
switch(config)# interface tengigabitethernet 0/1
```
3．インターフェースをレイヤ 2 スイッチポートとして設定するために、'switchport'コマンドを入力します。
```
switch(conf-if-te-0/1)# switchport
```
4．入力方向(ingress direction)に対する ACL として、レイヤ 2 DCB のインターフェースに適用される MAC ACL を指定するには、'mac-access-group'コマンドを入力します。
```
switch(conf-if-te-0/1)# mac access-group test_02 in
```

19.2.5　VLAN インタフェースへの MAC ACL 適用

適用する ACL が存在し、この VLAN インターフェースに必要な方法でトラフィックをフィルタリングするように設定されていることを確認します。ACL は'access-group'コマンドを使って明確に適用されるまで機能しません。ACL を明示的に VLAN インタフェースに適用することで、VLAN で受信されるフレームはフィルタされます。
VLAN インタフェースに MAC ACL を適用するには、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．VLAN インタフェースに MAC ACL を適用するため、'interface'コマンドを入力します。
```
switch(config)# interface vlan 50
```
3．VLAN に適用した MAC ACL を指定して'mac-access-group'コマンドを入力します。
```
switch(config-Vlan-50)# mac access-group test_02 in
```

19.2.6　MAC ACL ルールの変更

存在している MAC ACL のルールは変更できません。その場合、一旦ルールを削除して、必要な変更を行ったルールを再作成してください。
既存のルールの間に現在のシーケンス番号付けが許すより多くのルールを加える必要がある場合、シーケンス番号を再度割り当てるために、'resequence'コマンドを使用することができます。詳細については、236 ページの 『19.2.8 MAC ACL のシーケンス番号の並び替え』を参照してください。
変更したいルールを指定するためにシーケンス番号を使います。シーケンス番号がないと、リストの最後に新しいルールが追加されて、既存のルールは変更されません。

NOTE
"permit"と"deny"キーワードにより、多くの異なるルールを作成できます。このセクションの例では、MAC ACL を修正するために必要な基本的な知識を示します。

NOTE
この例は、test_02 が"deny any any"オプションで番号 100 のルールを持っていることを想定しています。

MAC ACL を修正するため、特権実行モードから次の手順を実行してください。
1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。
2．修正を行う"test_02"という名前の ACL を指定するため、'mac'コマンドを入力します。
```
switch(config)# mac access-list extended test_02
```
3．存在するルール 100 を削除するため、'no seq'コマンドを入力します。
```
switch(conf-macl-ext)# no seq 100
```
または、新しいパラメータで番号 100 のルールを再作成するため、'seq'コマンドを入力します。
```
switch(conf-macl-ext)# seq 100 permit any any
```

19.2.7　MAC ACL の削除

MAC ACL が DCB インタフェースまたは VLAN インタフェースに適用されている場合、その MAC ACL は削除することはできません。最初に DCB インタフェースまたは VLAN インタフェースにの access-group から削除する必要があります。
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
```

19.2.8　MAC ACL のシーケンス番号の並び替え

MAC ACL のルールにつけたシーケンス番号は並び替えが可能です。シーケンス番号の並び替えは、ACL にルールを挿入する時、利用可能なシーケンス番号が不足する場合に使います。デフォルトの初期シーケンス番号は 10 であり、デフォルトの増分は、標準および拡張 MAC ACL で 10 です。

最初のルールは、開始番号で指定した番号となります。それに続く各々のルールは、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
```

19.2.9　標準 IP ACL の作成

標準 IP ACL を作成するには、グローバルコンフィグレーション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．'ip access-list standard'コマンドを使用し、標準 IP ACL コンフィグレーションモードに移行します。

```
switch(config)# ip access-list standard stdACL3
```

3．ACL のためのルールを入力するには、'seq'コマンドを使用します。複数のルールを入力することができます。

```
switch(config-ipacl-std)# seq 5 permit host 10.20.33.4
switch(config-ipacl-std)# seq 15 deny any
```

4．グローバルコンフィグレーションモードに戻るには、'exit'コマンドを使用します。変更は自動的に保存されます。

```
switch(config-ipacl-std)# exit
switch(config)#
```

19.2.10　拡張 IP ACL の作成

拡張 IP ACL を作成するには、グローバルコンフィグレーション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．'ip access-list extended'コマンドを使用し、拡張 IP ACL コンフィグレーションモードに移行します。

```
switch(config)# ip access-list extended extdACL5
```

3．ACL のためのルールを入力するには、'seq'コマンドを使用します。複数のルールを入力することができます。

```
switch(config-ipacl-ext)# deny udp any any range 10 25
switch(config-ipacl-ext)# seq 5 deny tcp host 10.24.26.145 any eq 23
switch(config-ipacl-ext)# seq 7 deny tcp any any eq 80
switch(config-ipacl-ext)# seq 15 permit tcp any any
```

4．グローバルコンフィグレーションモードに戻るには、'exit'コマンドを使用します。変更は自動的に保存されます。

```
switch(config-ipacl-ext)# exit
switch(config)#
```

NOTE

'range'パラメータを使用する場合は、'seq'を指定することはできません。'seq'を指定しないルールは、シーケンス番号が自動的に割当てられ、定義済みルールに追加される(後に評価される)ことになります。従って、優先したいルールで'range'パラメータを使用する場合は、最初に評価する順番に定義してください。

19.2.11 管理インターフェースへの IP ACL の適用

IP ACL を適用するには、グローバルコンフィグレーション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．管理インターフェースのためのコンフィグレーションモードに移行するには、'interface'コマンドを使用します。

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

3．IPv4 標準 ACL を適用するには、'ip access-group'コマンドを使用します。

```
switch(config-Management-1/0)# ip access-group stdACL3 in
```

4．IPv6 標準 ACL を適用するには、'ip access-group'コマンドを使用します。

```
switch(config-Management-1/0)# ipv6 access-group stdV6ACL1 in
```

5．IPv4 拡張 ACL を適用するには、'ip access-group'コマンドを使用します。

```
switch(config-Management-1/0)# ip access-group extdACL5 in
```

6．グローバルコンフィグレーションモードに戻るには、'exit'コマンドを使用します。変更は自動的に保存されます。

```
switch(config-ip-std)# exit
switch(config)#
```

NOTE

管理インタフェースに対して UDP ACL を"permit" または "deny"することは、TCP protocol に対する暗黙の"deny"が成立します。その逆の場合も同様となります。

19.2.12 スタンドアロンモードまたはファブリッククラスタモードへの ACL の関連付け

スタンドアロンモード、またはファブリッククラスタモードでは、任意の ACL は、クラスタ中に存在する任意のノードに適用することができます。クラスタ中の任意のノードは RBridge ID により一意に識別することができます。管理インタフェースに対しては、IPv4 に対して一つの ACL が、IPv6 に対して一つの ACL がそれぞれ適用できます。新しい ACL を適用することは、以前に適用された古い ACL との入れ替えを意味します。'no' コマンドフォームはインタフェースからの ACL の削除を意味します。アクティブな ACL を削除することにより、デフォルトの動作である "permit any" として動作します。

管理インタフェースに対する入力方向の ACL として、一つの IP ACL を関連付けることができます。

19.2.13 IP ACL 設定の表示

IP ACL の設定を表示するには、特権実行モードで'show running-config ip access-list'コマンドを使用します。

```
switch# show running-config ip access-list
ip access-list standard stdACL3
 seq 5 permit host 10.20.33.4
 seq 7 permit any
!
ip access-list extended extdACL5
 seq 5 deny tcp host 10.24.26.145 any eq telnet
 seq 7 deny tcp any any eq 80
 seq 10 deny udp any any range 10 25
 seq 15 permit tcp any any
```

20 QoS の設定

20.1 QoS 概要

QoS は、スイッチからスイッチへのトラフィックの流れを制御する機能を提供します。異なる用途で使われる異なるトラフィックが存在するネットワークにおいて、QoS の目的はトラフィックタイプ毎に仮想パイプを提供することです。
スイッチを通過するトラフィックは、イーサのマルチキャストトラフィックかユニキャストトラフィックに分類できます。マルチキャストトラフィックは、送信元は一つですが複数の宛先に転送されます。ユニキャストトラフィックは、一つの送信元から一つの宛先に転送されます。
入力ポートから出力ポートへ転送さ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場合や管理セグメントに接続する場合に使います。

20.1.1 QoS の機能

QoS の機能は以下の通りです。

- リライト
  リライト(Rewriting)またはマーキング(Marking)は、優先度(Priority)や VLAN ID のようなフレーム内のヘッダフィールドを上書きします。
- キューイング
  キューイング(Queueing)とは、転送待ちのフレームを一時的に保管できるメモリを提供します。入力ポート、出力ポート、定義されたユーザーのプライオリティレベルに基づき保管されるキューが選択されます。
  - 輻輳制御 ー 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) 、Random Early Discard (RED)があります。
- BUM ストームコントロール(BUM_storm_control)
  パケットが LAN 上に溢れ、トラフィックストームが発生するとネットワークの性能は低下します。BUM ストームコントロールはブロードキャスト(Broadcast)、宛先不明ユニキャスト(Unknown unicat)及びマルチキャスト(Multicast)のトラフィックの総量を制限することでレイヤ 2 物理ポートのトラフィック溢れによる性能劣化を抑止します。任意の物理ポートにおいて、BUM トラフィックに対して設定された最大のトラフィックを超えたトラフィックは破棄されます。また、5 秒間のサンプリング期間以内に最大レートを超えた場合、インタフェースを閉塞するかどうか、閉塞インタフェースのログを採取するかどうかを指定することも出来ます。
- データセンタブリッジング(DCB)
  DCB は、単一の相互接続技術の上に、データセンター内の LAN、SAN、および IPC 等の様々な

アプリケーションの融合を可能にする拡張イーサネットを示しています。

NOTE
BUM ストームコントロールは、BS2500 搭載 DCBSW のみでサポートしています。

(1) 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 untrust で、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ープライオリティマッピングに基づいて行われます。

(2) キューイング
キューの選択は、設定されたユーザー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行われます。その後、各ユーザー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一つへ割り当てられます。

20.1.2　ユーザープライオリティマッピング
受信フレームをユーザー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 trust なインタフェースには明確なポリシーをもってユーザー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が QoS 設定が可能な trust なものなら、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では、下記の通り取り扱われます。
- 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ー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。

20.1.3　輻輳制御
キューが、例えばリンクのオーバーサブスクリプションやダウンストリームデバイスからのバックプレッシャーなどのいくつかの理由により、一杯になり始めることがあります。継続する長時間のキュ

ーへの滞留は、一般にネットワークで輻輳の兆しであり、キューイングによる遅延とフレーム損失によりアプリケーション性能に影響を及ぼします。
輻輳制御は、輻輳が発生した場合どのようにシステムが対応するかを定義し、ネットワークが輻輳状態に入るのを防ぐために行う対策を有効にすることまでを含みます。

(1) Tail drop

Tail drop キューイングは輻輳制御の最も基本的な形態です。フレームは FIFO でキューイングされ、バッファメモリが枯渇するまでキューイングされます。これは、特別な QoS 設定がない場合のデフォルトの動作です。
基本的な Tail drop アルゴリズムは、キューと関連付けられる複数の優先度やトラフィック毎の廃棄閾値という考えはありません。キューの深さが閾値を越えた場合、優先度を持ったフレームを受信しても廃棄されます。
図 20-1 は、低優先度のトラフィックが全くバッファメモリを使わないことを保証するために、本機能をどのように使うかを示しています。閾値は、また、各トラフィッククラスに対する最大のキュー遅延を制限するためにも使うことが出来ます。加えて、もしポートに対する閾値の合計をバッファメモリの 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。

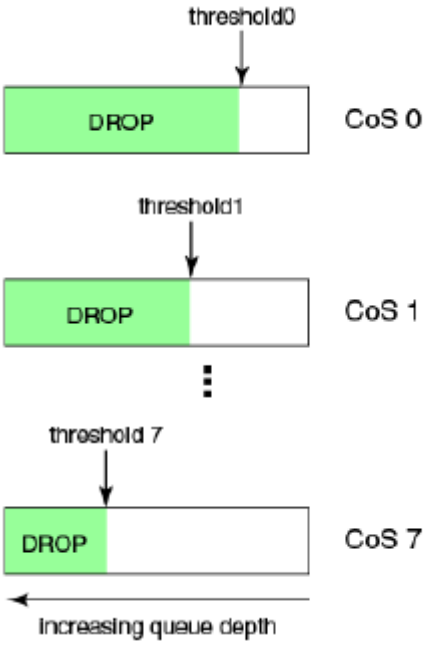

図 20-1　キューの深さ

Tail drop アルゴリズムは優先度別の破棄閾値をサポートするように拡張できます。入力ポートの CoS キューの深さが閾値に達すると、関連付けられたプライオリティ値で到着するどんなフレームも破棄されます。図 20-1 は、優先度の低いトラフィックが全体的にバッファメモリを全て消費しないことを保証するために、この機能を活用する方法について説明します。閾値は、また、各トラフィッククラスの最大キューイング遅延を関連することになります。加えて、ポートの閾値の合計がバッファメモ

リの 100%以下に設定されている場合、単一の CoS 値がポートに割り当てられた共有メモリプール全体を独占しないようにすることができます。

(2) CoS 閾値の設定

すべてのポートには、一つのポート Tail drop 閾値と 8 つのプライオリティ毎の閾値値の合計 9 つの CoS 閾値が関連付けられています。すべてのプライオリティからのトラフィックに対する公正なバッファ配分を与えるために、ポートバッファは異なるプライオリティ間で割り当てられます。これは、プライオリティ毎の Tail drop 閾値により実現されます。ポート Tail drop 閾値は、ポートに指定されたバッファの量を表し、プライオリティ毎の Tail drop 閾値(ここからは CoS Tail drop 閾値と呼びます)は、各 CoS に割り当てられるバッファを表します。

プライオリティに割り当てられているバッファが完全に消耗している時は、常にそのプライオリティに着信するすべてのトラフィックが廃棄されます。プライオリティ毎の tail drop 閾値が存在しない場合には、バッファは先入れ先出しの基本に基づき消費され、結果として全てのプライオリティ間で不公平に共有されることとなります。もし、どのプライオリティのトラフィックが多く見られるかが分かったら、それらのプライオリティに十分な数のバッファを与えることが、パケット破棄の数を低減する結果となります。

このように、標準プライオリティ値を使う代わりに、全 8 つのプライオリティの合計値で 100%を超えないように 0%から 100%まで任意の閾値をどこにでも割り当てることができます。

例えば、次の例に示すように、priorities 5 5 5 5 50 20 2 8 とすると合計 100%となります。

```
switch(conf-if-te-0/1)# qos rcv-queue cos-threshold 5 5 5 5 50 20 2 8
switch(conf-if-te-0/1)# do show qos in te 0/1
Interface TenGigabitEthernet 0/1
CoS-to-Traffic Class map 'default'
        In-CoS:  0  1  2  3  4  5  6  7
 ------------------------------------------------
 Out-CoS/TrafficClass: 0/1 1/0 2/2 3/3 4/4 5/5 6/6 7/7
Per-Traffic Class Tail Drop Threshold (bytes)
     TC:   0   1   2   3   4   5   6   7
-----------------------------------------------------------------
Threshold: 10180 10180 10180 10180 101808 40723  4072 16289
```

Tail drop 閾値は、100%を超えることは出来ませんが、下回ることは可能です。例えば、入力した Tail drop 閾値が 100%未満の場合は、バッファ割り当ては、設定された内容に従い割り当てられます。

(3) Random Early Discard

NOTE

この機能は、BS2500 搭載 DCB スイッチモジュールでのみサポートされています。

従来から、Random Early Discard (RED)は、一般的に更に積極的な対処としてだけではなく受動的な対応としてパケットを破棄するため TCP の通信に利用されています。もし RED が設定されていないと、スイッチに設定されたキューが一杯になり tail drop することになります。Tail drop の状況は、スイッチでの head-of-line(HOL)ブロック問題を引き起こし、好ましくありません。RED を設定することで、キューの状態が指定した閾値に達する前にパケットを破棄する確立を設定します。これは、輻輳を徐々に緩和し、パケット再送を避け、輻輳状態の TCP 通信のバースト状態を解消して、パケット遅延を制御します。

次のパラメータを使って RED を設定してください。

- RED プロファイル ID(0-384)
- キューの最小閾値(0-100%)
- キューの最大閾値(0-100%)
- 破棄確率(0-100%)

ASIC ドライバは、実際のキューサイズに対して設定された最小/最大パーセントをバイトで割り当てます。キューサイズは、ポートのバンド幅に依存しており、ポートのスピードに応じてバッファが割り当てられます。キューのバッファに最小閾値が設定されると、キューイングされたパケットは、ランダムに破棄されます。破棄確率パラメータは、破棄のランダム性を定義します。キューが最小閾値を超えると、パケットは設定された破棄確率に沿って破棄されます。キューバッファが、設定された最大閾値を超えると、パケットは 100%破棄されます。より高い確率が設定されることで、最小パーセントに到達すると多くのパケットが破棄されることになります。
また、CoS 値(0～7)に RED プロファイルを指定することも出来ます。

20.1.4　イーサネット Pause(Ethernet pause)

イーサネット Pause は、隣接デバイスへの送信規制のための IEEE802.3 で規定される仕組みです。Pause メッセージはオプションの MAC 制御サブレイヤを使うことによって送信されます。Pause フレームは、512bit 時間単位の Pause 期間を示す２バイトの値を持っています。デバイスが Pause フレームを受信すると、送信中のフレーム転送が完了した後、指定された時間インタフェースからのデータ送信を停止しなければなりません。標準的な仕組みによりフレームロスを低減する方法として、この機能は使えます。しかしながら、Pause メカニズムは、数ホップ離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。

(1) Ethernet Pause の特徴

イーサネット Pause は下記の特徴を持ちます。

- 全ての構成パラメータはインタフェース毎に個別に指定することが出来る
- Pause On/Off は、TX と RX 別々に指定することが出来る。auto-negotiation を無効にすることにより抑止することができます。
- Pause は入力(受信)キューに依存して生成される。キューレベルは、入力ポート単位に決定されます。各入力ポートの上限及び下限閾値を指定できます。もし、更にフレームを受信してキュー長がまだ下限閾値以上ならば、更に Pause フレームが生成されます。一旦、キュー長が下限閾値以下となれば、Pause の生成は終了します。
- Pause を受信して実行されると、Pause フレームで指定された期間、ポートに関連付けられた出力キューの伝送は保留されます。

(2) 1Gbps ポーズネゴシエーション

1Gbps ローカルポートがすでにオンラインで、'qos flowcontrol'コマンドが発行されると、Pause 設定は、すぐにローカルポートで有効になります。しかし、リンクが切り換えられると、Pause は再ネゴシエートされます。ローカルポートは、最新の QoS フロー制御設定を広告します。オートネゴシエーシ

ョンが完了すると、ローカルポートの Pause 設定は、表 20-1 に示されているように、802.3 Clause 28B に従って、Pause ネゴシエーションの結果に応じて変更されることがあります。

表 20-1　Pause ネゴシエーション結果

広告された LOCAL cfg	広告された REMOTE cfg	ネゴシエーション結果
Rx=off Tx=on	Rx=on Tx=on	asymmetrical: LOCAL Tx=on --> pause --> REMOTE Rx=on
Rx=on Tx=on	Rx=off Tx=on	asymmetrical: LOCAL Rx=on <-- pause <-- REMOTE Tx=on
Rx=on Tx=n/a	Rx=on Tx=n/a	symmetrical : LOCAL Tx/Rx=on <-- pause --> REMOTE Tx/Rx=on
Rx=n/a Tx=n/a	Rx=off Tx=off	disable pause both sides

(3) イーサネットプライオリティフロー制御

イーサネットプライオリティフロー制御(PFC)は、イーサネットポーズの基本的な拡張機能です。ポーズ MAC 制御メッセージは、8 つの 2 バイトのポーズ値とその値が有効であるかを示すためにビットマスクで拡張されます。各ポーズ値はベースポーズプロトコルと同様に解釈されていますが、それぞれが対応するイーサネット優先/クラスレベルに適用されます。

たとえば、ポーズ値 0 は、プライオリティ 0 に適用され、ポーズ値 1 は、プライオリティ 1 に適用されます。これは、リンク上のすべてのトラフィックが中断され、イーサネットのポーズメカニズムの一つの欠点に対処しています。しかし、その他のイーサネットポーズの制限は残ったままです。

イーサネットプライオリティフロー制御は、次の機能が含まれています。

- 各入力ポートに 8 つの上限と下限の閾値が存在する以外は上記のイーサネットポーズで述べたように全てが正確に動作します。つまりキューレベルは、優先付けされた入力ポート毎に動作することを意味しています。
- ポーズオン/オフがプライオリティ毎に TX と RX に独立して指定することができます。
- イーサネット MAC に指定されるポーズ時間は全てのプライオリティをカバーする単一の値です。
- イーサネット Pause またはイーサネットプライオリティフロー制御は互換性がないため、リンクの両端での設定は同じでなければなりません。

20.1.5　BUM ストーム制御

ネットワークストームは、パケットが LAN にフラッディングされ、過剰なトラフィックを生み出し、ネットワーク性能を低下させます。ブロードキャスト(Broadcast)、未学習のユニキャスト(unknown unicast)、マルチキャスト(Multicast)ストーム制御は、物理ポートの遮断を避けることが出来ます。

BUM ストーム制御は、指定されたポートまたはスイッチ全体でブロードキャスト、未学習のユニキャスト、マルチキャストの受信総量を制限するものです。設定されたレートを超える全てのトラフィッ

クは、破棄されます。また、５秒間に定義された最大値を超えた場合、インタフェースを shutdown することも出来ます。ポートが shutdown されると、ログメッセージを送信します。インタフェースを回復させるためには、手動で'no shutdown'コマンドを入力する必要があります。

(1) BUM ストーム制御の配慮と制限

- BUM ストーム制御は、次の物理インタフェースの一つに設定されなければなりません。
  - 1-gigabit Ethernet
  - 10-gigabit Ethernet
  - 40-gigabit Ethernet
- BUM ストーム制御と入力サービスポリシーは、同時に使用できません。
- BUM ストーム制御は、マルチキャストレート制限機能を代替するものです。このコマンドは、BS2000 及び BS500 搭載の DCB スイッチモジュールではサポートされていません。

20.1.6　スケジューリング

スケジューリングは、フレームを転送するために滞留している複数のキューを調停します。内蔵 DCB スイッチでは、絶対優先(Strict Priority:SP)スケジューリングと欠損荷重ラウンドロビン(Deficit Weighted Round Robin:DWRR)スケジューリングの２つのアルゴリズムをサポートしています。
また、SP-to-DWRR を使うことで、トラフィッククラスの数を自由に選択することが出来ます。同一トラフィッククラスに複数のキューが存在すると、スケジューリングはこれら等しい優先キューを考慮に入れます。

(1) 絶対優先(Strict priority:SP)スケジューリング

SP(Strict priority)は、遅延を重視するトラフィックに対する対応を容易にするために使用されます。
SP スケジューラーは低優先度のトラフィッククラスを転送する前に、最高優先キューに滞留する全てのフレームを転送します。このタイプのサービスの問題は、キューが低優先度のトラフィックで使い尽くされるポテンシャルがあることです。

図 20-2 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ます。高い番号を持つキューの SP2 が高い優先度を持っています。

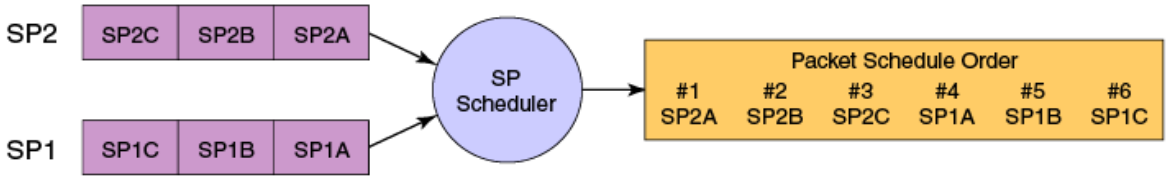

図 20-2　２つのキューでの SP スケジューリング

(2) 欠損荷重ラウンドロビン(Deficit weighted round robin:WRR)スケジューリング

WRR スケジューリングは、ネットワーク帯域の共有を制御することを容易にするために使用されます。

WRR はそれぞれのキューに重み付けを行います。その値は、キューに割り付けられた帯域の合計を決定します。スケジュールのラウンドロビンの挙動は、次のキューにデータが移動する前に総数を制限して送信したり、最低優先度がサービスされた後に最高優先度のキューに戻るように、各キューに対してサービスします。
図 20-3 は、２つの WRR キューを提供している WRR スケジューラに対して、フレームをスケジュールする順序を示しています。高い番号のキューは高い優先度(WRR2)と扱われ、重み付けは２つのキューでネットワーク帯域が２：１に配分されることを示しています。図 20-3 の WRR2 は帯域の６６％を受信し、WRR1 は３３％受信します。
WRR スケジューリングは、使用される余分な帯域を追跡して、キューを通る次のサイクルに割り当てられる帯域幅より余分な帯域を差し引きます。このように、帯域の利用率が長い期間にわたってキューの重み付けが統計的に一致するようになります。

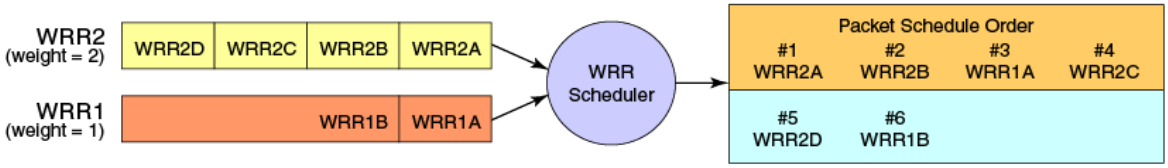

図 20-3　２つのキューでの WRR スケジューリング

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。

(3) トラフィッククラスのスケジューリングポリシー
トラフィッククラスは 0 から 7 の番号をもっており、大きい番号をもつトラフィッククラスは高い優先度として扱われます。内蔵 DCB スイッチでは、SP-to-WR キューの数を自由に決めることが出来ます。SP スケジューリングキューの数は N(SP1 から 8)の範囲で指定できます。その際、高い優先度のトラフィッククラスは SP サービスとして構成され、残りの 8 つは WRR サービスとなります。表 20-2 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 20-2　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 20-4 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。

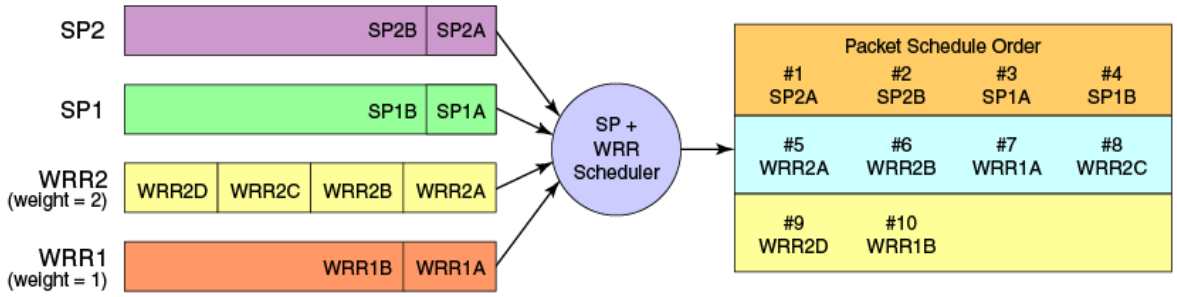

図 20-4　SP スケジューラと WRR スケジューラ

(4) マルチキャストキュースケジューリング

マルチキャストトラフィッククラスは 0 から 7 までの番号を持ち、大きい番号のトラフィッククラスは高い優先度として扱われます。マルチキャストトラフィッククラスから同等のユニキャストトラフィッククラスへの固定マッピングは、キュースケジューリングの振る舞いを選択するために適用されます。表 20-3 は、等価性マッピングが適用されたマルチキャストトラフィッククラスを示します。一旦、マルチキャストトラフィッククラスと同等のマッピングが適用されると、スケジューリングとスケジューラの構成は同等のユニキャストトラフィッククラスから継承されます。正確なマッピングの等価性の詳細については、表 20-3 を参照下さい。

表 20-3　マルチキャストトラフィッククラス同等のマッピング

マルチキャスト トラフィッククラス	等価ユニキャスト トラフィッククラス
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

ユニキャストのキューへの入力と出力は、SP+WRR サービスと同等のサービスレベルで複数の物理キューを同時にサポートする複合スケジューラを利用します。マルチキャストは、マルチキャスト拡張が追加キューに追加されます。マルチキャストトラフィッククラスはユニキャストのサービスレベルに相当しますので、それらはそれらと同等のユニキャストサービスポリシーとまったく同じように扱われています。

20.1.7　DCB での QoS

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。(VCS モードで、本 QoS 設定を使用します。)

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 20-4 は、デフォルトの DCB Priority Group Table 設定を示しています。

NOTE

PFC が有効になっている優先キューにマッピングできる CoS は一つだけです。CoS 番号は、優先キュー番号と同じにしておくべきです。もし、この制約を破った場合、エラーメッセージが表示され、Priority Group Table がデフォルト値に戻ります。

CEE マップが適用されているインタフェースが CNA と接続されると、絶対優先 PGID(PGID 15.0 ～ PGID 15.7)だけが許容されます。

表 20-4　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 20-5 は、デフォルト DCB Priority Table の設定を示します。

表 20-5　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

20.1.8　VCS ファブリック QoS

VCS ファブリック QoS は、わずかですがユーザー設定が必要です。変更する唯一のオプションは、ファブリックプライオリティとロスレスプライオリティだけです。

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。

(1) VCS モードのレイヤ 3 機能の制限事項

スイッチが VCS モードの時には、ロスレスプライオリティとファブリックプライオリティは、あらゆるレイヤ 3 QoS マーキングおよびクラスから分離される必要があります。したがって、スイッチが VCS モードで動作している時、特定の制限が一部のレイヤ 3 DSCP QoS 機能に適用されます。

以下は、VCS モードで適用可能なレイヤ 3 DSCP-Traffic-Class、DSCP-CoS マップ、およびの DSCP trust 機能を使用するための制限です。DSCP 変換マップは、VCS モードに影響されません。

- DSCP trust は、CoS trust で使用されるので VCS モードでは無効になります。
- VCS モードには、デフォルト DSCP マップがありません。DSCP trust がスタンドアロンモードで有効になっている場合、デフォルトのマップが発生します。
- 非デフォルトの DSCP-Traffic-Class マップには、次の制限があります。
  - DSCP 値は、Traffic Class 7 に分類することができません。

- DSCP 値は、デフォルト Traffic Class 3 によって、ロスレストラフィックを伝送キューに分類することができません。

- 非デフォルトの DSCP-CoS マップでは、次の制限があります。
  - DSCP 値は、CoS 7 にマークすることができません。
  - DSCP 値は、デフォルト CoS 3 によってロスレスプライオリティをマークすることができません。
- ロスレスプライオリティは、CEE マップを介して識別されます。
- DSCP ベースマーキングまたは分類を有効にするには、デフォルト以外の SCP-Traffic-Class マップと DSCP-CoS マップがインターフェースに適用されなければなりません。
- インターフェースに DSCP-Traffic-Class または ADSCP-CoS マップを適用するには、CoS およびトラフィッククラス値がロスレスプライオリティとして再マーキングする必要があります。例えば、DSCP-Traffic-Class マップ"abcd"が作成される時、それはデフォルトの内容を持つことになります。インターフェースに適用される時、ファブリックとロスレスプライオリティがマップで使用されることをエラーが表示し、インターフェースで適用することはできません。
- 有効な DSCP-Traffic-Class マップと DSCP-CoS マップがインタフェースに適用される時、DSCP trust が設定されているマップで有効にされます。

20.2 QoS の設定

20.2.1 QoS 設定の基本

NOTE
240 ページの『20.1.2 ユーザープライオリティマッピング』を参照してください。

(1) untrust インタフェースに対するデフォルトユーザープライオリティ
レイヤ 2 の QoS において、untrust に設定された場合は、デフォルトのユーザープライオリティである 0にマッピングされるのがデフォルトの動作です。これはベストエフォートであることを意味しています。
表 20-6 は、レイヤ 2 での QoS における untrust ユーザープライオリティのマッピングです。

表 20-6 untrust インタフェースのデフォルトユーザープライオリティ値

入力フレームの CoS 値	ユーザープライオリティ
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。

ユーザー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ープライオリティマッピングを上書きすることが出来ます。隣接デバイスが trust で、QoS 設定機能が利用できるならば、レイヤ 2 の QoS の信頼は CoS 値と IEEE802.1Q のデフォルトマッピングが適用されます。
表 20-7 は、802.1Q のデフォルトマッピングに準拠したレイヤ 2CoS ユーザー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ープライオリティテーブルを変更することが出来ます。

表 20-7　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	ユーザープライオリティ
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

(2) QoS マッピングの定義
(a) QoS の trust モードの設定
QoS の trust モードは入力トラフィックのユーザー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ープライオリティを設定します。もし、入力パケットが優先度付き tag フレームでなければ、デフォルトの CoS 値に戻ります。

NOTE
CEE マップがインタフェースに適用された場合、'qos trust'コマンドは使用できません。CEE マップは CoS trust モードのインタフェースに対して適用できます。

QoS trust モードを構成するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行します。
```
switch# configure terminal
```
2．イーサネットインタフェースを指定します。
```
switch(config)# interface TenGigabitEthernet 0/2
```
3．インタフェースモードを cos 'trust'に設定します。
スタンドアロンモードの場合：

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

VCS モードの場合：

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

NOTE

インタフェースから QoS trust モードを無効にするには、'no qos trust cos'を入力します。

4．特権実行モードに戻ります。

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

(b) CoS trust の確認

適用された CoS trust を確認するには、グローバルコンフィグレーションモードから次のコマンドを入力します。tengigabitethernet 0/2 は、インターフェース名です。

```
switch# do show qos interface tengigabitethernet 0/2
```

(c) ユーザープライオリティマッピングの設定

ユーザープライオリティマッピングを構成するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

2．イーサネットインタフェースを指定します。

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

3．インターフェースを優先度 3 に設定します。

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

(d) CoS-to-CoS 変換 QoS マップの作成

CoS-to-CoS 変換マップを作成するために特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

2．変換マップの名を指定してマップを作成します。下記の例では、"test"を使用しています。

```
switch(config)# qos map cos-mutation test 0 1 2 3 4 5 6 7
```

3．running-config file を startup-config file に格納するため、'do copy'コマンドを実行します。

```
switch(config)# do copy running-config startup-config
```

(e) CoS-to-CoS 変換 QoS マップの適用

CoS-to-CoS 変換 QoS マップを適用するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

2．イーサネットインタフェースを指定します。

```
switch(config)# interface TenGigabitEthernet 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。下記の例では"test"を使用しています。

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

NOTE

インターフェースからの変換マップを無効にするには、'no qos cos-mutation name'を入力します。

４．入力トラフィックに対して trust モードを指定します。

入力トラフィックのユーザープライオリティマッピングを適用する入力の QoS trust モードを指定するこのコマンドを使います。trust モードでない場合、全ての入力パケットのプライオリティは、インタフェースのデフォルト CoS 値で上書きされます。CoS モードは入力データの CoS 値に基づいてユーザー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
```

(f)　CoS-to-CoS 変換 QoS マップの確認

適用された QoS のマップを確認するには、グローバルコンフィグレーションモードから、次のオプションのいずれかまたは両方を使用することができます。

１．'do show qos maps cos-mutation'コマンドおよびマップ名を使用して、特定のマップのための QoS マッピングを確認します。

```
switch(config)# do show qos maps cos-mutation test
```

２．qos-mutation パラメータで'do show qos maps'コマンドを使用して、すべての QoS マッピングを確認します。

```
switch(config)# do show qos maps cos-mutation
```

(3) DSCP マップの定義

(a) DSCP trust モードの設定

QoS trust モードの様に、Differentiated Services Code Point(DSCP)trust モードは着信トラフィックのユーザー優先度マッピングを制御します。ユーザー優先度は、着信した DSCP 値に基づいています。この機能が有効になっていない場合、パケットの DSCP 値は無視されます。

DSCP 信頼が有効になっている時、表 20-8 は、デフォルト DSCP 優先度マッピングのユーザープライオリティを示しています。

表 20-8　デフォルト DSCP 優先度マッピング

DSCP 値	ユーザープライオリティ
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

NOTE

250 ページの『20.1.8 (1)VCS モードのレイヤ 3 機能の制限事項』のもとに、この機能の VCS モードでの使用の制限に注意してください。

DSCP trust モードを設定するには、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

2．イーサネットインタフェースを指定します。

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

3．インターフェースモードを'qos trust dscp'に設定します。

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

NOTE

インタフェースの DSCP trust モードを無効にするには、'no qos trust dscp'を入力します。

4．特権実行モードに戻ります。

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

(b)　DSCP trust モードの確認

適用された DSCP trust を確認するには、グローバルコンフィグレーションモードから次のコマンドを入力します。tengigabitethernet 10/0/2 は、インターフェース名です。

```
switch(config)# do show qos running-config interface TenGigabitEthernet 0/2
```

(c)　DSCP 変換マップの作成

NOTE

この機能は、BS2500 搭載 DCB スイッチモジュールでのみサポートされています。

DSCP 変換マップを作成し、受信パケットの受信 DSCP 値を送信 DSCP 値に再割り当てするために、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します。
```
switch# configure terminal
```
2．マップ名称を指定して DSCP 変換マップを作成します。次のコマンドは、マップ名称として"test"を使用し、トラフィッククラスに割り当てられるようシステムを DSCP 対応モードにします。
```
switch(config)# qos map dscp-mutation test
```
3．設定されたマップ(この場合は"dscp-mutation-test")に対してシステムが DSCP 変換モードになると、次の例のように'mark'コマンドを使って受信 DSCP 値を送信 DSCP 値に割り当てることが出来ます。
```
switch(dscp-mutation-test)# mark 1,3,5,7 to 9
switch(dscp-mutation-test)# mark 11,13,15,17 to 19
switch(dscp-mutation-test)# mark 12,14,16,18 to 20
switch(dscp-mutation-test)# mark 2,4,6,8 to 10
```
上記は次を設定したものです。
- DSCP 値：1,3,5,7 を DSCP9 として出力するよう設定
- DSCP 値：11,13,15,17 を DSCP19 として出力するよう設定
- DSCP 値：12,14,16,18 を DSCP20 として出力するよう設定
- DSCP 値：2,4,6,8 を DSCP10 として出力するよう設定

4．startup-config ファイルに running-config ファイルを格納するため'do copy'コマンドを入力します。
```
switch(config)# do copy running-config startup-config
```

(d) DSCP 変換マップのインタフェースへの適用

インタフェースに設定した DSCP 変換マップを適用するため、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します。
```
switch# configure terminal
```
2．インタフェースを指定します。
```
switch(config)# interface TenGigabitEthernet 2/0/2
```
3． DSCP 変換マップへの変更を有効化またはインタフェースへ適用します。この例では、"test"がマップ名称です。
```
switch(conf-if-te-2/0/2)# qos dscp-mutation test
```

NOTE

インタフェースからマップを無効化するには、'no qos dscp-mutation name'を入力します。

4．受信を DSCP trust モードに指定します。

スタンドアロンモードの場合：
```
switch(conf-if-te-2/0/2)# qos trust dscp
```
VCS モードの場合：
```
switch(conf-if-te-2/0/2)# qos dscp-cos test
switch(conf-if-te-2/0/2)# qos dscp-traffic-class test
```
5．特権実行モードに戻ります。
```
switch(conf-if-te-2/0/2)# end
```
6．startup-config ファイルに running-config ファイルを格納するため'do copy'コマンドを入力します。
```
switch# copy running-config startup-config
```

(e) DSCP 変換マップの確認

適用された DSCP マップを確認するために、グローバルコンフィグレーションモードから次のいずれかのオプションを使用します。;

- 'do show qos maps dscp-mutation'コマンドとマップ名称を使って、指定されたマップに対する DSCP マッピングを確認します。

```
switch(config)# do show qos maps dscp-mutation test
```

- マップ名称を指定せず'do show qos maps dscp-mutation'コマンドを使って、全ての DSCP マッピングを確認します。

```
switch(config)# do show qos maps dscp-mutation
```

- 'do show qos interface'コマンドを使って、指定されたインタフェースに DSCP 変換マッピングを確認します。

```
switch(config)# do show qos interface te 3/1/2
```

(4) DSCP-to-CoS マッピングの定義

(a) DSCP-to-CoS 変換マップの作成

入力インタフェースで DSCP-to-COS 変換マップを設定することにより、発信 802.1P CoS プライオリティ値を再割り当てするために、入力パケットの着信 DSCP 値を使用することができます。次の手順を使用してください。

NOTE

250 ページの『20.1.8 (1)VCS モードのレイヤ 3 機能の制限事項』を参照し、この機能の VCS モードでの使用の制限に注意してください。

1．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

2．マップ名を指定して、dscp-to-cos マップを作成します。DSCP 値を CoS 値にマップすることができるように、以下のコマンドはマップ名として"test"を使用し、dscp-cos マップモードでシステムを置きます。

```
switch(configure)# qos map dscp-cos test
```

3．一旦、システムが設定されマップに対する dscp-cos マップモードとなったら、次の例のように'mark'コマンドを使用して、送信 CoS プライオリティ値に着信 DSCP 値をマッピングすることができます。

```
switch(dscp-cos-test)# mark 1,3,5,7 to 3
switch(dscp-cos-test)# mark 11,13,15,17 to 5
switch(dscp-cos-test)# mark 12,14,16,18 to 6
switch(dscp-cos-test)# mark 2,4,6,8 to 7
```

これは、以下をセットします：

・DSCP 値 1、3、5、7 は CoS プライオリティ 3 として出力に設定されています。

・DSCP 値 11、13、15、17 は CoS プライオリティ 5 として出力に設定されています。

・DSCP 値 12、14、16、18 は CoS プライオリティ 6 として出力に設定されています。

・DSCP 値 2、4、6、8 は CoS プライオリティ 7 として出力に設定されています。

4．running-config file を startup-config file に格納するため、'copy'コマンドを実行します。

```
switch(dscp-cos-test)# end
```

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

(b) インターフェースへの DSCP-to-CoS マップの適用

インタフェースへの DSCP-to-CoS 変換マップを適用するには、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに移行します。
```
switch# configure terminal
```
2．イーサネットインタフェースを指定します。
```
switch(config)# interface TenGigabitEthernet 0/2
```
3．DSCP-to-CoS 変換マップに加えられた変更をアクティブにして適用します。下記の例では"test"を使用しています。
```
switch(conf-if-te-0/2)# qos dscp-cos test
```

NOTE

インタフェースからマップを無効にするには、'no qos dscp-cos name'を入力します。

4．着信トラフィックの DSCP trust モードを指定します。
受信インタフェースを DSCP trust モードに指定するためこのコマンドを使用します。これにより、着信トラフィックのユーザー優先度マッピングを制御することができます。untrust モードは、DSCP に基づいてパケットを分類しません。DSCP trust モードでは、着信した DSCP 値に基づいてパケットを分類します。着信パケットがタグ付けされた優先度である場合は、頼れるものは、CoS 値に基づいてパケットを分類することです。
```
switch(conf-if-te-0/2)# qos trust dscp
```
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
```

(c) DSCP-to-CoS 変換マップの確認

DSCP-to-CoS マップを確認するには、グローバルコンフィグレーションモードから次のオプションのいずれかまたは両方を使用することができます。

1．'do show qos maps dscp-cos'コマンドおよびマップ名を使用して、特定のマップに DSCP マッピングを確認します。
```
switch(config)# do show qos maps dscp-cos test
```
2．dscp-cos パラメータのみで'do show qos maps'コマンドを使用して、すべての DSCP マッピングを確認します。
```
switch(config)# do show qos maps dscp-cos
```
3．'do show qos interface'コマンドを使用してインターフェースを指定することにより、インターフェースの DSCP-to-CoS 変換マッピングを確認します。
```
switch(config)# do show qos interface te 0/2
```

(5) 柔軟性のためのトラフィッククラスマップの設定

キュー選択に追加の柔軟性が必要な場合は、259 ページの『20.2.2 トラフィッククラスマッピング』を参照してください。

20.2.2　トラフィッククラスマッピング

内蔵 DCB スイッチは、アプリケーションデータの異なる優先度に対して、分離とサービス制御のために８つのユニキャストトラフィッククラスをサポートしています。トラフィッククラスは０から７に割り当てられます。大きい番号ほど高い優先度となります。

トラフィッククラスマッピングの段階では、キュー選択を行います。

- マッピングとは、例えば１バイト(256 値)のユーザープライオリティを 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。
- ユーザー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 20-9 は、IEEE802.1Q のデフォルトマッピングに準拠するための CoS ベースユーザー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 20-9　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ープライオリティ

ユーザープライオリティ	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適用されます。

(2) マルチキャストトラフィック

内蔵 DCB スイッチは、アプリケーションデータの異なる優先度に対する分離とサービス制御のために８つのマルチキャストトラフィッククラスをサポートしています。トラフィッククラスは０から７に割り当てられます。大きい番号ほど高い優先度となります。トラフィッククラスマッピングの段階では、キュー選択を行います。

表 20-10 は、IEEE802.1Q のデフォルトマッピングに準拠するための CoS ベースユーザー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 20-10　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ープライオリティ

ユーザープライオリティ	トラフィッククラス
0	1
1	0
2	2
3	3
4	4
5	5
6	6
7	7

一旦トラフィッククラスマッピングが実行されると、入出力ポートの全てのキューイングに対して絶えず適用されます。'CoS-to-traffic class-map'または'DSCP-to-traffic class-map'のいずれかでインタフェースを設定できます。

(3) CoS-to-traffic-class マップの設定

CoS-to-traffic-class マップを設定する場合は、次に示すトピックを考慮して下さい。

(a) CoS-to-Traffic-Class マッピング

CoS-to-Traffic-Class をマッピングするため、特権実行モードから次の手順を実行してください。

NOTE

CoS-to-Traffic-class-map の作成は、スタンドアロンモードだけで利用できます。

1．グローバルコンフィグレーションモードに入ります。

```
switch# configure terminal
```

2．名称とマッピングを指定することにより、CoS-Traffic-Class マッピングを作成します。

```
switch(config)# qos map cos-traffic-class test 1 0 2 3 4 5 6 7
```

3．特権実行モードに戻ります。

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

4．running-config file を startup-config file に格納するため、'copy'コマンドを実行します。

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

(b) インタフェースへの CoS-to-Traffic-Class マッピングの適用

CoS-to-Traffic-Class マッピングを有効化するため、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに入ります。

```
switch# configure terminal
```

2．インタフェースを指定します。

```
switch(config)# interface TenGigabitEthernet 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。下記の例では"test"を使用しています。

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

NOTE

インタフェースからの変換マップを無効にするには、'no qos cos-traffic-class'を入力します。

４．特権実行モードに戻ります。

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

(c) CoS-to-Traffic-Class マッピングの確認

CoS-to-Traffic-Class のマッピングを確認するには、グローバルコンフィグレーションモードから、次のオプションのいずれかまたは両方を使用することができます。

- 'do show qos maps cos-traffic-class'コマンドを使用し、マップ名を指定して、CoS-Traffic-Class マッピングを確認します。

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

- cos-traffic-class だけの'do show qos maps'コマンドを使用して、すべての COS-to-Traffic-Class マッピングを確認します。

```
switch(config)# do show qos maps cos-traffic-class
```

- 'show qos interface'コマンドを使用しインタフェースを指定して、インタフェースのための CoS-Traffic-Class のマッピングを確認します。

```
switch(config)# do show qos interface te 0/2
```

(4) Configuring DSCP-to-traffic-class maps

DSCP-to-traffic-class マップを設定する場合は、次に示すトピックを考慮して下さい。

(a) DSCP-to-Traffic-Class マッピング

入力 DSCP 値は、DSCP-to-Traffic-Class マップを使用して、入力インターフェースのトラフィックを特定のトラフィッククラスに分類するために使用することができます。DSCP-to-Traffic-Class をマッピングするには、特権実行モードで次の手順を実行します。

NOTE

250 ページの『20.1.8 (1)VCS モードのレイヤ 3 機能の制限事項』を参照し、この機能の VCS モードでの使用の制限に注意してください。

１．グローバルコンフィグレーションモードに入ります。

```
switch# configure terminal
```

２．以下のコマンドは、作成したマップのマッピングを設定することができるように、マップ名として"test"を使用し、dscp-traffic-class モードに移行します。

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

３．一旦、システムが設定されマップのための dscp-traffic-class モード(このケースでは、dscp-traffic-class-test)になったら、次の例のようにマークパラメータを使用して、トラフィック

クラスに DSCP 値をマッピングすることができます。

```
switch(dscp-traffic-class-test) mark 1,3,5,7 to 3
switch(dscp-traffic-class-test) mark 11,13,15,17 to 5
switch(dscp-traffic-class-test) mark 12,14,16,18 to 6
switch(dscp-traffic-class-test) mark 2,4,6,8 to 7
```

これは、以下をセットします：

・DSCP 値 1、3、5、7 はトラフィッククラス 3 にマッピングされます。

・DSCP 値 11、13、15、17 はトラフィッククラス 5 にマッピングされます。

・DSCP 値 12、14、16、18 はトラフィッククラス 6 にマッピングされます。

・DSCP 値 2、4、6、8 はトラフィッククラス 7 にマッピングされます。

４．特権実行モードに戻ります。

```
switch(dscp-traffic-class-test) end
```

５．running-config file を startup-config file に格納するため、'copy'コマンドを実行します。

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

(b) インタフェースへの DSCP-to-Traffic-Class マッピングの適用

DSCP-to-Traffic-Class マッピングを有効にするには、特権実行モードで次の手順を実行します。

１．グローバルコンフィグレーションモードに入ります。

```
switch# configure terminal
```

２．インタフェースを指定します。

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

３．DSCP-to-Traffic-Class マッピングを有効にします。この場合、"test"がマップ名です。

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

NOTE

インタフェースから DSCP-to-Traffic クラスマップを無効にするには、'no qos dscp-traffic-class name' を入力します。

４．特権実行モードに戻ります。

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

(c) DSCP-to-Traffic-Class マッピングの確認

DSCP-to-Traffic-Class マッピングを確認するには、グローバルコンフィグレーションモードから、次のオプションのいずれかまたは両方を使用することができます。

- 'do show qos maps dscp-traffic-class'コマンドを使用し、マップ名を指定して、DSCP-Traffic-Class マッピングを確認します。

```
switch(config)# do show qos maps dscp-traffic-class test
```

- dscp-traffic-class パラメータだけの'do show qos maps'コマンドを使用して、すべての DSCP-Traffic-Class マッピングを確認します。

```
switch(config)# do show qos maps dscp-traffic-class
```

- 'do show qos interface'コマンドを使用し、インタフェースを指定して、インタフェースのための DSCP-to-Traffic-Class マッピングを確認します。

```
switch(config)# do show qos interface te 0/2
```

20.2.3　輻輳制御機能の設定

(1) TailDrop 閾値の変更

NOTE
本機能は BS2500 向け内蔵 DCB スイッチのみのサポートとなります。

Tail drop の閾値を変更するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに入ります。
```
switch# configure terminal
```
2．各マルチキャストトラフィッククラスに対する Tail drop 閾値を変更します。例では、1000pkt が使われています。
```
switch(config)# qos rcv-queue multicast threshold 1000 1000 1000 1000 1000 1000 1000 1000 1000
```
3．特権実行モードに戻ります。
```
switch(config)# end
```
4．running-config file を startup-config file に格納するため、'copy'コマンドを実行します。
```
switch# copy running-config startup-config
```

(2) Random Early Discard(RED)の設定

NOTE
本機能は BS2500 向け内蔵 DCB スイッチのみのサポートとなります。

(a) RED プロファイル

RED を設定する場合は、次の点を考慮してください。

- trunk ポートは、帯域がアクティブリンクの数に従って変更されるので、他のポートと RED プロファイルを共有することは出来ません。
- RED プロファイルのキュー閾値がパーセントで設定された場合、スイッチはポートスピードに依存してアロケートされたバッファに、トータルバイト数を設定します。
- 最大で 384 RED プロファイルをサポートしています。

リンクアグリゲーション(LAG)に対する RED プロファイル使う場合次の点を考慮してください。

- RED プロファイルは LAG インタフェースに適用することが出来ます。しかし、プロファイルは LAG の個々のメンバインタフェースに設定されます。

(b) RED プロファイルの設定

出力の RED 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．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．RED プロファイルを設定します。この場合は、プロファイル ID に 10 を使っています。'min-threshold','max-threshold','drop-probability'はパーセントで指定しています。
```
switch(config)# qos red-profile 10 min-threshold 10 max-threshold 80 dropprobability 80
```

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
```

(c) CoS 値をインタフェースの RED プロファイルに割り当てる

ポートの CoS 値を 263 ページの『20.2.3 (2)(a) RED プロファイル』で作成した RED プロファイルに割り当てるため、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入ります。

```
switch# configure terminal
```

２．インタフェースを指定します。

```
switch(config)# interface TenGigabitEthernet 1/0/2
```

３．ポートの CoS 値を使ってプロファイルを割り当てます。次の例は、Cos 値 3 を RED プロファイル ID10 に割り当てています。

```
switch(conf-if-te-1/0/2)# qos random-detect cos 3 red-profile-id 10
```

NOTE

インタフェースからマップを無効化するには、'`no qos random-detect cos value`'コマンドを使用します。

４．特権実行モードに戻ります。

```
switch(conf-if-te-1/0/2)# 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
```

(d) RED プロファイルの確認

'`show qos red profiles`'コマンドを使って、設定された RED プロファイルを確認します。

```
switch# show qos red profiles
```

'`show qos interface interface-name`'コマンドを使って、インタフェースに適用された RED プロファイルをテストします。これは、RED プロファイルだけでなく、DSCP trust, DCSP-to-DSCP マップ, CoS-Traffic クラスマップなどのようにインタフェースに適用された QoS 設定も表示します。

```
switch# show qos red statistics interface tengigabitethernet 1/0/2
```

(3) フロー制御の設定

本設定は、イーサネット pause フレームを有効にすることに加えて、フロー制御の設定をします。接続先のフロー制御パラメータも設定し、オプションは"auto"のままにすることを推奨します。

243 ページの『20.1.4 イーサネット Pause(Ethernet pause』を参照してください。イーサネット pause のオプションはスタンドアロンモードでのみ利用できます。

(a) イーサネット Pause の有効化

ここでは、フロー制御を設定し、加えてイーサネットポーズフレームを有効にします。接続しているデバイスでフロー制御パラメータを設定し、オプションを"auto"にしたままとすることをお勧めします。

NOTE
イーサネット Pause オプションは、スタンドアロン・モードでのみ使用できます。

イーサネット Pause を有効化するために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに入ります。
```
switch# configure terminal
```
2．イーサネットインタフェースを指定します。
```
switch(config)# interface TenGigabitEthernet 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
```

NOTE
インタフェースのイーサネット Pause を無効にするには、'no qos flowcontrol'を入力します。

4．特権実行モードに戻ります。
```
switch(conf-if-te-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
```

(b) イーサネット PFC の有効化

イーサネット PFC を有効にするには、特権実行モードで次の手順を実行します。

1．グローバルコンフィグレーションモードに入ります。
```
switch# configure terminal
```
2．イーサネットインタフェースを指定します。
```
switch(config)# interface TenGigabitEthernet 0/2
```
3．インタフェースのイーサネット PFC を有効にします。
```
switch(conf-if-te-0/2)# qos flowcontrol pfc 3 tx on rx on
```

NOTE
インタフェースのイーサネット PFC を無効にするには、'no qos flowcontrol pfc cos value'を入力します。

4．特権実行モードに戻ります。
```
switch(conf-if-te-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
```

20.2.4　マルチキャストレート制限の設定

NOTE
本機能は BS2500 向け内蔵 DCB スイッチのみのサポートとなります。

受信キューのマルチキャストレート制限を設定するために、特権実行モードから次の手順を実行してください。

1．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
```

20.2.5　BUM ストーム制御の設定

NOTE

本機能は BS2500 向け内蔵 DCB スイッチのみのサポートとなります。

interface 101/0/2にブロードキャストに対して1000000bpsのレートリミットでストーム制御を設定するため、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．トラフィックを制御したいインタフェースを指定します。

```
switch(config)# interface tengigabitethernet 101/0/2
```

3．インタフェースにブロードキャストのリミットを設定するため、'storm-control ingress'コマンドを実行します。

```
switch(conf-if-te-101/0/2)# storm-control ingress broadcast 1000000
```

4．'show storm-control'コマンドで設定を確認してください。

```
switch(conf-if-te-101/0/2)# do show storm-control
```

- Interface　Type　　rate (Mbps) conformed　　violated　　total

```
Te102/4/1  broadcast         100,000      12500000000 12500000000 25000000000
Te102/4/1  unknown-unicast  100,000      12500000000 12500000000 25000000000
Te102/4/1  multicast         100,000      12500000000 12500000000 25000000000
Te102/4/2  broadcast         100,000      12500000000 12500000000 25000000000
Te102/4/3  broadcast         100,000      12500000000 12500000000 25000000000
Te102/4/4  unknown-unicast  100,000      12500000000 12500000000 25000000000
```

NOTE

インタフェースのストーム制御を無効にするには、'no storm-control ingress'コマンドに続いて、モード(broadcast, unknown-unicast, multicast)、 リミット(limit-bps,r limit-percent)、レート、オプションの monitor か shutdown を指定してください。

20.2.6　スケジューリングの設定

(1) 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 1 dwrr 10 20 20 10 10 10 10 10
```

3．特権実行モードに戻ります。

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

4．running-config file を startup-config file に格納するため、'copy'コマンドを実行します。

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

(2) QoS マルチキャストキューのスケジューリング

QoS マルチキャストキューをスケジューリングするために、特権実行モードから次の手順を実行してください。

1．グローバルコンフィグレーションモードに入ります。

```
switch#configure terminal
```

2．利用するスケジュールポリシーと帯域マッピングに対するトラフィッククラスを指定します。

```
switch(config)# qos queue multicast scheduler dwrr 10 20 20 10 10 10 10 10
```

3．特権実行モードに戻ります。

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

4．running-config file を startup-config file に格納するため、'copy'コマンドを実行します。

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

20.2.7　DCB QoS の設定

267 ページの『20.2.7 DCB QoS の設定』を参照してください。

(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-cee-map-default)# 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
```

(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。

以下の例では、２つの Priority Group を用意し、Priority Group 1 (PG1)に帯域 90%を割り当て、PFC 機能を有効化します。Priority Group 2 (PG2)に残りの帯域 10%を割り当て、PFC 機能を無効化する例を示します。

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．DCB マップを生成します。マップ名称は"default"だけが使えます。

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

3．PGID 2 の DCB マップを定義します。

```
switch(config-cee-map-default)# priority-group-table 2 weight 50 pfc off
```

CEE マップ中で定義される PG の合計帯域が 100%を超えないよう設定する必要があります。

4．PGID 1 の DCB マップを定義します。

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

５．特権実行モードに戻ります。

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

６．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

(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。

以下の例では PG1 に QoS 値５を、PG2 に QoS 値５以外の値を設定します。

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．'cee-map'コマンドを使用して定義するために、DCB マップの名前を指定します。この例では、"default"で使用されています。

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

３．マップを定義します。

```
switch(config-cee-map)# priority-table 2 2 2 2 2 1 2 15.0
```

NOTE

priority-table の定義の詳細については、『Network OS Command Reference』の'cee-map (configuration)'コマンドを参照してください。

４．特権実行モードに戻ります。

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

５．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

(4) インタフェースへの DCB プロビジョニングマップの適用

DCB プロビジョニングマップを適用するために、特権実行モードから次の手順を実行してください。

１．グローバルコンフィグレーションモードに移行します。

```
switch# configure terminal
```

２．イーサネットインタフェースを指定します。この例では、101/0/2 を使っています。

```
switch(config)# interface tengigabitethernet 101/0/2
```

３．インタフェースに DCB マップを適用します。

```
switch(conf-if-te-101/0/2)# cee default
```

NOTE

インタフェースのマップを無効にするには、'no cee'を入力します。

４．特権実行モードに戻ります。

```
switch(conf-if-te-101/0/2)# end
```

５．running-config を startup-config へ格納するため、'copy'コマンドを入力します。

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

(5) DCB マップの確認

CoS DCB マップを確認するには、グローバルコンフィグレーションモードから'show cee maps default'コマンドを使用します。

```
switch# show cee maps default
CEE Map 'default'
   Precedence: 1
   Remap Fabric-Priority to Priority 0
   Remap Lossless-Priority to Priority 0
   Priority Group Table
     1:  Weight 90, PFC Enabled, BW% 90
     2:  Weight 10, PFC Disabled, BW% 10
     15.0: PFC Disabled
     15.1: PFC Disabled
     15.2: PFC Disabled
     15.3: PFC Disabled
     15.4: PFC Disabled
     15.5: PFC Disabled
     15.6: PFC Disabled
     15.7: PFC Disabled
   Priority Table
      CoS:    0    1    2    3    4    5    6    7
     ----------------------------------------
     PGID:    2    2    2    2    2    1    2 15.0
   Enabled on the following interfaces:
```

20.2.8　VCS ファブリックの QoS 設定

(1) VCS ファブリック QoS の設定

VCS ファブリックで再設定されるプライオリティを設定するため、グローバルコンフィグレーションモードから次の手順を実行してください。

1．CEE マップコンフィグレーションモードに移行するため、'cee-map'コマンドを入力します。

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

2．VCS ファブリック QoS のロスレスプライオリティを設定するため、'remap lossless priority'コマンドを使用します。デフォルトロスレスプライオリティは 0 です。

```
switch(config-cee-map-default)# remap lossless-priority priority 2
```

3．VCS ファブリック QoS のファブリックプライオリティを設定するため、'remap fabric priority'コマンドを使用します。デフォルトファブリックプライオリティは 0 です。

```
switch(fabric-cee-map-default)# remap fabric-priority priority 2
```

4．グローバルコンフィグレーションモードに戻るため'exit'コマンドを使います。

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

5．受信データインタフェースを指定します。

```
switch(config)# interface tengigabitethernet 22/0/1
```

6．インタフェースに CEE プロビジョニングマップを適用します。

```
switch(conf-if-te-22/0/1)# cee default
```

21 SFP breakout モードの設定

21.1 SFP breakout 概要

SFP breakout は、新しいポート設定パラメータです。Breakout インタフェースは、breakout SFP 上に生成されます。生成されるインタフェースの数は、SFP タイプによります。例えば、QSFP が breakout モードではない場合、単一の 40Gbps インタフェースだけが存在します。しかし、QSFP の breakout モードが有効な場合、４つの 10Gbps インタフェースが生成されます。これらのインタフェースは、breakout モードが有効か否かに係わらず、breakout 機能を持たない標準的な SFP 上に生成されるインタフェースと同様に管理され動作します。

ISL(ファブリック間接続)は、breakout モードでも利用できます。breakout インタフェースのデフォルト管理ステータスは、有効です。

21.1.1 Breakout mode properties

breakout インタフェースは、基本的に標準のインタフェースでサポートされる全ての動作・設定をサポートします。(271 ページの『21.1.4 breakout モードの制限』に示す一部の例外を除きます。)つまり、次の特性を持ちます。

- インタフェース独自に管理状態・動作状態を持ちます。
- インタフェース独自に統計情報を持ちます。
- 標準の SFP インタフェースに定義可能な全ての設定が可能です。
- port-channel や vLAG を構成することが出来ます。

SFP のデフォルト状態は、"no breakout"です。

21.1.2 breakout モードのサポート

次の表は、breakout モードをサポートするスイッチの一覧です。

表 21-1 Breakout モードをサポートするスイッチ

スイッチ種	ポート構成	QSFP ポート数
BS2500 内蔵 DCB スイッチ	10Gbps 56 ポート 40Gbps 2 ポート	2 ポート (40Gb activate license が必要)

21.1.3 breakout モードインタフェース

SFP コネクタ ID は、フロントパネルの SFP の位置を示し、インタフェース名称の port ID として使用されます。コネクタ ID は、breakout モードの設定変更の結果、どのインタフェースが生成または削除されるか示します。このコネクタの全てのインタフェースは、コマンド実行前に無効にしなければな

りません。breakout モードが有効な SFP 上に生成されるインタフェースは、インタフェース名称に続いてコロン(:)とともに数字が付加されます。
この命名規則で、ポートが breakout モードであることを判別できます。例えば、breakout モードではない QSFP を持つ RBridge ID 3 のノードのポートを考えます。もし、breakout が有効にされれば、既存のインタフェース Fo 3/0/1 が削除され、４つの新しいインタフェース、Te 3/0/1:1, Te 3/0/1:2, Te 3/0/1:3, Te 3/0/1:4 が生成されます。インタフェースが削除されると、このインタフェースのいずれの設定も削除されます。生成された新しいインタフェースは、デフォルトのポート設定となっています。
もし、breakout モードが無効に設定されると、４つの Te interface は削除され、一つの Fo interface が生成されます。コマンドを実行する条件は、インタフェースが shutdown 状態の時のみであり、有効にするにはスイッチの再起動(reload)が必要です。
次の表は、breakout モードの SFP の例とインタフェース名称を示しています。

表 21-2　SFP Breakout 設定値

SFP # (rbridge/slot/port)	SFP タイプ	インタフェース名称	
		Breakout 無効	Breakout 有効
3/2/1	QSFP (4 x10G)	Fo 3/0/1	Te 3/0/1:1
			Te 3/0/1:2
			Te 3/0/1:3
			Te 3/0/1:4

21.1.4　breakout モードの制限

ほとんどの環境では、breakout インタフェースはポート属性と状態の観点で非 breakout(通常の)インタフェースと同じ動作となります。各 breakout インタフェースは、管理状態と動作状態と統計情報を持っています。例外は、物理層の情報で、breakout インタフェース毎の情報を持っていません。

- SFP 媒体

  breakout モードでは、SFP 自身のものとなり、breakout メディア毎の情報はありません。'show media'コマンドは、全ての breakout インタフェースに対して同じメディア情報を表示します。

NOTE
40G モジュールでは、'show media'コマンドの TX Power フィールドはサポートしていません。

- LED 状態

  breakout インタフェースの LED 状態とインタフェースの状態を次表に示します。

表 21-3　breakout インタフェースの LED

LED 状態	インタフェース状態
消　灯	トランシーバが挿入されていないか、ケーブル未接続か、有効化されているがリンクダウンしている
緑点灯	リンクアップしている
橙点滅	無効化(shutdown 設定)されている

21.2　breakout モードの設定

ASIC のリソースを再割り当てする必要があるため、SFP モードの変更はポートの再起動が必要です。次の設定を行う前に、SFP インタフェースを shutdown 状態にしなければなりません。

それぞの SFP に対して次の設定手順を実行してください。

1．SFP 上に存在する全てのインタフェースを停止します。
   a．breakout モードを無効にするため、４つの Te interface(10Gbps)を shutdown します。
   b．breakout モードを有効にするため、ひとつの Fo interface(40Gbps)を shutdown します。
2．対象ポートに'SFP breakout'コマンドを実行します。
   a．対象ポートが QSFP の場合は、breakout モードを無効化した結果、４つの Te interface(10Gbps)は削除され、breakout モードを有効化した結果、ひとつの Fo interface(40Gbps)が削除されます。対象以外の設定には影響有りません。
3．全ての SFP が設定された後、running-config ファイルを startup-config ファイルにコピーしてください。(これは、スタンドアロンモードとファブリッククラスタモードの場合実行します。)
   a．スタンドアロンモードまたはファブリッククラスタモードの場合、running-config を startup-config に格納しなければなりません。SFP 設定は、reboot 後に使用される startup-config に格納されなければなりません。
   b．ロジカルシャーシクラスタモードならば、running-config を startup-config にコピーする必要はありません。
4．スイッチをリブートします。
   a．ポート毎に SFP breakout モードに対応したインタフェースが生成されます。QSFP の場合、breakout 無効化設定なら一つの Fo interface が生成され、breakout 有効化設定なら４つの Te interface が生成されます。
   b．システムが初めて立ち上がったかのように、デフォルトのコンフィグレーションで、新しいモードの SFP インタフェースが使用できます。影響のないインタフェースは、reboot 前のコンフィグレーションのままです。

21.3　追加の breakout モードシナリオの設定

次のコンフィグレーションサンプルは、40G QSFP を breakout モードに設定する方法、breakout モード中に 40G QSFP ポートを予約する方法、breakout モード中に 40G QSFP ポートを開放する方法を示

しています。

21.3.1　40G QSFP ポートを breakout モードに設定する

次の例は、40G QSFP ポートを breakout モードに設定し、任意に 40G ポートの DPOD 設定を予約・開放する方法を示しています。

NOTE

'copy default-config startup-config'コマンドがロジカルシャーシクラスタモードで実行されると、breakout インタフェース設定は失われます。breakout モードにするには、40G ポートを shutdown し、コンフィグレーションのリストアを実行してください。もし、リストア中ポートが shutdown でない場合、手動で breakout モードを設定しなければなりません。

```
switch# config
Entering configuration mode terminal

switch(config)# interface FortyGigabitEthernet 48/0/49

switch(conf-if-fo-48/0/49)# shut

switch(conf-if-fo-48/0/49)# exit

switch(config)# hardware

switch(config-hardware)# connector 48/0/49

switch(config-connector-48/0/49)# sfp breakout
%Warning: Sfp Breakout is a disruptive command.
 Please save the running-config to startup-config and a power-cycle for the changes
to take place.

switch(config-connector-48/0/49)# do copy running-config startup-config
This operation will modify your startup configuration. Do you want to continue? [y/
n]:y

switch(config-connector-48/0/49)# do reload
Warning: Unsaved configuration will be lost. Please run `copy running-config startup-
config` to save the current configuration if not done already.
Are you sure you want to reload the switch? [y/n]:y

The system is going down for reload NOW !!
switch# show ip int br
Interface                      IP-Address     Vrf                Status
Protocol
============================   ==========     ================   =========
=========
FortyGigabitEthernet 48/0/50   unassigned     default-vrf        up down
FortyGigabitEthernet 48/0/51   unassigned     default-vrf        up down
FortyGigabitEthernet 48/0/52   unassigned     default-vrf        up down
TenGigabitEthernet 48/0/1      unassigned     default-vrf        up up (ISL)
TenGigabitEthernet 48/0/2      unassigned     default-vrf        up down
TenGigabitEthernet 48/0/3      unassigned     default-vrf        up down

TenGigabitEthernet 48/0/47     unassigned     default-vrf        up down
TenGigabitEthernet 48/0/48     unassigned     default-vrf        up down
TenGigabitEthernet 48/0/49:1   unassigned     default-vrf        up down(ISL)
TenGigabitEthernet 48/0/49:2   unassigned     default-vrf        up down(ISL)
TenGigabitEthernet 48/0/49:3   unassigned     default-vrf        up down(ISL)
TenGigabitEthernet 48/0/49:4   unassigned     default-vrf        up down(ISL)
Vlan 1                         unassigned     administratively   down down
Vlan 4093                      unassigned                        up down
Vlan 4095                      unassigned     administratively   down down
```

21.3.2　breakout モード中に 40G QSFP ポートを予約する

次の例は、breakout モード中に 40G QSFP ポートを予約する方法を示しています。

```
switch# config
Entering configuration mode terminal

switch(config)# dpod 48/0/
Possible completions:
  1   2   3   4   5   6   7   8   9   10  11  12  13  14  15  16  17  18  19
  20  21  22  23  24  25  26  27  28  29  30  31  32  33  34  35  36  37  38
  39  40  41  42  43  44  45  46  47  48  49  50  51  52

switch(config)# dpod 48/0/49:1 reserve
Invalid InterfaceId.

switch(config)# dpod 48/0/49 reserve

switch(config-dpod-48/0/49)# do show dpod
rbridge-id: 48
   48 10G ports are available in this switch
    4 40G ports are available in this switch
   10G Port Upgrade license is installed
   40G Port Upgrade license is installed
     Dynamic POD method is in use
  48 10G port assignments are provisioned for use in this switch:
        24 10G port assignments are provisioned by the base switch license
        24 10G port assignments are provisioned by the 10G Port Upgrade license
   2 10G ports are assigned to installed licenses:
         2 10G ports are assigned to the base switch license
         0 10G ports are assigned to the 10G Port Upgrade license
  10G ports assigned to the base switch license:
     48/0/1, 48/0/31
  10G ports assigned to the 10G Port Upgrade license:
     None
  10G ports not assigned to a license:
     48/0/2, 48/0/3, 48/0/4, 48/0/5, 48/0/6, 48/0/7, 48/0/8, 48/0/9, 48/0/10, 48/0/11
     48/0/12, 48/0/13, 48/0/14, 48/0/15, 48/0/16, 48/0/17, 48/0/18, 48/0/19, 48/0/20,
48/0/21
     48/0/22, 48/0/23, 48/0/24, 48/0/25, 48/0/26, 48/0/27, 48/0/28, 48/0/29, 48/0/30,
48/0/32
     48/0/33, 48/0/34, 48/0/35, 48/0/36, 48/0/37, 48/0/38, 48/0/39, 48/0/40, 48/0/41,
48/0/42
     48/0/43, 48/0/44, 48/0/45, 48/0/46, 48/0/47, 48/0/48
  46 license reservations are still available for use by unassigned ports
   4 40G port assignments are provisioned for use in this switch:
         0 40G port assignments are provisioned by the base switch license
         4 40G port assignments are provisioned by the 40G Port Upgrade license
   2 40G ports are assigned to installed licenses:
         0 40G ports are assigned to the base switch license
         2 40G ports are assigned to the 40G Port Upgrade license
  40G ports assigned to the base switch license:
     None
  40G ports assigned to the 40G Port Upgrade license:
     48/0/49, 48/0/50
  40G ports not assigned to a license:
     48/0/51, 48/0/52
   2 license reservations are still available for use by unassigned ports
```

21.3.3　breakout モード中に 40G QSFP ポートを開放する

次の例は、breakout モード中に 40G QSFP ポートを開放する方法を示しています。

```
switch(config-dpod-48/0/49)# dpod 48/0/49 release
Port should be Offline to change POD assignment.
switch(config-dpod-48/0/49)# exit
switch(config)# interface TenGigabitEthernet 48/0/49:1
switch(conf-if-te-48/0/49:1)# shut
switch(conf-if-te-48/0/49:1)# interface TenGigabitEthernet 48/0/49:2
switch(conf-if-te-48/0/49:2)# shut
switch(conf-if-te-48/0/49:2)# interface TenGigabitEthernet 48/0/49:3
switch(conf-if-te-48/0/49:3)# shut
switch(conf-if-te-48/0/49:3)# interface TenGigabitEthernet 48/0/49:4
switch(conf-if-te-48/0/49:4)# shut
switch(conf-if-te-48/0/49:4)# exit
switch(config)# dpod 48/0/49 release
switch(config-dpod-48/0/49)#
```

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(ミラーパケット)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の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ような場合、SPAN 機能を用いてアナライザに接続したポートにパケットをコピーすることで特定ポートのトラフィックを監視することが可能となります。通常、このトラフィック(ミラーパケット)は受信パケットのみ、または送信パケットのみなど、片方向に限定されますが、Network OS は送信元ポートにおける双方向のトラフィックのモニタが可能です。

22.1.1 ロジカルシャーシモードにおける SPAN

ロジカルシャーシモードにおける SPAN は、クラスタ上に存在する異なるスイッチの任意のポートから送信元ポート及び宛先ポート(送信先ポート)を選択することで、異なるスイッチを跨ぐパケットミラーリング機能を提供します。ロジカルシャーシモードにおける SPAN の設定は、'source'コマンドを除き同様の手順で設定できます。

22.1.2 RSPAN

リモート SPAN(Remote SPAN, RSPAN)は SPAN を拡張し、複数のスイッチに跨るリモートミラーリングを提供します。各々の RSPAN セッションのトラフィックは、管理者が設定した RSPAN VLAN により送受信されます。この RSPAN VLAN は RPAN セッション専用であり、全てのスイッチ間で共通の値に設定する必要があります。送信元からの SPAN トラフックは RSPAN VLAN に移され、その後 RPAN VLAN を監視している任意の RSPAN 送信先へトランクポートを経由して送信されます。

NOTE

RSPAN は BS2500 向け内蔵 DCB スイッチのみのサポートとなります。BS2000, BS500 向け内蔵 DCB スイッチは RSPAN はサポートしていません。

RSPAN は RSPAN 送信元インタフェース(送信元ポート)と単一の RSPAN VLAN により構成されます。送信元として設定されたインタフェース(ポート)は RSPAN VLAN にミラーされ、そしてその RSPAN VLAN のメンバポートがミラーされたトラフィックを受信します。

そのため、RSPAN に参加する全てのスイッチはレイヤ 2 にてトランクとしてそれぞれ接続される必要があります。さらに、RSPAN セッションに参加する全てのスイッチは、RSPAN VLAN を設定する必要があります。

22.1.3　標準 SPAN のガイドライン及び制限

標準 SPAN 接続の制限は下記の通りです。

- ミラーパケットの転送先である宛先ポート(送信先ポート)に対する設定として、
  - スイッチ上の任意のポートを宛先ポート(送信先ポート)として設定することができます。
  - スイッチ当たり一つのポートのみ受信ミラー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のみ送信ミラー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するべきではありません。
- ある任意のポートを複数のポートに向けてミラーすることはできません。(宛先ポートは一つのみ設定可能です。)
- スイッチ上のある任意のポートがすでにミラーリングのタイプ(受信ミラーポート、送信ミラーポート、または双方向ミラーポートのいずれか)を問わず、ミラーリングの宛先ポートとして設定されている場合は、そのポート以外のポートは双方向ミラーリングの宛先ポートにすることはできません。
- スイッチ上のある任意のポートが、双方向のミラーリングの宛先ポートとして設定されている場合は、そのポート以外のポートはミラーリングのあらゆるタイプの宛先ポートとして設定することはできません。
- Network OS は、送信元ポート及び宛先ポートがサポートしているラインレート(1G、10G または 40G)で動作します。ですが、実際の性能は宛先ポートがサポートしているリンクスピードに依存します。(40G は BS2500 向け内蔵 DCB スイッチのみのサポートになります。) もし複数のポートが一つの宛先ポートへミラーするよう設定された場合などでは、宛先ポートに指定された物理ポートがサポートしているリンクスピード上限分のミラートラフィックのみがミラーされ、残りは破棄されます。
- 送信元ポートがトラフィックバーストを受信し、一方、宛先のミラーポートがすべてのバーストトラフィックを処理することはできない場合、バーストトラフィックの一部はミラーされません。
- ISL ポートをミラーリングすることも可能です。しかし、宛先ポートは送信元 ISL ポートに設定された RBridgeID と同じ RBridgeID が設定されている必要があります。(ISL ポートを監視する場合、宛先ポートを同一スイッチ上のポートに設定する必要があります。)
- LAG またはポートチャネルインタフェースのミラーリングは未サポートです。ですが、LAG のメンバポート各々をミラー化することは可能です。
- TRILL ポートを宛先ポート(送信先ポート)として指定することはできません。
- TRILL ポートを送信元ポートとして設定することができます。しかし、宛先ポート(送信先ポート)はローカルノード内(同一スイッチ上)のポートに制限されます。
- イーサネットポーズフレームはミラーリングされません。
- トランクポートとしてのミラーリングはサポートされていません。トランクをミラーリングするには、個別にすべてのメンバポートのミラーリングを有効にする必要があります。
- あるポートが SPAN の送信元ポートとして指定されている場合、そのポートから送信されるマルチキャストおよびブロードキャストの統計情報(送信パケット数)に関して、通常の送信パケットに加えミラーされたトラフィック数も含めて更新・追加されます。
- 宛先ポート(送信先ポート)では、'shutdown'および'no shutdown'を除くすべてのコマンドがブロックされます。

- ポートがミラー先の宛先ポートとして指定されると、その指定されたポートのインターフェースカウンタは自動でクリアされます。
- 'show interface' コマンドで表示される "Receive Statistics" と "Rate Info (Input)" の情報は宛先ポートでは表示されません。
- あるポートを宛先ポートとして設定する際には、事前にそのポートの MTU をデフォルト値の 2500 バイトに設定する必要があります。ポートが正常に宛先ポートとして設定されると、そのポートの MTU は、Network OS がサポートしている MTU の上限である、9208 バイトの最大値に自動的に設定されます。ポートの宛先ミラーポートとして設定が解除されると、MTU はデフォルト値(2500 バイト)に復元されます。
- ポートミラーリング機能は、ユーザー設定可能な任意の物理ポートでサポートされています。LAG、VLAG、VLAN の一部である任意のメンバポート、またはその他任意のユーザー構成の一部から任意のポートを選択し、送信元ポートとして設定することができます。
- ロジカルシャーシモード、またはファブリッククラスタモードでは、最大 512 のミラーセッションをサポートします。一方、スタンドアロンモードでサポートされるミラーのセッション数は最大２４となります。(BS2500 向け DCB スイッチではスタンドアロンモードは未サポートです。)

22.1.4　ロジカルシャーシモードにおける SPAN のガイドライン及び制限

上述した標準 SPAN 接続のガイドライン及び制限に加え、ロジカルシャーシモードでの SPAN は下記のガイドライン及び制限を考慮する必要があります。

- BS500 及び BS2000 向け DCB スイッチ上のポートは、ロジカルシャーシモードでは SPAN 送信元ポートとして設定することはできません。宛先ポート(送信先ポート)としては設定可能です。
- BS2500 向け DCB スイッチ上のポートでは、ロジカルシャーシモードにて送信元ポート、宛先ポートのどちらでも設定することができます。
- ロジカルシャーシモードでは、最大 512 のミラーセッションをサポートします。
- リモートノード(スイッチ)上のポートを宛先ポート(送信先ポート)として設定しているような SPAN 構成の場合、'show span path session <session-number>' コマンドでクラスタ内でミラーパレットが経由するパスを確認することができます。

22.1.5　Remote SPAN (RSPAN)のガイドライン及び制限

上述したガイドライン及び制限に加え、RSPAN は下記のガイドライン及び制限を考慮する必要があります。

(1) 基本的な考え方

- RSPAN に参加する全てのスイッチはレイヤ 2 トランクで接続される必要があります。
- RSPAN では ISL ミラーリングは未サポートです。
- TRILL(ISL)ポートは、送信元ポート及び、宛先ミラーポートとして設定することはできません。
- RSPAN はマルチホップをサポートしています。
- RSPAN はファブリッククラスタモード、ロジカルシャーシモードの両方でサポートされます。しか

し、ロジカルシャーシモードにおいて RSPAN を使用すると、トランクポートである ISL 上にミラーされたトラフィックが流れるため、ISL の帯域が消費されることになります。

- 送信元ポートがレイヤ 2 ではなく、かつタグなしトラフィックがミラー対象として設定されている場合、RSPAN ではミラーすることはできません。これは、ISL トランクリンク上ではタグなし、または未分類(unclassified)トラフィックはドロップされるためです。
- BS2500 向け DCB スイッチでは、送信元ポートが unknown モードである場合(すなわち、送信元ポートがレイヤ 2 でもレイヤ 3 でもない場合)、送信元ポートで送受信されるパケットは破棄され、なおかつミラーすることも出来ません。
- イーサネットポーズフレームはミラーすることは出来ません。

(2) VLAN に関する考え方

- RSPAN セッションを設定するにあたり、まず RSPAN VLAN を作成する必要があります。
- ネイティブ VLAN は RSPAN VLAN としては使用することはできません。
- RSPAN VLAN として使用する VLAN は、他の用途には使用することはできません。さらには、RSPAN VLAN として設定する前に、もしその VLAN に既にメンバが割り当てられているような場合、そのような VLAN を RSPAN VLAN として設定することはできません。一度 RSPAN VLAN として設定された VLAN に対しては、RSPAN セッションの設定を削除し、RSPAN VLAN の設定を削除することで他の用途にも使用することができます。
- RSPAN セッションに参加する全てのネットワークデバイス(スイッチ)が、各々の RSPAN セッションで一意な RSPAN VLAN を使用でき、RSPAN VLAN 用途にのみ設定できる場合に限り、そのような任意の VLAN を RSPAN VLAN として使用することが可能です。
- 送信元ポート、経由スイッチ及び送信先のスイッチの全てのスイッチ上で RSPAN VLAN を各々設定する必要があります。
- RSPAN トラフィックを転送するためのポート以外のポートには RSPAN VLAN を設定してはいけません。一方、RSPAN 宛先ポート(送信先ポート)では全ての設定が許されています。
- RSPAN としてミラーされるパケットの VLAN ID は RSPAN として設定された VLAN ID に書き換えられます。
- アクセスポートに対しては、送信先ポートとして RSPAN VLAN を追加することができます。
- MAC アドレス学習は RSPAN VLAN では無効化されます。

22.1.6 RSPAN ミラーリングにおける制限

Network OS v4.1 以降では、RBridgeID を超え、宛先ポートにミラーパケットを転送するために ISL を使用します。すべての SPAN スタンドアロンコマンドは、RBridge に対して以下の制限があります。

- BS2000 向け、及び BS500 向け DCB スイッチは RSPAN の送信元ポートとしては使用することができません。
- 複数のスイッチを跨ぐミラーリングは、ISL を経由してミラーパケットが転送されます。そのため、ISL パスが混雑しているような場合、ミラーパケットは破棄されトラフィックが失われてしまう可能性があります。

- FCoE ミラーリングは未サポートです。
- TRILL ポートは宛先ポート(送信先ポート)として使用することはできません。
- TRILL ポートは送信元ポートとして使用することは可能ですが、転送先(送信先ポート)はローカルノード(同一スイッチ)上に設定する必要があります。
- スイッチ間を超えて転送されるトラフィックに対して、もしソースポートが、ノード自身がレイヤ 2 でもレイヤ 3 でもない unknown モードの場合、タグなしパケットは破棄されます。
- イーサネットポーズフレームはミラーすることは出来ません。

22.2 入力(Ingress)SPAN の設定

以下の例では SPAN の送信元ポートが受信するパケットに対するミラー設定の例を示します。グローバルコンフィグレーションモードで実行して下さい。

1．モニタセッションをオープンし、セッション番号を割り当てます。
```
switch(config)# monitor session 1
```
2．受信パケットに対する'rx'パラメータを指定し、ソースポートと宛先ポートを設定します。
```
switch(config-session-1)# source tengigabitethernet 1/0/15 destination
tengigabitethernet 1/0/18 direction rx
```

NOTE

以下のエラーが表示される場合、宛先ポート(送信先ポート)で'lldp disable' コマンドを実行して下さい。
```
% Error: Destination port cannot have LLDP configuration on it.
```

3．オプション設定：'description'コマンドでモニタセッションにラベルを付加します。
```
switch(config-session-1)# description Hello World!
```
4．ステップ１から２を必要なポートに対して繰り返します。
モニタセッションは一つのソースポートしか定義できません。追加ポートのために、別のモニタセッションを作成しなければなりません。

22.3 出力(Egress)SPAN の設定

以下の例では SPAN の送信元ポートが送信するパケットに対するミラー設定の例を示します。グローバルコンフィグレーションモードで実行して下さい。

1．モニタセッションをオープンしセッション番号を割り当てます。
```
switch(config)# monitor session 1
```
2．送信パケットに対する'tx'パラメータを指定し、ソースポートと宛先ポートを設定します。
```
switch(config-session-1)#source tengigabitethernet 1/0/15 destination
tengigabitethernet 1/0/18 direction tx
```

NOTE

以下のエラーが表示される場合、宛先ポート(送信先ポート)で'lldp disable' コマンドを実行して下さい。
```
% Error: Destination port cannot have LLDP configuration on it.
```

3．オプション設定：'description'コマンドでモニタセッションにラベルを付加します。

```
switch(config-session-1)# description Hello World!
```

4．ステップ１から２を必要なポートに対して繰り返します。
モニタセッションは一つのソースポートしか定義できません。追加ポートのために、別のモニタセッションを作成しなければなりません。

22.4　双方向(bidirectional)SPAN の設定

以下の例では SPAN の送信元ポートが送受信するパケットに対するミラー設定の例を示します。グローバルコンフィグレーションモードで実行して下さい。

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．双方向のため'both'パラメータを指定し、ソースポートと宛先ポートを設定します。

```
switch(config-session-1)# source tengigabitethernet 1/0/15 destination
tengigabitethernet 1/0/18 direction both
```

3．オプション設定：'description'コマンドでモニタセッションにラベルを付加します。

```
switch(config-session-1)# description Hello World!
```

NOTE

以下のエラーが表示される場合、宛先ポート(送信先ポート)で'lldp disable' コマンドを実行して下さい。

```
% Error: Destination port cannot have LLDP configuration on it.
```

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

以下の例では SPAN セッションから一つの接続を削除する例を示します。

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# configure terminal
switch(config)# monitor session 1
```

3．特定のポート接続を削除するため'no'オプションを使います。

```
switch(config-session-1)# no source tengigabitethernet 1/0/15 destination
tengigabitethernet 1/0/18 direction both
```

4．接続が削除されたかを確かめるためモニターセッションを表示します。

```
switch(config)# end
switch# show monitor session 1
```

22.6　SPAN セッションの削除

以下の例では SPAN セッションを削除する例を示します。

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．'configure terminal'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
```

22.6.1　ロジカルシャーシモードにおける SPAN の設定

277 ページの『22.1.4 ロジカルシャーシモードにおける SPAN のガイドライン及び制限』も参照してください。

上述した SPAN 設定に用いる'source' コマンドは、インタフェース識別子によりロジカルシャーシクラスタ中の任意のポートを制御することができます。そのためロジカルシャーシモードにおける SPAN 設定では、クラスタ上の任意の送信元ポートと送信先ポートを一意のインタフェース識別子を用いることで上述した SPAN 設定と同様に設定することができます。送信元ポート及び送信先ポートは、ロジカルシャーシクラスタ上のスイッチであればどのポートでも指定することか可能です。例として、ロジカルシャーシクラスタ上の 3 つめのスイッチのポート 15 (3/0/15)を送信元ポート(監視ポート)と指定し、送信先ポートをクラスタ上の 5 つめのスイッチのポート 18(5/0/18)を指定することができます。

```
switch(config-session-1)# source tengigabitethernet 3/0/15 destination
tengigabitethernet 5/0/18 direction tx
```

NOTE
VCS ファブリックをまたがる SPAN は BS2500 向け内蔵 DCB スイッチのみのサポートとなります。

この設定ルールは入力(Ingress)、出力(Egress)及び、双方向(Both)SPAN に適用されます。275 ページの『22.1 スイッチドポートアナライザプロトコルの概要』を参照してください。

'show monitor' または'show span path' コマンドにより、送信元と送信先ポートを確認することができます。以下に実行例を示します。本コマンドは特権実行モードで実行して下さい。

```
switch# show span path session 1
Session :1
Path :Te 1/0/10 -> Te 3/0/15 (ISL-exit port) -> Te 5/0/18
switch# show monitor
Session :1
Description :Test monitor session
State :Enabled
Source interface :Te 3/0/15 (Up)
Destination interface :Te 5/0/18 (Up)
Direction :Rx
```

22.7　RSPAN の設定

NOTE

RSPAN は BS2500 向け内蔵 DCB スイッチのみのサポートとなります。BS2000, BS500 向け内蔵 DCB スイッチは RSPAN はサポートしていません。

277 ページの『22.1.5 Remote SPAN (RSPAN)のガイドライン及び制限』も参照してください。

SPAN の設定と RSPAN の設定の主たる違いとしては、RSPAN は RSPAN 専用の VLAN(リモート VLAN)を始めに設定する必要があります。これは'rspan-vlan'コマンドにより設定できます。以下に双方向 RSPAN の設定を行うコマンドの実行例を示します。

1．'config'コマンドに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．VLAN を作成します。(この例ではリモート VLAN の番号を「100」とします。)

```
switch(config)# interface vlan 100
```

3．'rspan-vlan'コマンドにより作成した VLAN をリモート VLAN に設定します。

```
switch(config-vlan-100)# rspan-vlan
```

4．'exit'コマンドによりグローバルコンフィグレーションモードに戻ります。

5．以下のコマンドで monitor セッションを開き、セッション番号を割り当てます。

```
switch(config-vlan-100)# monitor session 1
```

6．ソースポート(送信元ポート)及び宛先ポート(送信先ポート)を設定します。この例では送信元ポートの送受信パケットをミラーリングするため、"both" パラメータを使用します。監視パケットの方向指定を行いたい場合は、"both" の代わりに"tx" または"rx" のパラメータを指定して下さい。

RSPAN の設定では、宛先ポート識別子の代わりにリモート VLAN ID を指定します。

```
switch(config-session-1)# source tengigabitethernet 1/0/15 destination rspan-vlan
100 direction both
```

NOTE

以下のエラーが表示される場合、宛先ポート(送信先ポート)で'lldp disable' コマンドを実行して下さい。

```
% Error: Destination port cannot have LLDP configuration on it.
```

7．オプションで、以下のコマンドによりミラーセッションに名称(ラベル)を付与することが出来ます。

```
switch(config-session-1)# description Hello World!
```

8．ミラーパケットを転送可能とするために、'switchport' コマンドを用いて RSPAN VLAN をポートに設定します。

```
switch(config-session-1)# exit
switch (config)# interface ten 1/0/15
switch(conf-if-te-1/0/15)# switchport access rspan-vlan 100
```

9．以下のコマンドで設定を確認します。

```
switch(conf-if-te-1/0/15)# do show vlan rspan-vlan
```

RSPAN ではリモート VLAN のメンバポートにミラーパケットが転送されます。必要に応じ、パケットの宛先ポート(送信先ポート)のスイッチ及び、ミラーパケットを経由するスイッチ全てに手順２－３で示すコマンドを用いてリモート VLAN を生成します。さらに、ミラーパケットが経由するポート及び宛

先ポート(送信先ポート)に手順８で示すコマンドを用いてリモート VLAN を設定することでミラーパケットを受信することが出来るようになります。

23 スイッチのインバンド管理

23.1 インバンド管理の概要

BladeSymphony 内蔵 DCB スイッチは、マネジメントモジュールにバックプレーン経由で接続された専用の管理 LAN ポート経由でのスイッチモジュール管理(アウトバンド管理)がデフォルトで有効化されています。一方、内蔵 DCB スイッチ上のインバンド管理を用いることで、スイッチの物理イーサネットポートを介してスイッチモジュールを管理することができます。
インバンド管理では、管理用のトラフィックとデータトラフィックが同一の物理ポートを使用するため、管理トラフィックをサポートするため特別なインフラは必要ありません。インバンド管理インタフェースは、比較的簡単に設定でき、最もコスト効果の高い管理ソリューションです。また、インバンド管理を有効化することでネットワークの管理をサーバ(シャーシ)側の管理から分離することが可能になります。欠点は、管理トラフィックとは関係のないようなデータネットワーク内で発生する任意の問題によりスイッチモジュールへの接続が失われ、データトラフィックに対する障害に加え、スイッチ管理機能にも影響が及ぶ可能性があるということです。したがって、インバンド管理が利用できなくなった時のために、スイッチ管理用のシリアル接続環境、またはアウトバンド管理用にデータトラフィックとは分離された管理専用ネットワークを構築することをお勧めします。

NOTE
BS2500 向け内蔵 DCB スイッチのシリアル管理はオプション品のシリアルマネジメントケーブル(GV-LR4MNC1N1)が必要となります。

表 23-1 は、インバンド管理で使用できるアプリケーションのいくつかを示します。アプリケーションのリストは、全ケースを網羅しているものではありません。

表 23-1 インバンド管理用にサポートされるアプリケーション

アプリケーション	説明
FWDL	外部サーバから FTP または SCP を使用してリモートデバイスにファームウェアをダウンロードします。
SCP	Secure Copy Protocol(SCP)を使ってファイルを転送します。
SSH	Secure Shell アプリケーションを介してデバイスに接続します。
SNMP	Secure Network Management Protocol(SNMP)を使用してデバイスを管理します。
telnet	telnet を使用してデバイスに接続します。

23.1.1 前提条件

スイッチのインバンド管理を可能とするには、管理ステーションが IP アドレスを取得でき、なおかつ

管理ネットワークへアクセスすることができる必要があります。静的に IP アドレスをを手動で設定して管理ステーションに IP アドレスを設定することができます。デフォルトゲートウェイの設定を行うことで、ゲートウェイを介して管理ステーションから管理ネットワークへアクセスすることも可能です。詳細は 56 ページの『3.3 スイッチへ接続する』を参照してください。

Network OS V3.0.0 以降が稼動しているスイッチでは、レイヤ 2 またはレイヤ 3 ネットワークを介してデバイスを管理するため、VCS モードでインバンド管理がサポートされています。スタンドアロンモードでは、管理ステーションはスタンドアロンモードの個々のノードに直接接続しなければなりません。Network OS v3.0.0 以前のファームウェアが稼働しているスイッチでは、スタンドアロンモードでのみインバンド管理がサポートされています。
インバンド管理は、特別なコンフィグレーションコマンドを必要としません。なぜなら、管理用トラフィックは、既存の IP ルーティングインフラストラクチャに乗り、インバンド管理インターフェースを設定するために必要なコマンドは、ターゲットデバイスへの接続を提供するために、静的または動的なルーティングプロトコルでサポートされる IP インターフェースを設定するコマンドと同じだからです。

NOTE
BS2500 向け内蔵 DCB スイッチはスタンドアロンモードは未サポートです。

23.1.2　サポートインタフェース

インバンド管理は、表 23-2 に示すインターフェースでサポートされます。これらの各インターフェースに使用できるコンフィグレーションオプションの詳細については、『Network OS Command Reference』の'interface'コマンドのマニュアルを参照してください。

表 23-2　インバンド管理が設定可能なポート

インタフェース	アドレス指定	説明
TenGigabitEthernet (Te)	rbridge-id/slot/port	10Gbイーサネット物理インタフェース
FortyGigabitEthernet (Fo)	rbridge-id/slot/port	40Gbイーサネット物理インタフェース
Port-channel (Po)	interface-id	ポートチャネルインタフェース スタンドアロンモードのみサポート
Vlan	vlan-id	VLAN インタフェース v 2.0 でのみサポート
Virtual Ethernet (Ve)	interface-id(VLAN ID 対応)	仮想イーサネットインタフェース

NOTE
Virtual Ethernet (Ve)インタフェースは、レイヤ 3 スイッチに設定された Virtual LAN (VLAN)に関連付けられた論理ポートです。外部ルータを使用せずに、一つのレイヤ 3 VLAN から別の VLAN にトラフィッ

クを中継するレイヤ 3 スイッチ機能を有効にするため仮想インタフェース上にルーティングパラメータを設定することが出来ます。Ve インターフェースを設定する前に、対応する VLAN を設定する必要があります。

23.1.3　インバンド管理方式のサポート状況

Network OS は、バージョンアップによりインバンド管理方式がエンハンスされており、更に動作モードにより利用できるアプリケーションでの利用状況が異なります。表 23-3 にインバンド管理方式でのサポート状況を示します。また、表 23-4 にアウトバンド管理でのサポート状況を示します。

表 23-3　インバンド管理でのサポート状況

NOS バージョン			2.0.1			3.0.0			4.0.1			4.1.x		
設定インタフェース			Vlan,Te,Po			Ve,Te,Po			Ve,Te,Po			Ve,Te,Fo		
NOS 動作モード			SA	FC	LC	SA	FC	LC	SA	FC	LC	SA	FC	LC
アプリケーション	FWDL		○	×		○	○			○	×	○	○	注１
	SCP		○	×		○	○			○	×	○	○	○
	SSH		○	×		○	○			○	×	○	○	○
	telnet		○	×		○	○			○	×	○	○	○
	SNMP	Get	×	×		○	○			○	×	○	○	○
		Set	×	×		○	○			○	×	○	○	○
		Trap	×	×		注２	注２			注２	×	注２	注２	注２

注１：Principal スイッチからファブリック内の全ノードのアップデートが可能。本動作モードでは、メジャーバージョン間のバージョンダウン(4.1.x から 3.0.0/2.0.1 へ)はできません。

注２：送信元 IP アドレスは、アウトバンド管理用に設定した IP アドレスとなります。

表 23-4　アウトバンド管理でのサポート状況

NOS バージョン			2.0.1			3.0.0			4.0.1			4.1.x		
NOS 動作モード			SA	FC	LC	SA	FC	LC	SA	FC	LC	SA	FC	LC
アプリケーション	FWDL		○	○		○	○			○	×	○	○	注１
	SCP		○	○		○	○			○	×	○	○	○
	SSH		○	○		○	○			○	×	○	○	○
	telnet		○	○		○	○			○	×	○	○	○
	SNMP	Get	○	○		○	○			○	×	○	○	○
		Set	○	○		○	○			○	×	○	○	○
		Trap	○	○		○	○			○	×	○	○	○

注１：Principal スイッチからファブリック内の全ノードのアップデートが可能。本動作モードでは、メジャーバージョン間のバージョンダウン(4.1.x から 3.0.0/2.0.1 へ)はできません。

23.1.4　インバンド管理における接続トポロジ

インバンド管理において、使用するインタフェースにより接続構成が異なります。表 23-5 に、各インタフェースに対する、接続方式を示します。

表 23-5　インバンド管理のためのトポロジ

インタフェース	接続方式	補　足
TenGigabitEthernet (Te)	各スイッチの設定済みインタフェースに接続	動作モードに関係なく、全スイッチに接続(個々のスイッチ単独の管理用途)
FortyGigabitEthernet (Fo)		
Port-channel (Po)		
Vlan	Vlan/Ve に所属するいずれかのインタフェースに接続	スタンドアロンモード：全スイッチに接続 VCS モード：いずれかのスイッチに接続。
Virtual Ethernet (Ve)		

(1) スタンドアロンモードでのインバンド管理接続トポロジ

図 23-1 は、スタンドアロンモードでインバンド管理インターフェースの構成を示します。この例では、Switch-A と Switch-B のための管理ステーション IP アドレスとイーサネットポートインタフェース IP アドレスのすべてが、同じサブネット内にあり、管理ステーションと Switch-A を介して Switch-B に接続するためのルーティングプロトコルは必要ではありません。サーバまたはワークステーションの管理ステーションは、物理的に決戦された switch-A に接続し、switch-A から物理的にカスケード接続された switch-B に接続することができます。

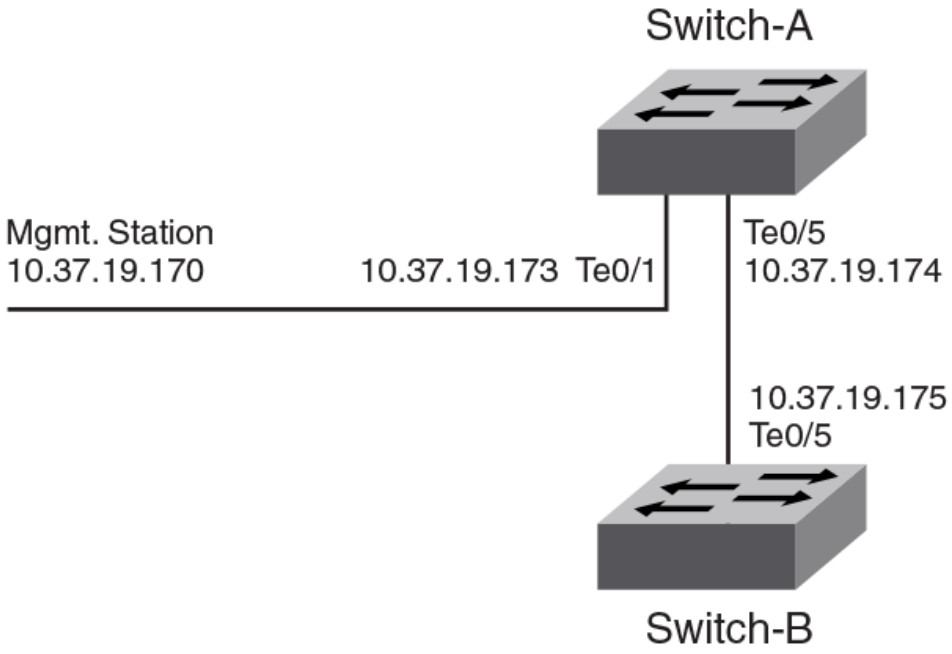

図 23-1　スタンドアロンモードにおけるインバンド管理接続トポロジ

図 23-1 に示す構成では、次の操作をサポートします。

- 管理ステーションから Switch-A に SSH または telnet セッションを介して接続する。
- 管理ステーションと Switch-A 間で Secure Copy Protocol(SCP)または FTP を使用してファイルを転送する。
- Switch-A と Switch-B 間で Secure Copy Protocol(SCP)を使用してファイルを転送する。
- Switch-A と Switch-B の間で、表 23-1 のアプリケーションのいずれかを使用する。

NOTE

BS2500 向け内蔵 DCB スイッチはスタンドアロンモードは未サポートです。

---

(2) VCS モードでのインバンド管理接続トポロジ

図 23-2 は、Switch-A と Switch-B からなる VCS fabric を形成する場合におけるインバンド管理インターフェースの構成を示します。

この例ではインバンド管理のために Ve 100 を用意します。その Ve を RBridgeID に関連付け、Ve インタフェース上で、IP アドレスを設定します。この Ve 100 をインバンド管理として使用したい物理ポート(TenGigabitEthernet、FortyGigabitEthernet または Port-channel)に関連付けることで、該当インタフェースをインバンド管理ポートとして使用することが可能になります。

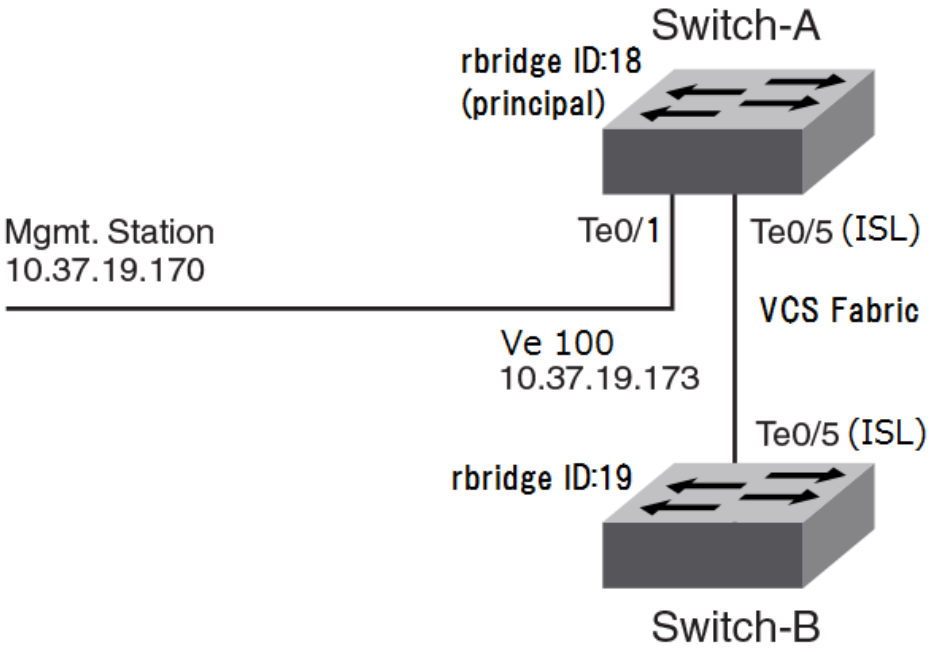

図 23-2　VCS モードにおけるインバンド管理接続トポロジ

図 23-2 に示す構成において、ファブリッククラスタモードでは、次の操作をサポートします。

- 管理ステーションから Switch-A に SSH または telnet セッションを介して接続する。
- 管理ステーションと Switch-A 間で、表 23-1 のアプリケーションのいずれかを使用する。
- 管理ステーションから Switch-B に SSH または telnet セッションを介して接続する。
- 管理ステーションと Switch-B 間で、表 23-1 のアプリケーションのいずれかを使用する。

ロジカルシャーシモード(LC モード)では、管理ステーションと VCS ファブリックの代表スイッチ(Principal スイッチ)間のセッションで、ファブリック内の全てのスイッチを制御することが出来ます。ファブリッククラスタモードと同様、Principal スイッチではないスイッチに対しても IP アドレスを RBridgeID に関連付けられた Ve インタフェースに設定し、SSH または telnet セッションを介して接続することは出来ますが、スイッチの構成情報の参照のみが可能となります。

図 23-2 に示す構成において、ロジカルシャーシモードでは、次の操作をサポートします。

- 管理ステーションから Switch-A に SSH または telnet セッションを介して接続する。
- 管理ステーションと Switch-A 間で、表 23-1 のアプリケーションのいずれかを Switch-A 及び Switch-B に対して使用する。
- 管理ステーションから Switch-B に接続し、その CLI 上からファブリックの構成情報を参照する。

23.2　インバンド管理インタフェースの設定

23.2.1　スタンドアロンモードでのインバンド管理インタフェースの設定

次の手順は、図 23-1 に示すように、インバンド管理インターフェースを設定します。

1．利用可能な場合、シリアルコンソールを介して、または管理インタフェースを介してスイッチに接続します。

2．グローバルコンフィグレーションモードを入力するために、'configure terminal'コマンドを入力します。
3．'interface'コマンドに続いて設定したいインタフェースのタイプを入力します。
スタンドアロンインバンド管理インターフェースの場合、物理的なユーザーポート(1GbE、10GbE)だけは、IP アドレスで設定する必要があります。VLAN または VE のインタフェースのいずれかを設定する必要はありません。
4．インタフェースに IPv4 アドレスを設定するには、'ip address <IPv4_address/prefix_length>'コマンドを入力します。

NOTE
プライマリ IP アドレスのみ、設定する必要があります。セカンダリ IP アドレスはサポートされていません。

5．バイト単位でインタフェースの IP Maximum Transmission Unit (MTU)を設定するために、'ip mtu'コマンドを入力します。
6．Address Resolution Protocol(ARP)のためのインタフェースタイムアウトパラメータ値を分単位で設定するために、'arp-ageing-timeout'コマンドを入力します。デフォルトのタイムアウト値は 4 時間です。
7．未使用の ARP エントリを削除するには、'no-refresh'オプションで'do clear-arp-cache'コマンドを入力して、ARP キャッシュをクリアします。
8．'ip proxy-arp'コマンドを使用してインターフェース毎にプロキシ ARP を設定します。
9．'show ip interface'コマンドを使用してコンフィグレーションを表示します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# interface TenGigabitEthernet 1/0/1
switch(conf-if-te-1/0/1)# no shutdown
switch(conf-if-te-1/0/1)# ip address 1.1.1.1/24
switch(conf-if-te-1/0/1)# ip mtu 1200
switch(conf-if-te-1/0/1)# ip arp-ageing-timeout 200
switch(conf-if-te-1/0/1)# do clear arp cache no-refresh
switch(conf-if-te-1/0/1)# ip proxy-arp
switch(conf-if-te-1/0/1)# exit
switch(config)# exit

switch# show ip interface TenGigabitEthernet 1/0/1
TenGigabitEthernet 1/0/1 is up protocol is up
Primary Internet Address is 1.1.1.1/24 broadcast is 1.1.1.255
IP MTU is 1200
Arp ageing timeout value is 03:20:00
Proxy Arp is Enabled
Vrf:default-vrf
```

VCS モードにおけるインバンド管理インターフェースの設定

スタンドアロンモードにおけるインバンド管理と同様に、VCS モードにおいてもスイッチをインバンドで管理することが可能です。本節では、Ve インタフェースを使った VCS モードにおけるインバンド管理の設定方法について例示します。

(1) ファブリッククラスタモードにおけるインバンド管理インターフェースの設定
以下の例では、RBridgeID: 18 に設定されたスイッチモジュールの外部ポート#1 (18/0/1)に対してインバンド管理の為の IP アドレスを設定する手順を示します。この外部ポート(18/0/1)は管理ステーションからアクセス可能なネットワークに接続されている必要があります。

1．マネジメントモジュール経由の管理専用インタフェース(アウトバンド管理)経由でスイッチモジュールに接続します。
2．グローバルコンフィグレーションモードを入力するために、'configure terminal'コマンドを入力します。
```
switch# configure terminal
Entering configuration mode terminal
```
3．インバンド管理のための VLAN インタフェース(本例では 100)を生成します。 生成後、'exit' と入力し、グローバルコンフィグレーションモードに戻ります。
```
switch(config)# interface Vlan 100
switch(config-Vlan-100)# exit
```
4．以下のコマンドを実行し、インバンド管理ポートに対して switchport 設定及び、生成した VLAN を関連付けます。最後に'exit' と入力し、グローバルコンフィグレーションモードに戻ります。
```
switch(config)# interface TenGigabitEthernet 18/0/1
switch(conf-if-te-18/0/1)# switchport
switch(conf-if-te-18/0/1)# switchport mode access
switch(conf-if-te-18/0/1)# switchport access vlan 100
switch(conf-if-te-18/0/1)# no shutdown
switch(conf-if-te-18/0/1)# exit
```
5．'rbridge-id <スイッチの RBridge#>' と入力し、RBridge ID コンフィグレーションモードに移行します。本例では、'rbridge-id 18' と入力します。
```
switch(config)# rbridge-id 18
```
6． RBridge ID コンフィグレーションモードにて、VLAN インタフェースコンフィグレーションモードに移行します。
```
switch(config-rbridge-id-18)# interface Ve 100
```
7． 以下のコマンドで VLAN インタフェースにインバンド用の IP アドレスを設定し、VLAN インタフェースを有効化します。最後に'exit' を３回入力し、特権実行モードに戻ります。
```
switch(config-Ve-100)# ip address 10.37.19.173/24
switch(config-Ve-100)# no shutdown
switch(config-Ve-100)# exit
switch(config-rbridge-id-18)# exit
switch(config)# exit
```
8．特権実行モードで以下のコマンドを実行しインバンド管理用の IP アドレスが設定されていることを確認します。
```
switch# show running-config rbridge-id 18 interface Ve
rbridge-id 18
 interface Ve 100
  ip proxy-arp
  ip address 10.37.19.173/24
  no shutdown
 !
!
```

ファブリッククラスタモードにて、クラスタ内の各々のスイッチを同様にインバンド管理設定にしたい場合は上記の Step１から Step８の手順を各々のスイッチに対して実行します。その際、RBridge ID、設定する外部ポート番号及び IP アドレスはそれぞれ適切な値に変更の上、上記コマンドを実行して下

さい。

NOTE
VCS モードでは、'show vcs'コマンドで管理用の IP アドレスを確認することができます。ただし、このコマンドで表示される IP アドレスは、アウトバンド用管理ポート(マネジメントモジュールと接続される専用管理ポート)に設定された IP アドレスが表示されます。

(2) ロジカルシャーシモードにおけるインバンド管理インターフェースの設定
以下に、ロジカルシャーシモードにおける RBridgeID: 18 に設定されたスイッチモジュールの外部ポート#1 (18/0/1)に対してインバンド管理の為の IP アドレスを設定する手順を示します。この外部ポート(18/0/1)は管理ステーションからアクセス可能なネットワークに接続されている必要があります。

NOTE
BS2500 向け内蔵 DCB スイッチはロジカルシャーシモードは未サポートです。

1．マネジメントモジュール経由の管理専用インタフェース(アウトバンド管理)経由でスイッチモジュールに接続します。このとき、接続するスイッチは Principal スイッチである必要があります。Principal スイッチは、'show vcs'コマンドで確認します。"Hostname"に">"表示があるスイッチに接続してください。

```
switch # show vcs
Config Mode    : Distributed
VCS Mode       : Logical Chassis
VCS ID         : 1
VCS GUID       : 07d60895-d23a-4cf9-b5cd-9590c828642c
Total Number of Nodes           : 2
Rbridge-Id       WWN                              Management IP   VCS Status
Fabric Status        HostName
-------------------------------------------------------------------------------
-------------------------------
18              >10:00:00:05:33:FF:8E:EF*       192.168.0.78    Online
Online               SW2
19               10:00:00:05:33:FF:CA:BC        192.168.0.79    Online
Online               SW3
```

2．グローバルコンフィグレーションモードを入力するために、'configure terminal'コマンドを入力します。

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

3．インバンド管理のための VLAN インタフェース(本例では 100)を生成します。 生成後、'exit' と入力し、グローバルコンフィグレーションモードに戻ります。

```
switch(config)# interface Vlan 100
switch(config-Vlan-100)# exit
```

4．以下のコマンドを実行し、インバンド管理ポートに対して switchport 設定及び、生成した VLAN を関連付けます。最後に'exit' と入力し、グローバルコンフィグレーションモードに戻ります。

```
switch(config)# interface TenGigabitEthernet 18/0/1
switch(conf-if-te-18/0/1)# switchport
switch(conf-if-te-18/0/1)# switchport mode access
```

```
switch(conf-if-te-18/0/1)# switchport access vlan 100
switch(conf-if-te-18/0/1)# no shutdown
switch(conf-if-te-18/0/1)# exit
```

5．'rbridge-id <スイッチの RBridge#>' と入力し、RBridge ID コンフィグレーションモードに移行します。本例では、'rbridge-id 18' と入力します。

```
switch(config)# rbridge-id 18
```

6． RBridge ID コンフィグレーションモードにて、VLAN インタフェースコンフィグレーションモードに移行します。

```
switch(config-rbridge-id-18)# interface Ve 100
```

7． 以下のコマンドで VLAN インタフェースにインバンド用の IP アドレスを設定し、VLAN インタフェースを有効化します。最後に'exit' を３回入力し、特権実行モードに戻ります。

```
switch(config-Ve-100)# ip address 10.37.19.173/24
switch(config-Ve-100)# no shutdown
switch(config-Ve-100)# exit
switch(config-rbridge-id-18)# exit
switch(config)# exit
```

8．特権実行モードで以下のコマンドを実行しインバンド管理用の IP アドレスが設定されていることを確認します。

```
switch# show running-config rbridge-id 18 interface Ve
rbridge-id 18
 interface Ve 100
  ip proxy-arp
  ip address 10.37.19.173/24
  no shutdown
 !
!
```

9．LC モードでは、ファブリック内の他のスイッチに対しても同一セッションで IP アドレスなどで設定することが出来ます。以下に RBridgeID: 19 の外部ポート Te19/0/1 に IP アドレス 10.37.19.174 を追加で設定する手順を示します。手順３にて Principal スイッチ上で VLAN100 を生成済みのため、改めて VLAN を生成する必要がない点に注意して下さい。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# rbridge-id 19
switch(config-rbridge-id-19)# interface Ve 100
switch(config-Ve-100)# ip address 10.37.19.174/24
switch(config-Ve-100)# no shutdown
switch(config-Ve-100)# exit
switch(config-rbridge-id-19)# exit
switch(config)# exit
```

NOTE

VCS モードでは、'show vcs'コマンドで管理用の IP アドレスを確認することができます。ただし、このコマンドで表示される IP アドレスは、アウトバンド用管理ポート(マネジメントモジュールと接続される専用管理ポート)に設定された IP アドレスが表示されます。

---

24 IGMP の設定

24.1 IGMP の概要

Internet Group Management Protocol (IGMP)は、ホストとルータのグループ化を可能とするプロトコルで、ＩＰマルチキャストの一部です。この章では、IGMP の全ての機能を説明するのではなく、snooping メカニズムにフォーカスしています。

24.2 IGMP snooping 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転送は、VLAN に所属するポートで受信したマルチキャストパケットをレイヤ 2 転送することにより、容易に実現できます。しかし、この単純な方法は効率的に帯域を使えません。メンバポートの一部だけをマルチキャストパケットを受信したいデバイスに接続しなければならないからです。最悪ケースとしては、一つの VLAN メンバだけが受信したい場合でも、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)にデータ転送されてしまいます。このシナリオでは、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が損失することになります。
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 は、IGMPv1/v2 スヌーピングのみサポートしており、レイヤ 3 IGMP 機能はサポートしていません。

24.2.1 Multicast ルーティングと IGMP snooping

マルチキャストルーターは、接続された各物理ネットワーク上のメンバのグループを学習するために IGMP を使います。マルチキャストルーターは、接続されたそれぞれのネットワークのマルチキャストグループメンバのリストと各メンバーのタイマーを保持します。

NOTE
“マルチキャストグループメンバー”は、利用可能な接続されたネットワーク上のマルチキャストグループのメンバーが少なくともーつあることを意味します。

ホストがマルチキャストルーティンググループに参加するには２つの方法があります。

- 要求されていない IGMP join リクエストを送信する
- マルチキャストルーターからの一般的な問合せに対する応答として IGMP join リクエストを送信する

リクエストの応答では、スイッチはその VLAN に対してレイヤ 2 フォワーディングテーブルにエントリを作成します。その他のホストが同じマルチキャストに対して join リクエストを送信すると、スイッチは存在するテーブルエントリにそれらを追加します。一つのエントリだけが、各マルチキャストグループに対してレイヤ 2 フォワーディングテーブル上に VLAN 毎に生成されます。
IGMP snooping は、マルチキャストグループ当たり一つのホスト 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。

24.2.2　vLAG および LAG プライマリポート

vLAG および LAG の現在の DCE の実装では、いわゆるプライマリポートの概念を持っています。vLAG および LAG のメンバポートの一つがプライマリポートとなり、LAG または VLAG から出力するすべてのマルチキャストトラフィックは、プライマリポートで送信されます。したがって、通常のハッシュベースのフォワーディングは、マルチキャストトラフィックでは実行されず、トラフィックやデータを制御します。図 24-1 に示すように、rbridge R1 が Po10 のグループ G1 で IGMP join リクエストを受信した場合を考えます。これにより、Po10 がグループ G1 のために IGMP レシーバのリストに加えられることになります。次に、vLAG のプライマリポートが R4 と S1 を接続するリンクとなった場合を考えます。このように、元々の Join リクエストは R1 で受信されましたが、何れのマルチキャストトラフィックは、R1 からでなく R4 から vLAG Po10 からグループ G1 の出力となるよう、クラスタでは受信されます。

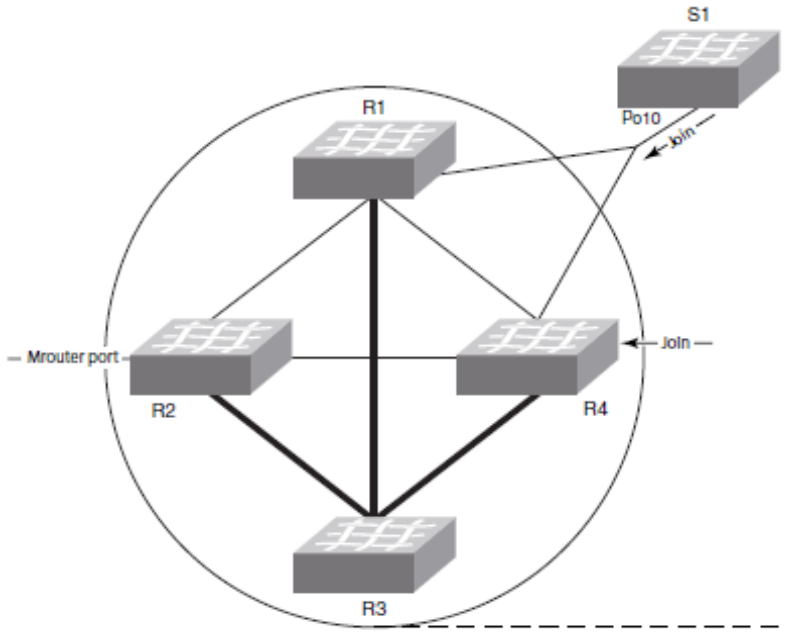

図 24-1　VCS ファブリックモードの IGMP スヌーピング

vLAG プライマリポートが変わった場合、例えば図 24-1 の R4 と S1 の間のリンクがダウンした場合、マルチキャストトラフィックは vLAG 上の新しいプライマリポートから出します。上記のケースでは、

新しいプライマリポートは、R1 と S1 を接続するリンクとなります。

24.2.3　IGMP スケーラビリティ

このセクションでは、スイッチ操作のさまざまなモードで Network OS のための IGMP Snooping 機能のスケーラビリティの限界と、スケーラビリティの限界を説明する際に関与するさまざまな動作条件を説明しています。

IGMP の動作条件値は次のとおりです。

IGMP 測定器順	詳　細
サポートされる IGMP グループの最大数	この動作条件値は、利用できるハードウェア資源(例えば、MGID、構成リプレイおよび eNS 配布帯域幅)に基づいて計算されます。
IGMP Snooping 構成でサポートされる VLAN の最大数	この動作条件は、スイッチ上で実行されている IGMP のソフトウェアプロセス、eNS 分布幅の一般的なクエリーパケットの生成容量の数によって制限されます。
スイッチ当たりの最大 IGMP パケット処理速度	この動作条件によって記述されるスケーラビリティ番号は、スイッチで実行している IGMP ソフトウェアプロセスで処理できるパケット数の上限を示唆しています。パケットが複数のポート/ VLAN からの着信であれば、同じ処理帯域が共有されます。
VCS ファブリッククラスタ当たり最大 IGMP パケット処理速度	この動作条件は、論理的 VCS ファブリックスイッチに着信する最大 IGMP パケットレートの上限を指定します。それは、VCS ファブリッククラスタ内のノード数の eNS 配布帯域幅によって制限されます。

(1) スタンドアロンモード

表 24-1 から表 24-4 に、動作条件レベルを記述します。

表 24-1　スタンドアロンモードの動作条件

動作条件	上限	コメント
サポートされる IGMP グループの最大数	2000	Join リクエストは、同じスイッチの 4 つのポートで送信されます。
IGMP 構成でサポートされる VLAN の最大数	128	
スイッチ毎の最大 IGMP パケット処理速度	512 パケット／秒	

(2) VCS ファブリッククラスタモード

データセンターでフラットレイヤ 2 ネットワークをサポートする場合は、スイッチがクラスタを形成するために、任意の順序で接続することができます。クラスタに含まれるノードの数は、4 ノードから 24 ノードの範囲です。次の表に、動作条件レベルを記述します。

表 24-2　4 ノードクラスタの動作条件

動作条件	上限	コメント
サポートされる IGMP グループの最大数	2000	Join リクエストは、同じスイッチの 4 つのポートで送信されます。
IGMP 構成でサポートされる VLAN の最大数	128	
スイッチ毎の最大 IGMP パケット処理速度	512 パケット／秒	
VCS ファブリッククラスタ当たり最大 IGMP パケット処理速度	512 パケット／秒	

表 24-3　20 ノードクラスタの動作条件

動作条件	上限	コメント
サポートされる IGMP グループの最大数	2000	Join リクエストは、同じスイッチの 4 つのポートで送信されます。
IGMP 構成でサポートされる VLAN の最大数	128	
スイッチ毎の最大 IGMP パケット処理速度	512 パケット／秒	
VCS ファブリッククラスタ当たり最大 IGMP パケット処理速度	512 パケット／秒	

表 24-4　IP マルチキャスト動作条件

動作条件	上限	コメント
レイヤ 3 フォワーディングエントリ数	256	
IGMP snooping フォワーディングエントリ数	8000	
マルチキャストフロー数	10000	
PIM インタフェース数	32	

24.3　IGMP snooping の設定

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。

24.3.1　IGMP snooping の有効化

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．オプション：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。

NOTE

IGMP snooping の設定は、同一のＶＣＳファブリッククラスタの全てのスイッチで同じでなければなりません。例えば、スイッチ上の VLAN2 に'ip igmp snooping enable'を設定するなら、クラスタ内の全てのスイッチの VLAN2 に同じコマンドを設定しなければなりません。

24.3.2　IGMP snooping クエリヤーの設定

マルチキャストトラフィックが、Protocol-Independent Multicast (PIM)や IGMP が定義されていないため、中継されないなら VLAN に IGMP snooping クエリヤーを使います。

IGMP snooping クエリヤーは、IP マルチキャストトラフィックを受信しようとするスイッチからの IGMP レスポンスの契機となる IGMP クエリーを送信します。IGMP snooping は、適切な転送アドレスをマップするため、これらのレスポンスをリッスンします。

NOTE

IGMP snooping クエリヤーは、マルチキャストルーター(mrouter)インタフェースと同じインタフェース上に設定することは出来ません。

このセクションのコマンドに関する完全な情報は『Network OS Command Reference』を参照下さい。

IGMP snooping クエリヤーを設定するため、次の手順を使います。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．VLAN インタフェース番号を選択するために、'interface'コマンドを入力します。

```
switch(config)# interface vlan 25
```

3．VLAN の IGMP クエリヤー機能を活性化します。値の範囲は、1 から 18000 秒の範囲で指定できます。デフォルトは、125 秒です。

```
switch(config-vlan-25)# ip igmp query-interval 125
```

4．最後のメンバクエリー間隔を設定します。値の範囲は、1000 から 25500 ミリ秒です。デフォルトは 1000 ミリ秒です。

```
switch(config-vlan-25)# ip igmp last-member-query-interval 1000
```

5．Max Response Time(MRT)を設定します。1 から 25 秒までが指定可能です。デフォルトは 10 秒です。

```
switch(config-vlan-25)# ip igmp query-max-response-time 10
```

6．VLAN に対する IGMP クエリヤー機能を活性化します。

```
switch(config-vlan-25)# ip igmp snooping querier enable
```

24.3.3　IGMP の監視

IGMP トラフィックの性能監視により、スイッチ上の潜在的な問題も診断することが可能となります。これは、マルチキャストをリクエストしているホストにだけ IP マルチキャストトラフィックを転送するよう設定することで、より効果的に帯域を利用することを助けます。

このセクションのコマンドに関する完全な情報は『Network OS Command Reference』を参照下さい。

IGMP snooping を監視するため、次の手順を使います。

1．グローバルコンフィグレーションモードに移行するため、'configure terminal'コマンドを入力します。

2．IGMP マルチキャストグループの全ての情報を表示するため、'show ip igmp groups'コマンドを入力します。全てのインタフェースや特定のインタフェースの全てのグループまた特定インタフェースの特定グループの設定されたエントリを含む全てのグループの IGMP データベースを表示するため、このコマンドを使います。

```
switch# show ip igmp groups
```

3．VLAN やインタフェースの IGMP 統計情報を表示するため、'show ip igmp statistics'コマンドを使用します。

```
switch# show ip igmp 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、297 ページの『24.3 IGMP snooping の設定』または 298 ページの『24.3.2 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。

---

25 トラブルシュート

25.1　トラブルシュート概要

この章は、内蔵 DCB スイッチを使用中に発生するかもしれない問題を解決する秘訣や手順を提供しています。また、共通のトラブルシュートツールを幾つか紹介しています。

25.2　問題解決情報の収集

次の情報は、保守員・ベンダーに問合せする際、問題の調査・解決に役に立つ情報です

- ネットワーク構成図と接続情報
- 問題に至った手順や事象の記録
- 事象発生時に動作していたアプリケーション、管理用エージェントやスクリプトのリスト
- 内蔵 DCB スイッチのログファイル(supportsave)
- もし SFP トランシーバに関連した問題であれば'show media'コマンドの出力結果
- お客様自身でトラブルシュートのために実行したコマンドの出力結果
- Wireshark やその他アナライザを使ってキャプチャしたネットワークトレース情報
- もし TACACS に関連した問題であれば、TACACS サーバのバージョン情報

25.2.1　supportsave データの採取

'copy support'コマンドは、診断コマンドを実行するだけでなく、core dump、トレースやその他関連データを採取します。加えて、これら全ての情報をリモートサーバへコピーします。リモートサーバにコピーされたデータにより、ベンダでの障害解析を進めることが出来ます。
supportsave を採取するために、次の手順を実行してください。

1．スイッチにログインする。
2．特権実行モードで、supportsave を採取するために'copy support'コマンドを入力します。
'copy support'コマンドは、FTP または SCP を使って supportsave をリモートサーバにコピーするオプションを持っています。単一のコマンドラインまたは、対話モードでコマンドを実行することが出来ます。
次の例は、FTP を使ってリモートサーバへコピーするために単一のコマンドラインモードで supportsave を実行しています。

```
switch# copy support ftp host 10.38.33.131 user admin directory 108
Password: *****
```

次の例は、FTP を使った対話モードの例です。

```
switch# copy support-interactive
Server Name or IP Address: 10.38.33.131
Protocol (ftp, scp): ftp
User: admin
Password: *****
Directory:/home/admin/support
VCS support [y/n]? (y): y
```

25.2.2　トラブルシュートのアプローチ

このセクションでは、トラブルシュート方法の概要を述べます。

1．スイッチが全ての必要なライセンスをインストール済みかチェックします。
- ライセンスには、VCS Fabric license や FCoE license があります。
- ライセンスタイプは、VCS Fabric(Network OS v3.0.0 以前で３つ以上のノード用のライセンス)や FCoE です。
- VCS Fabric ライセンスは、２つ以下の VCS ファブリッククラスタでは必要ありません。
- FCoE ライセンスは、インストールされた VCS ファブリックモードが有効でなければなりません。
- FCoE が追加・変更された後は、ライセンスを有効にするためスイッチをリブートします。

2．転送が行われるようトポロジやスイッチの設定を確認します。
3．'copy support'コマンドを入力します。
4．障害の手がかりや切っ掛けを探すため、例えば'show logging raslog'などの参照コマンドを実行します。
5．様々なリソースの利用率をチェックします。
ａ．CPU の使用状況を知るために、'show process cpu'コマンドを入力します。
ｂ．メモリの利用状況を知るために、'show process me'コマンドを入力します。
ｃ．使用されている MAC アドレスの数を知るために、'show mac-address-table count'コマンドを入力します。
ｄ．ルートの数を知るために、'show fabric route topology'コマンドを入力します。
ｅ．VCS ファブリックノードの数を知るために、'show fabric all'コマンドを入力します。
ｆ．光モジュールの問題を調査するために、'show media'コマンドを入力します。
6．データパスファブリックの継続試験を実施します。
ａ．エンドステーションまたはデバイスから、エンドステーションまたはデバイスへの ping 実行。
ｂ．もしパケットがエラー受信または破棄されるなら、'show interface'コマンド出力のカウンターをチェックする。
ｃ．使用されている光モジュールが Brocade 製か確認する。'show media'コマンドを入力し Vender name フィールドに"Brocade"が表示されているか確認する。また、Tx Power フィールドと Rx Power フィールドがゼロではないことをチェックする。
ｄ．MAC アドレステーブルが MAC アドレスを学習しているか確認する。
ｅ．もしスイッチがＶＣＳファブリッククラスターの一部なら、MAC アドレステーブルがクラスタ内の全てのスイッチにわたって正しく同期されているか確認する。
ｆ．LLDP が隣接スイッチを報告しているか確認する。
ｇ．MAC アドレステーブルが他の VCS ファブリックスイッチから学習された MAC アドレスを通知することを保証することにより Ethernet Name Server(ENS)の機能をチェックする。
ｈ．データパスファブリックの接続性を確認するため'l2traceroute'コマンドを使用する。このコ

マンドは、パケットがファブリック内のどこで破棄されたかを特定することを手助けします。
コマンドは、幾つかの基本的なパラメータ入力と拡張パラメータを入力することが出来ます。

現在、サポートしている基本的なパラメータは下記です。
・動的に学習された MAC アドレスの Source Address (SA)と Destination Address (DA)
・VLAN
・Edge routing bridge ID

現在、サポートしている拡張パラメータは下記です。
・プロトコルタイプ(IP)
・ソースと宛先 IP アドレス
・IP プロトコルタイプ(TCP 推奨)
・ソースと宛先ポート番号
IP パラメータの目的は、特定の ECMP 接続を通る'traceroute'パケットを作るためです。

CAUTION
次に示す手順は、コンフィグレーションに影響があるので、注意して使用する必要があります。

7. ファブリック内の流れを追跡するため、許可 ACL を使ってカウンタの増分を観測します

25.3 トラブルシュートのホットスポットを理解する

このセクションは関連する背景説明と問題が報告される Network OS の機能に関連するベスト・プラクティス・ガイダンスを行います。このガイダンスに沿って、多くの可能性がある問題を回避することが出来るはずです。

25.3.1 ライセンス

ライセンスされた機能が働かない時、可能性の高い原因の一つとして、ライセンスが正しくインストールされていないことがあります。機能が正当にライセンスされて正しくインストールされるように 99 ページの『7 ライセンスの管理』に示すガイドラインと手順に従ってください。
ライセンスの回復手順は、318 ページの『25.4.6 ライセンスが正しくインストールされない』を参照下さい。

25.3.2 他社スイッチとの STP 接続性

Juniper や Cisco などの他社スイッチとの間でスパニングツリープロトコル(STP)を使用するため、共用スパニングツリーMAC アドレス(0100.0ccc.cccd)に BPDU を送信するためインタフェースを設定する必要があります。この設定がないと、RPVST+/PVST+のルートブリッジが VLAN1 を含む全ての VLAN を認識しません。

```
switch(conf-if-te-0/1)# spanning-tree bpdu-mac 0100.0ccc.cccd
```

INFORMATION
本設定は、工場出荷時のデフォルトコンフィグで有効になっています。

もし内蔵 DCB スイッチが tagged ポートを設定した VLAN が定義されていて、各 VLAN 上で Rapid Spanning Tree Protocol(RSTP)が有効ならば、VLAN に所属するポートに pvst-mode が定義されていなければ、tagged ポートで受信した BPDU は破棄されます。
次の例は、tagged ポートと VLAN 上で RSTP を有効化する設定例です。

```
vlan 2
tagged ethe 1/24 ethe 2/1 to 2/2
router-interface ve 2
rstp priority 100
```

もし条件が一致すれば、tag 付 BPDU がスイッチを通過するように設定され全てのポートは pvst-mode になるはずです。もし、pvst-mode が有効でない場合は、次の手順で有効化してください。

```
Brocade(config)# interface ethernet 2/1
Brocade(config-if-2/1)# pvst-mode
```

25.3.3　負荷分散配信

負荷分散に関する問題を理解するために、負荷分散アルゴリズムにより使用される条件の基本的な知識をもつ必要があります。表 25-1 は、負荷分散を提供する各機能の詳細を示しています。

表 25-1　負荷分散アルゴリズム

機能	アルゴリズム
ECMP IP	パスは次のパラメータから導出されたハッシュに基づいて選択されています： ・送信元 MAC アドレス ・宛先 MAC アドレス ・VID ・IP プロトコル ・送信元 IP アドレス ・宛先 IP アドレス ・レイヤ 4 送信元ポート ・レイヤ 4 宛先ポート 'fabric-ecm load-balance'および'fabric-ecmp load-balance-hash-swap'コマンドを使用してハッシュフィールドを設定できます。 関連の回復手順については、313 ページの 『25.4.3 期待通り ECMP が負荷分散しない』を参照してください。
LACP	フィールドがフレームで利用可能であるかに応じて、最大 7 つの基準に基づく負荷分散を提供します。
Brocade trunk	メンバリンクの間で、均等パケット負荷分散(ラウンドロビン)を提供します。

25.3.4　RBridge ID の静的割当

RBridge ID の重複は、イーサファブリックにスイッチを組み込む際にエラーの一般的な原因となります。イーサファブリックにスイッチを追加する前に、ユニークな RBridge ID を割り当てなければなりません。もし、新しいスイッチが既存の VCS ファブリッククラスタに追加される場合は、クラスタ内の他のスイッチと同じ VCS ID を割り当てなければなりません。一旦スイッチが追加されると、principal routing bridge は新しいスイッチを含む制御プレーンでネゴシエーションを実行しファブリックを再構築します。データプレーンは影響を受けません。

RBridge ID の重複から回復する手順は 324 ページの『25.4.11 RBridge ID の重複』に記載しています。

25.3.5　FSPF 経路変更

Fabric Shortest Path First (FSPF)アルゴリズムは新たな経路を選択し、一時的なトラフィックの中断を発生させます。これは、古い経路が最初途切れて新しい経路が作成されるので通常の振る舞いです。このような経路変更は、FSPF が新しい最短ルートを構築する時もしくは、現在の経路がダウンした際に発生します。

25.3.6　VCS ファブリックとスタンドアロンモード

スタンドアロンモードと VCS ファブリックでトラブルシュートの際注意すべき重要な違いが存在します。

スタンドアロンモードは、デフォルトでインタフェースが無効、VCS ファブリックではインタフェースが有効となっています。デフォルトコンフィグレーションが適用された場合、この点を考慮してください。

INFORMATION

BS500/BS2000 搭載 DCB スイッチでは、工場出荷時の設定では、スタンドアロンモードでインタフェースは有効になっています。ここでのデフォルトは、スタンドアロンモード/VCS ファブリックを切替えた直後の状態となります。

インタフェースは、スタンドアロンモード/VCS ファブリックでレイヤ 2 スイッチポートとして設定できます。

VCS ファブリックとスタンドアロンモード間の切り替えや元のモードへの切替は、コンフィグレーションの消失やデフォルトコンフィグレーションを使った再起動となります。

port-profile ポートはレイヤ 2 ポートにのみ割当可能です。

管理ポートを介したアウトバンド管理は、デフォルトゲートウェイを設定してください。

25.3.7　vLAG

vLAG の問題をトラブルシュートする前に、vLAG 機能の次の要点に気をつけてください。

- vLAG 上のマルチキャスト(BUM)トラフィック
- エッジポートの要件
- フェイルオーバー

(1)　vLAG 上のマルチキャストトラフィック

フラッディングはいつも vLAG のプライマリリンクを通過します。トラフィックの帯域を設計する際、

この制限を考慮しなければなりません。このリンクは、'show port-channel'コマンドの出力結果であり、アスタリスク(*)で示されます。

```
switch# show port-channel 38
LACP Aggregator: Po 38
Aggregator type: Standard
Admin Key: 0038 -Oper Key 0038
Partner System ID -0x8000,01-e0-52-00-20-00
Partner Oper Key 0038
Member ports:
Link: Te 0/13 (0x180D0102) sync: 1
Link: Te 0/14 (0x180E0103) sync: 1 *
```

(2) vLAG に対するエッジポート要件

LACP はエッジポートで、"Brocade"または"Standard type"の何れかを設定することが出来ます。もし、"Brocade"を選択した場合、リンクリセット(LR)プリミティブを正しく交換するために、エッジの接続先が Brocade Converged Network Adapter(CNA)かスタンドアロンモードの Brocade VDX スイッチか Brocade 8000 であるかを確認してください。

(3) フェイルオーバーと vLAG

高速なフェイルオーバーのために、'vlag ignore-split'コマンドを使用することを推奨します。これにより１秒以下の切り替えを可能とします。このコマンドは Network OS 3.0 以降にアップグレードする時や Network OS 3.0 以降で新たな port-channel を追加すると、自動的に全ての port-channel に設定されます。

この機能を使用する場合、vLAG メンバが互いに切り離してしまう「スプリット・ブレイン」問題を回避するために注意を払ってください。vLAG メンバ間を物理的に分離された複数の経路でスイッチ間接続(ISL)することを推奨します。

25.3.8　vLAG とスプリット・ブレイン

次のトピックは「スプリット・ブレイン」問題とそれを軽減する方法について述べます。

(1) 「スプリット・ブレイン」の解説

「スプリット・ブレイン」は、エンド・ホストやエッジスイッチが vLAG(LACP 使用)により２つの別々のクラスタに接続するケースで発生します。エンド・デバイスは、これらの２つのスイッチが LACP で同じシステム ID を広告するので一つのスイッチのように見えます。

レアケースですが、２つのクラスタスイッチ間の全ての ISL が切断されて、クラスタスイッチが LACP パートナーに同じシステム ID を広告し続けます。これにより、「ファブリックの分離」や「スプリット・ブレイン」状態が発生します。そして、エンド・ホストやエッジスイッチは、このセグメンテーションを検出しないことがあり、両 vLAG スイッチを一つのスイッチとして取り扱うことになります。この状態は、パケットの複製や想定外のパケット喪失となります。

(2) スプリット・ブレイン状態での Network OS のトラフィック防止

デフォルトで、Network OS は「スプリット・ブレイン」問題から回復する機能を持っています。全て

のクラスタスイッチ間の ISL がダウンした時、より低い RBridge ID を持つスイッチが port-channel からセグメント化されたことをエッジスイッチパートナーに伝えるため LACP を使います。それは、広告されるシステム ID を変更することにより行われます。エッジスイッチがメンバの一つから異なるシステム ID を学習すると、その port-channel からこのメンバを削除します。そして、より高い RBridge ID をもつ一つの vLAG メンバスイッチとだけ動作し続けます。他の vLAG メンバスイッチは、依然リンクアップしていますが、もともとの port-channel(sync:0)からセグメント化されたままとなります。この機能で、「スプリット・ブレイン」に起因するパケットの複製やパケット破棄の可能性を回避します。

(3) メンバスイッチがリロードされた場合
より低い RBridge ID をもったスイッチのリロードは何にも影響がありません。

より高い RBridge ID を持ったスイッチがリロードされると、他の vLAG メンバは全ての ISL がダウンしたと認識します。これは、本当の「スプリット・ブレイン」ではありませんが、より低い RBridge ID を持ったスイッチは区別することができず、変更されたシステム ID をパートナーに通知することになります。
パートナーエッジスイッチは２つのイベントと認識するでしょう。

- あるリンク変更でのシステム ID
- 他のインタフェースのダウン

このケースでは、LACP は再ネゴシエーションして port-channnel を再構築します。その間、port-channel はバタついて、一時的にトラフィックに影響を与えます。スイッチが起動しファブリックに再度参加する場合に同様の影響が発生します。

このように、もしより高い RBridge ID を持ったスイッチが再起動すると、一時的にトラフィックを妨害することになる port-channel のバタつきが起こります。低い RBridge ID を持ったスイッチがリロードする時には影響がないことに注意してください。

(4) スイッチリロード中のトラフィック影響の防止
Network OS の動作するスイッチは、論理 port-channel に対して設定できる特別な'vlag ignore-split'オプションを持っており、ユーザーに柔軟性を提供します。このオプションは両方の vLAG メンバポートに設定しなければなりません。

このオプションを設定することは、低い RBridge ID を持ったスイッチのシステム ID の変更を防止することが出来ます。そして、両方のスイッチが同じシステム ID を広告し続けます。この動作は、スイッチの一つがリロードされてトラフィックが操作される時に、対向エッジスイッチの変更を検出することを防止します。

(5) ‘vlag ignore-split’オプションを使用する

‘vlag ignore-split’オプションを使用する場合、全ての ISL が同時にダウンするような状況を回避するために、ISL 周辺に冗長性をもたせる必要があります。全ての接続が同時にダウンする可能性を取り除くために、物理的に分離された複数経路の ISL を使用することを推奨します。

25.3.9 Principal RBridge の可用性

もし新しい Principal RBridge が動作中の VCS ファブリッククラスタに導入、もしくは、Principal ルーティングスイッチが失われることにより新しいスイッチが選出されると、ファブリックのコントロールプレーンは再構築され、データプレーンは混乱無くトラフィックの転送を継続します。VCS ファブリックでの Principal RBridge の初期の役割は、次の通りです。

- RBridge ID の配分
- 仮想管理 IP アドレスの所有
- 構成データベースの同期維持

25.3.10 Brocade トランク

Brocade トランクは、ISL 使用時に動作する唯一のアグリゲーション方法です。

Brocade ISL トランクは、対向スイッチとの間でラインリセット(LR)プリミティブを使って自動的に形成されます。

同一の隣接 Brocade スイッチに接続された全ての ISL ポートはトランクを形成しようとします。トランクの形成に成功するために、スイッチ上の全てのポートは、同じスピードに設定されなければなりません。トランクはデフォルトで有効です。

Brocade トランクは 1G リンクではサポートされません。

Brocade スイッチ間の Brocade トランクの利点を活用するため、少なくとも２つのメンバと複数の ECMP パスを持つことを推奨します。それはまた不慮の切断に備えて接続性を確保するため物理的に分離されたケーブルで経路を確保することも推奨します。

25.3.11 vLAG と NIC チーミング

NIC チーミングは、サーバとスイッチ間リンクのアグリゲーションを可能とします。NIC チーミングは、active/passive モデルか active/active モデルのいずれかです。いずれの場合も、スイッチに必要な設定については、NIC チーミング機能の使用条件に合わせる必要があります。『LAN 拡張機能設定手順書』を参照して、スイッチ側の設定を行ってください。

25.3.12 MTU の選択

通常、スイッチにはホストの最大 MTU+100 バイトを設定します。MTU の定義が時々ベンダの解釈により異なることがあるので、この方法が推奨されます。もし、スイッチの MTU が接続された MTU と同じであれば、パケットがドロップするかもしれません。

25.3.13 オーバーサブスクリプションの回避

ある輻輳条件の下、’show qos rcv-queue interface’コマンドの出力にある“tail-drops”を意味する"packets

dropped"が増加するかを観測してください。

```
switch# show qos rcv-queue interface tengigabitethernet 5/0/1
Interface TenGigabitEthernet TenGigabitEthernet 5/0/1
  In-use 0 bytes, Total buffer 144144 bytes
  0 packets dropped
            In-use          Max
  CoS       Bytes          Bytes
  -------------------------
  0             0            18018
  1             0            18018
  2             0            18018
  3             0            18018
  4             0            18018
  5             0            18018
  6             0            18018
  7             0            18018
```

この状況では、まずボトルネックを特定して輻輳状態を軽減するアクションを採らなければなりません。

(1) 輻輳のボトルネックを特定する
ボトルネックを特定するために、様々な箇所で'show interface'コマンドを入力します。そして、TX 及び RX の破棄が増加しているインタフェースを特定します。TX または RX の破棄に依存して、輻輳は下流のどこかで発生しているはずです。

(2) 輻輳の軽減
輻輳を軽減するために次のアクションを試してください。

- ボトルネックとなる帯域の増加
  - LAG や ECMP パスへの接続数の追加
  - 更に高速なインタフェースの使用
- ボトルネック箇所や隣接デバイスへのフロー制御設定
- QoS の設定
  - クリティカルトラフィックへの分類、マーキング、優先設定
  - スケジューリングの変更。SP または DWRR の効果を検討・比較してください。

フロー制御を有効化するには、サーバなどのエンドステーションからのトラフィックを受信するポートと接続しているエンドデバイス自身に、それぞれ設定してください。port-channel の場合の設定例を次に示します。

```
switch(config)# interface port-channel 100
switch(config-Port-channel-100)# qos flowcontrol tx on rx on
```

一度フロー制御が有効化して、再度'show qos rcv-queue interface'コマンドを入力して、出力をチェックしてください。"packet drops"は見られなくなっているはずです。もし、"packet drops"が継続しているか受信レートが期待より低い場合は、更なる調査のため保守員またはサポート窓口に問合せ下さい。

フロー制御は非対称に設定することを推奨します。任意の隣接する２つのデバイスに対して、一方のデバイスは Rx:ON で Tx:OFF、もう一方は Rx:OFF で Tx:ON です。
輻輳制御については、36 ページの『1.5.4 輻輳制御とキューイング』を参照してください。

25.3.14 ACL の制限事項

もし、表 25-4 に示す ACL 使用時の制限事項を守っているなら、システム制限に遭遇することは殆どありません。ACL は迅速かつ正確にインスタンスかする必要があります。

表 25-2　ACL の制限

条　件	制限
標準または拡張ACL数は、各々のスイッチのために作成されますが、適用されません。	50
標準または拡張 ACL ごとのルール数	256
ACL が同時に適用される物理インタフェイス数	60(スタンドアロンモード) 48(VCS モード)
ACL が同時に適用される VLAN インタフェイス数	100
ACL カウンタ数	252
TCAM テーブルエントリ数	1000
スイッチ当たりの ACL ルール数	6000
適用された共存の標準および拡張 ACL 数	50

加えて、30,720 までの MAC アドレスをサポートしています。
これらの制限の組み合わせに近づいたり越えたりすると、ACL ルールのインスタンス化が遅延したり、プロセス例外が発生したり、MAC 学習問題のために ACL が失敗したりする可能性があります。
もし、ACL や VLAN の数が超過すると、ACL ルールとカウンターのインスタンス化において数分の遅延が発生します。L2SYS プロセスメッセージキューが一杯になるか、プロセス切り替えやスケジューリングが ACL のインスタンス化を遅延させるまで増加します。
‘show statistics access-list mac’コマンドの周期的なモニタリングにより、非ゼロの 252 以上の ACL ルールと正しくインスタンス化されハードウェアカウンタが割り当てられたルールに対して増加するフレームカウントが無いことを確認します。
プロセス例外は、ACL の組合せが限界に近づくか超過した場合、時々L2YSD プロセスで発生します。
一定の MAC 学習や破棄は、チップ内のテーブル限界が超過した場合に発生します。MAC アドレステーブルエントリ数が超過した場合、レイヤ 2 フレームスイッチングは失敗します。

25.4　トラブルシューティング手順

この章では、遭遇する可能性のある幾つかの問題の説明と、その問題の調査及び解決方法に関して提案を行っています。もし、これらの手順で問題の解決に至らない場合、ページの“Getting technical help”

に記載しているように、サポート窓口や保守員に問合せの準備をしてください。

- 310 ページの AMPP が動作しない
- 313 ページの不意の CPU 利用率高騰
- 313 ページの期待通り ECMP が負荷分散しない
- 314 ページの ENS の機能チェック
- 315 ページの ISL が動作しない
- 318 ページのライセンスが正しくインストールされない
- 318 ページのハードウェアでのパケット破棄
- 324 ページの Ping 失敗
- 324 ページの tail drops
- 324 ページの QoS は正しくパケットをマーキング・取り扱わない
- 324 ページの RBridge ID の重複
- 325 ページの SNMP MIB の不正値報告
- 325 ページの SNMP trap 通知の失敗
- 325 ページのスイッチへの telnet 失敗
- 326 ページの Trunk メンバ未使用
- 327 ページのアップデート失敗
- 327 ページの VCS ファブリックが形成されない
- 328 ページの vLAG が形成されない

25.4.1　AMPP が動作しない

Automatic Migration of Port Profiles (AMPP)を設定するのは複雑です。AMPP はスタンドアロンモードと VCS ファブリックモードの何れでも動作します。AMPP の設定に関する詳細は『13 AMPP の設定』を参照下さい。

AMPP を使用する場合に遭遇する問題は、ポートプロファイル自身の定義エラーによることが一般的です。そのエラーは、仮想マシン(VM)との関連付けやホストアダプタと AMPP の互換性問題などがあります。特に、AMPP の問題は、次の条件で発生します。

- ポートプロファイルの定義が対象スイッチ上に無い、または、switchport や VLAN の定義を含んでいない。311 ページの『25.4.1 (1)ポートプロファイルの定義の確認』を参照下さい。
- VM の MAC アドレスが MAC アドレステーブルにない。311 ページの『25.4.1 (2)VM の MAC アドレスの確認』を参照下さい。
- ポートプロファイルが有効化されない、または正しい MAC アドレスに関連付けされない。312 ページの『25.4.1 (3) ポートプロファイル状態の確認』を参照下さい。
- VM カーネルの MAC アドレスがそれぞれのスイッチのポートプロファイルと正しく関連付けされない。312 ページの『25.4.1 (4) VM カーネルの MAC アドレスの確認』を参照下さい。
- VM とその関連付けたホストが共通のストレージデバイスを共用しない。312 ページの『25.4.1 (5) 共用ストレージデバイスの確認』を参照下さい。

- ポートプロファイルが非プロファイル VLAN で学習される。312 ページの『25.4.1 (6) 学習済みプロファイル MAC アドレスの状態確認』を参照下さい。
- ポートプロファイルが同一インタフェースでコンフリクトしている。313 ページの『25.4.1 (7)ポートプロファイルの競合がないことを確認』を参照下さい。
- イーサネットネームサーバが正しく動作しない。313 ページの『25.4.1 (8) イーサネットネームサーバの確認』を参照下さい。
- ESX ホストがインストールされたネットワークアダプタやドライバと互換性が無い。313 ページの『25.4.1 (9) ESX ホストの確認』を参照下さい。

(1) ポートプロファイルの定義の確認

有効なポートプロファイルは、対象のスイッチ上に存在していなければなりません。そしてポートプロファイルは、基本的な switchport 設定と VLAN 設定が含まれている必要があります。

1. 特権実行モードにおいて、対象スイッチ上にポートプロファイルが存在するか、また基本的な switchport 及び VLAN の定義が含まれているか確認するため、'show running-config port-profile' コマンドを入力します。

```
switch# show running-config port-profile
port-profile UpgradedVlanProfile
 vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
 !
!
port-profile default
vlan-profile
switchport
switchport mode trunk
switchport trunk allowed vlan all
switchport trunk native-vlan 1
!
!
port-profile pp1
vlan-profile
!
!
port-profile pp2
vlan-profile
!
```

2. もしポートプロファイルの定義が存在してなかったり、必要な switchport や VLAN の定義を忘れている場合は、157 ページの『13.2 AMPP ポートプロファイルの構成』の記載に従ってポートプロファイルを作成してください。

(2) VM の MAC アドレスの確認

AMPP を正しく機能させるために、VM に対する MAC アドレスとその関連付けられたホストが、MAC アドレステーブルに登録されていなければなりません。

1. VM の MAC アドレスがスイッチの MAC アドレステーブルに登録されているか確認するため、'show mac-address-table'コマンドを入力します。

```
switch# show mac-address-table
VlanId Mac-address Type State Ports
```

```
1 0000.0010.0001 Dinamic Active Te 4/0/3
1 0000.0010.0002 Dinamic Active Te 4/0/3
Total MAC addresses : 2
```

2．もし、VM の MAC アドレスが存在していない場合は、更に調査するためサポート窓口か保守員に問い合わせて、情報を提供してください。

(3) ポートプロファイル状態の確認

AMPP を正しく機能させるには、ポートプロファイルは有効であり、正しい MAC アドレスに関連付けられている必要があります。

1．ポートプロファイルが有効で正しい MAC アドレスに関連付けられているかを確認するため、'show port-profile status'コマンドを入力します。

```
switch# show port-profile status
Port-Profile           PPID        Activated        Associated MAC
Interface
UpgradedVlanProfile      1           No               None                    None
pp1                        2           No               None
None
pp2                        3           No               None
None
```

2．次に示すような設定ミスを修正します。

もし、ポートプロファイルが有効でない場合、有効化するために、'port-profile [profile-name] activate'コマンドを入力します。

もし、ポートプロファイルが MAC アドレスに関連付けられてない場合は、関連付けするために'port-profile [port-profile-name] static'コマンドを入力します。

```
switch(config)# port-profile pp3 static 0050.5600.10030
```

もし、ポートプロファイルが誤った MAC アドレスに関連付けられている場合、正しくない MAC アドレスとの関連付けを切るため、'no port-profile port-profile-name static'コマンドを入力し、それから正しい MAC アドレスに関連付けてください。

```
switch(config)# no port-profile pp3 static 0050.5600.10020
switch(config)# port-profile pp3 static 0050.5600.10030
```

ポートプロファイルの有効化や MAC アドレスへの関連付けの詳細については、160 ページの『13.2.2 新しいポートプロファイルの構成』を参照してください。

(4) VM カーネルの MAC アドレスの確認

VM カーネルの MAC アドレスがそれぞれのスイッチ上にあるポートプロファイルに関連付けられているかを確認します。もし関連付けられていない場合、311 ページの『25.4.1 (1) ポートプロファイルの定義の確認』の記載に従って、関連付けてください。

(5) 共用ストレージデバイスの確認

VM とその関連するホストがストレージデバイスを共用しているか確認します。もし共用されて無い場合は、ストレージデバイスを共用するように VM とホストを再設定してください。

(6) 学習済みプロファイル MAC アドレスの状態確認

AMPP を正しく機能させるために、MAC アドレスは有効なソースであるプロファイル VLAN から学習される必要があります。この手続きは、MAC アドレスが有効なソースから学習されているかどうかで決定されます。

1．学習済みのプロファイル MAC アドレスの状態をチェックするために、'show mac-address-table

port-profile'コマンドを入力します。

```
switch# show mac-address-table port-profile
Legend: Untagged(U), Tagged (T), Not Forwardable(NF) and Conflict(C)
VlanId Mac-address Type State Port-Profile Ports
1 0050.5679.5351 Dynamic Active Profiled(U) Te 111/0/10
1 0050.567b.7030 Dynamic Active Profiled(U) Te 111/0/12
1 005a.8402.0000 Dynamic Active Profiled(T) Te 111/0/24
1 005a.8402.0001 Dynamic Active Profiled(NF) Te 111/0/24
1 005a.8402.0002 Dynamic Active Not Profiled Te 111/0/24
1 005a.8402.0003 Dynamic Active Not Profiled Te 111/0/24
1 005a.8402.0004 Dynamic Active Not Profiled Te 111/0/24
(output truncated)
Total MAC addresses : 17
```

"Not Profiled."と表示される MAC アドレスを確認、調査します。

(7) ポートプロファイルの競合がないことを確認

1．競合無く複数のポートプロファイルがインタフェースに適用されているかを確認するために、'show port-profile name pp1_name name pp2_name validate'コマンドを入力します。

```
switch# show port-profile name pp1 name pp2 validate
Port-Profile Port-Profile Conflicts

pp1 pp2
vlan-profile vlan-profile No
qos-profile qos-profile No
security-profile security-profile No
```

2．もし競合しているなら、一方のポートプロファイルを再設定します。

共存ルールに関する情報は、155 ページ『13 AMPP の設定』を参照してください。

(8) イーサネットネームサーバの確認

AMPP はクラスタ内の各 VCS ファブリックスイッチが MAC アドレステーブルで同一に見えることが必要です。どのような違いがあっても、イーサネットネームサーバ(ENS)の問題を意味しています。詳細は、314 ページの『25.4.4 ENS の機能チェック』を参照してください。

(9) ESX ホストの確認

各 ESX ホストが適切なドライバとともに正しい Converged Network Adapter (CNA)がインストールされており、Cisco Nexus 1000V 仮想スイッチが使われていないかを確認します。(Cisco Nexus 1000V は、加工された特別なパケットを送信するので動作しません。)

25.4.2　不意の CPU 利用率高騰

不意の CPU 利用率高騰は、普通、CPU サイクルを大量に消費するプロセスの結果です。その結果、telnet でのスイッチへのアクセスを妨げたり、ISL を動作させなくします。

もし、CPU 利用率高騰が疑われるなら、次の手順を実行してください。

1．特権実行モードで、どのプロセスが CPU を消費しているかを確認するため'show process cpu'コマンドを実行してください。

2．対応するインタフェースを shutdown したり、CPU 消費の原因と疑われる設定を削除してください。

25.4.3　期待通り ECMP が負荷分散しない

Equal cost multipath (ECMP)ルーティングは、最適コストで複数経路を通るトラフィックを分散させることによりスループットを増大させます。もし、期待通りトラフィックが分散されていないと疑われ

る場合、次の手順を実行してください。

1．特権実行モードで、ECMP 経路が期待通りか確認するため、'show fabric route topology'コマンドを入力してください。

```
switch# show fabric route topology

Total Path Count: 1

Src  Dst  Out  Out            Nbr  Nbr
RB-ID RB-ID Index Interface    Hops Cost Index Interface     BW  Trunk
------------------------------------------------------------------------------
66     60     6      T3 66/0/4   1     500   6      Te 60/0/7    10G Yes
```

もし、出力結果がソースとデスティネーションスイッチ間の equal cost path が表示されたら、ECMP の負荷分散は期待通りです。

2. 期待されるフロー数になっているかを確認するため、インタフェースの利用率をチェックします。

3．レイヤ 2/3/4 のフローがそれぞれの ECMP リンクにハッシュされているか調査するため'l2traceroute'コマンドを入力します。

ECMP 固有操作の妨害を避けるため、正しく機能する Brocade ルーティング方針は、一つの決定的な経路に沿って特定のフローを送信します。追加のフローは利用可能なコスト等価のルートを使います。この手順は、このハッシュ方針が正しく機能しているかを確認するものです。

'l2traceroute'コマンドの使用方法詳細は、330 ページの『25.5.1 Layer 2 traceroute』を参照下さい。

25.4.4　ENS の機能チェック

イーサネットネームサーバ(ENS)は、MAC アドレステーブルの内容が同一 VCS ファブリッククラスタ内のスイッチ間で一致している時、正しく動作しています。ENS が正しく動作しているかを確認するため次のチェックを行ってください。

- ファブリックメンバの情報が期待通りかチェックする。314 ページの『25.4.4 (1) ファブリックの確認』を参照してください。
- MAC アドレスがポート間を移動してないか確認する。315 ページの『25.4.4 (2) ポート間の MAC アドレスの移動をチェック』を参照してください。
- エッジポートが外部ループを持っていないか確認する。315 ページの『25.4.4 (3) エッジポートの外部ループの確認』を参照してください。

(1) ファブリックの確認

'show fabric all'コマンドを入力し、VCS ファブリッククラスタの全てのスイッチに関して情報が表示されるかを確認します。

```
switch# show fabric all

VCS Id: 1
Config Mode: Local-Only

Rbridge-id  WWN                       IP Address        Name
------------------------------------------------------------------------------
  1         50:00:51:E4:44:40:0E:04   0.0.0.0           "fcr_fd_1"
  2         50:00:51:E4:44:50:0F:09   0.0.0.0           "fcr_xd_2_128"
 60         10:00:00:05:33:5F:EA:A4   10.24.81.65       "switch"
 66         10:00:00:05:33:67:26:78   10.24.81.66      >"switch"
The Fabric has 4 Rbridge(s)
```

(2) ポート間の MAC アドレスの移動をチェック
ポートからポートへの MAC アドレスの移動は、同一のソースアドレスが複数のポートで検出される時発生します。この状態は、"MAC address flapping"として知られています。
MAC address flapping をチェックするため、'show mac-address-table'コマンドを複数回入力し、出力をチェックします。

(3) エッジポートの外部ループの確認
物理的な外部ループをチェックします。

25.4.5 ISL が動作しない

VCS ファブリッククラスタ内の２つのスイッチ間の接続(ISL)の失敗には、様々な理由があります。

- ISL 設定が無効になっている。315 ページの『25.4.5 (1) ISL ステータスの確認』を参照下さい。
- ISL がセグメントされている。315 ページの『25.4.5 (1) ISL ステータスの確認』を参照下さい。
- VCS ファブリックモードが一方のスイッチで無効になっている。316 ページの『25.4.5 (2) VCS ファブリック設定とルートブリッジ ID の確認』を参照下さい。
- 各スイッチで VCS ID が異なっている。316 ページの『25.4.5 (2) VCS ファブリック設定とルートブリッジ ID の確認』を参照下さい。
- 隣接スイッチに LLDP が通知されてない。317 ページの『25.4.5 (3) LLDP の確認』を参照下さい。
- CPU オーバーロードで keepalive パケット生成に失敗している。318 ページの『25.4.5 (4) CPU 過負荷の確認』を参照下さい。

(1) ISL ステータスの確認
もし、どのポートも動作が怪しい場合、ISL ステータスをチェックします。

1．スイッチ上の異常なリンクの両端にて、特権実行モードで、ISL 接続の状態を見るため、'show fabric isl'コマンドを入力します。

```
switch1# show fabric isl
Rbridge-id: 2 #ISLs: 2
Src Src Nbr Nbr
Index Interface Index Interface Nbr-WWN BW Trunk Nbr-Name

1 Te 2/0/1 1 Te 3/0/1 10:00:00:05:1E:CD:7A:7A 10G Yes "switch1"
2 Te 2/0/2 ? Te ?/?/? ??:??:??:??:??:??:??:?? (segmented -incompatible)
26 Te 2/0/26 56 Te 25/0/56 10:00:00:05:33:40:2F:C9 60G Yes "Edget12r31_25"
34 Te 2/0/34 58 Te 26/0/58 10:00:00:05:33:41:1E:B7 40G Yes "Edget12r32_26"

Ports on which the ISL link is broken appear with the text "(segmented -incompatible)."
Ports for which the ISL configuration is disabled do not appear in the output.
```

2．疑わしいポートの状態に関して、更に情報を採取するため'show fabric islports'コマンドを入力します。

```
sw0# show fabric islports
Name:          sw0
Type:          107.4
State:         Online
Role:          Fabric Subordinate
VCS Id:        10
Config Mode:   Local-Only
Rbridge-id:    11
WWN:           10:00:00:05:33:6d:7f:77
FCF MAC:       00:05:33:6d:7f:77
```

```
 Index    Interface   State   Operational State
=====================================================================
  1       Te 11/0/1   Up      ISL 10:00:00:05:33:00:77:80 "sw0" (upstream)(Trunk
Primary)
  2       Te 11/0/2   Down
  3       Te 11/0/3   Down
  4       Te 11/0/4   Up      ISL (Trunk port, Primary is Te 11/0/1 )
  5       Te 11/0/5   Down
  6       Te 11/0/6   Down
  7       Te 11/0/7   Down
  8       Te 11/0/8   Down
  9       Te 11/0/9   Down
 10       Te 11/0/10  Down
 11       Te 11/0/11  Up      ISL 10:00:00:05:1e:00:50:00 "sw0" (Trunk Primary)
121       Fi 11/0/1   Up LS   ISL 50:00:53:37:b6:93:5e:02 "fcr_fd_160"
(downstream)
(Trunk Primary)
122       Fi 11/0/2   Up LS   ISL (Trunk port, Primary is Fi 11/0/1 )
123       Fi 11/0/3   Down
124       Fi 11/0/4   Down
125       Fi 11/0/5   Down
126       Fi 11/0/6   Down
127       Fi 11/0/7   Down
```

3．もし、ポートの状態が"Down"なら、'no shutdown'コマンドでポートを有効化します。

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# no shutdown
```

4．もし、ポートの状態が"Up"だが、ISL がセグメントされている場合、セグメントされている理由のため"Operational State"を更なる手がかりとして調べる。

'show fabric islports'コマンドとセグメントされた ISL の"Operational State"文字列の説明は、『Network OS Command Reference』を参照してください。

(2) VCS ファブリック設定とルートブリッジ ID の確認

ISL を正常に動作させるために、次の条件を守らなければなりません。

- 両スイッチで VCS ファブリックモードが有効であること
- 両スイッチで同じ VCS ID を使っていること
- 各スイッチでユニークなルーティング ID を使っていること

条件をチェックするため、次の手順を実行してください。

1．各スイッチで、'show vcs'コマンドを入力する

2．出力によって、次の手順を実行する

もし、どちらかのスイッチで VCS ファブリックモードが有効でない場合、有効にするため'vcs enable'コマンドを入力する。

```
switch1# show vcs
Config Mode : Local-Only
VCS Mode       : Fabric Cluster
VCSID :1
Total Number of Nodes : 1
Rbridge-Id   WWN                          Management IP   VCS Status       Fabric
Status        HostName
-----------------------------------------------------------------------------
-----------------------------
66           >10:00:00:05:33:FF:8E:EF* 192.168.0.79    Online           Online
switch1

switch2# show vcs
```

```
state : Disabled

switch2# vcs vcsid 77 enable
```

もし、'show vcs'コマンドの結果、互いの VCS ID が一致していない場合、設定を誤っているスイッチの VCS ID を修正するため'vcs vcsid'コマンドを入力します。

```
switch1# show vcs
Config Mode : Local-Only
VCS Mode       : Fabric Cluster
VCS ID         : 1
Total Number of Nodes           : 1
Rbridge-Id   WWN                          Management IP   VCS Status       Fabric
Status        HostName
-------------------------------------------------------------------------------
------------------------------
66           >10:00:00:05:33:FF:8E:EF* 192.168.0.79    Online           Online
switch1

switch2# show vcs
Config Mode : Local-Only
VCS Mode       : Fabric Cluster
VCS ID         : 2
Total Number of Nodes           : 1
Rbridge-Id   WWN                          Management IP   VCS Status       Fabric
Status        HostName
-------------------------------------------------------------------------------
------------------------------
77           >10:00:00:05:33:A4:E3:33*  192.168.0.77    Online           Online
swith2
swith2# vcs vcsid 1
```

もし、両スイッチとも同じ RBridge ID を持っているなら、RBridge ID をユニークな値に変更するため、'vcs rbridge-id'コマンドを入力する。

```
switch1# show vcs
Config Mode  : Local-Only
VCS Mode       : Fabric Cluster
VCS ID         : 1
Total Number of Nodes           : 1
Rbridge-Id   WWN                          Management IP   VCS Status       Fabric
Status        HostName
-------------------------------------------------------------------------------
------------------------------
66           >10:00:00:05:33:FF:8E:EF* 192.168.0.79    Online           Online
switch1


switch2# show vcs
Config Mode  : Local-Only
VCS Mode       : Fabric Cluster
VCS ID         : 1
Total Number of Nodes           : 1
Rbridge-Id   WWN                          Management IP   VCS Status       Fabric
Status        HostName
-------------------------------------------------------------------------------
------------------------------
66           >10:00:00:05:33:FF:CA:BC* 192.168.0.78    Online           Online
swith2
swith2# vcs rbridge-id 77
```

(3) LLDP の確認

ISL が正しく機能するとき、'show lldp neighbors'コマンドは VCS ファブリッククラスタ内の各隣接スイッチの情報を表示します。

1．全ての隣接スイッチの LLDP 通知を確認するため'show lldp neighbors'コマンドを入力します。

```
switch1# show lldp neighbors
Local Intf Dead Interval Remaining Life Remote Intf Chassis ID Tx Rx
Te 66/0/55 120 106 port1 0005.1e78.f004 20300 19914
Te 66/0/60 120 108 port0 0005.1e55.16c8 20300 19911
```

2．もし隣接スイッチが無ければ、更なる調査を行うか、サポート窓口か保守員に連絡してください。

(4) CPU 過負荷の確認

異常な CPU 高負荷は ISL の誤動作の原因となります。CPU 過負荷のトラブルシュートのために、313 ページの『25.4.2 不意の CPU 利用率高騰』の記載に従って、'show process cpu'コマンドを使ってください。

25.4.6　ライセンスが正しくインストールされない

ライセンスされた機能が機能していないなら、大抵はその機能に対するライセンスが正しくインストールされていないからです。いずれかのライセンスがインストールされていないか、インストールされているが必ず必要なシステムリブートが実行されてないかのいずれかです。

もし、３つ目のスイッチを VCS ファブリッククラスタに追加できないなら、恐らく VCS Fabric license がインストールされていないでしょう。(NOS v3.0.0_dcb3 以前の場合。)

もし、ライセンスが正しくインストールされていない疑いがあるなら、次の手順を実行してください。

1．特権実行モードで、現在どのライセンスがインストールされているかを確認するため、'show license'コマンドを実行してください。

```
switch# show license
rbridge-id: 66
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
       VCS Fabric license
       Feature name:VCS_FABRIC
       License is valid
```

2．ライセンスが'show license'コマンドで表示されなかった場合、インストールされていません。特権実行モードにて、ライセンスをインストールするために、'license add lictstr'コマンドを入力してください。

```
switch# license add licstr "*B
slSETgzTgeVGUDeQR4WIfRx7mmXODdSwENoRGEnAmX3Ca3uHeZgXK0b,jzxyzfzKLrMsPN8ClSxvD
QRRT8VyuULyyKTO0ryU6qm4s1jjiSAeV,COoedzCx1v6ycQgnYMeSVp#"

License Added [*B
slSETgzTgeVGUDeQR4WIfRx7mmXODdSwENoRGEnAmX3Ca3uHeZgXK0b,jzxyzfzKLrMsPN8ClSxvD
QRRT8VyuULyyKTO0ryU6qm4s1jjiSAeV,COoedzCx1v6ycQgnYMeSVp#]
```

25.4.7　ハードウェアでのパケット破棄

この章では、全てのトラフィック、特定のトラフィック、特定のタイプのトラフィック、定常的、一時的にパケット破棄が発生した時の問題のトラブルシュートについて説明します。パケット破棄は次に示す多くの理由で発生します。

- エンドデバイスでの高遅延。319 ページの『25.4.7 (1) 高遅延エンドデバイスによるパケット破棄』を参照下さい。
- データパスの障害。321 ページの『25.4.7 (2) データパスの確認』を参照下さい。
- CRC エラー、パケットエラー、NIC との相互接続性エラーによるオプティカルライン上のノイズ。323 ページの『25.4.7 (3) オプティカルラインのノイズをチェック』を参照下さい。

(1) 高遅延エンドデバイスによるパケット破棄

エンドデバイスが想定より応答に時間がかかることが原因で、ファブリック内のバッファオーバーランにより時々パケットが破棄されることがある。例えば、想定程早くデータを処理できないために、過負荷のディスクアレイがそのような遅延を発生さます。長時間データ受信を停止するデバイスは過度の遅延を発生させます。

これらの問題に対する究極のソリューションは、エンドデバイス自身を修正することです。しかし、スイッチとファブリックの設定に調整を加えることで問題を軽減することができます。

エンドデバイスでの遅延に起因する輻輳とパケット破棄を検出・緩和するために、次の手順を実行してください。

1．エンドデバイスが DCB に準拠していることを示す"DCBX TLVs"をチェックし、DCB ケイパビリティを広告しているかを確認するため、'show lldp neighbors detail'コマンドを入力してください。

```
switch# show lldp neighbors detail
Neighbors for Interface Te 66/0/11

MANDATORY TLVs
===============
Local Interface: Te 66/0/11  (Local Interface MAC: 0005.33ff.8f1e)
Remote Interface: 0090.fa27.e24b (Remote Interface MAC: 0090.fa27.e24b)
Dead Interval: 120 secs
Remaining Life : 98 secs
Chassis ID: 0090.fa27.e24b
LLDP PDU Transmitted: 79  Received: 28

OPTIONAL TLVs
==============
System Description: Emulex OneConnect 10Gb Multi function Adapter
System Capabilities: Station Only
System Capabilities Enabled: Station Only

DCBX TLVs
===========
Version : CEE
DCBX Ctrl OperVersion: 0  MaxVersion: 0  SeqNo: 2 AckNo: 2
DCBX ETS OperVersion: 0  MaxVersion: 0  Enabled: 1  Willing: 1 Error: 0
Enhanced Transmission Selection (ETS)
  Priority-Group ID Map:
    Priority : 0  1  2  3  4  5  6  7
    Group ID : 0  0  0  0  1  0  0  0
  Group ID Bandwidth Map:
    Group ID  :   0   1   2   3   4   5   6   7
    Percentage:  50  50   0   0   0   0   0   0
    Number of Traffic Classes supported: 2
DCBX PFC OperVersion: 0  MaxVersion: 0  Enabled: 1  Willing: 1 Error: 0
Priority-based Flow Control (PFC)
     Enabled Priorities: 4
     Number of Traffic Class PFC supported: 8
FCoE App OperVersion: 0  MaxVersion: 0  Enabled: 1  Willing: 1 Error: 0
FCoE Application Protocol
     User Priorities: none
iSCSI App OperVersion: 0  MaxVersion: 0  Enabled: 1  Willing: 1 Error: 0
iSCSI Application Protocol
     User Priorities: 4
```

2．Pause フレームをチェックするため、'show qos flowcontrol interface'コマンドを入力します。

```
switch# show qos flowcontrol interface tengigabitethernet 66/0/55
Interface TenGigabitEthernet 66/0/55
 Mode PFC
```

```
 DCBX enabled for PFC negotiation
 TX 4926331124 frames
     TX    TX      RX      RX     Output Paused
CoS Admin  Oper    Admin   Oper   512    BitTimes
----------------------------------------
 0  Off    Off     Off     Off         0
 1  Off    Off     Off     Off         0
 2  Off    Off     Off     Off         0
 3  On     On      On      On          0
 4  Off    Off     Off     Off         0
 5  Off    Off     Off     Off         0
 6  Off    Off     Off     Off         0
 7  Off    Off     Off     Off         0
```

3．Cos 統計情報をチェックするため、'show qos queue interface'コマンドを入力します。

```
switch# show qos queue interface tengigabitethernet 66/0/60
Interface TenGigabitEthernet 66/0/60
           RX       RX             TX          TX
 CoS     Packets   Bytes   TC    Packets     Bytes
 ---------------------------------- ----------------------------------
  0     1600    354184     0        0           0
  1        0         0     1     7962      636960
  2        0         0     2        0           0
  3     8508    544832     3       18        6048
  4        0         0     4        0           0
  5        0         0     5        0           0
  6        0         0     6        0           0
  7        0         0     7     2123      282360
 untag 2082 216528
```

4．破棄されたパケット、バッファ消費、およびリアルタイムのキュー統計を含む輻輳の指標をチェックするため、'show qos rcv-queue interface'コマンドを入力します。

```
switch# show qos rcv-queue interface tengigabitethernet 66/0/55
Interface TenGigabitEthernet TenGigabitEthernet 66/0/55
 In-use 27216 bytes, Total buffer 144144 bytes
 0 packets dropped
         In-use    Max
 TC      Bytes   Bytes
-------------------------
  0       0      252
  1       0      252
  2       0      252
  3   27216     75284
  4       0      252
  5       0      252
  6       0     57456
  7       0      9576
```

5．QoS の設定をチェックするため、'show qos interface'コマンドを入力します。

```
switch# show qos interface tengigabitethernet 66/0/55
Interface TenGigabitEthernet 66/0/55
 Provisioning mode cee
 Priority Tag disable
 CEE Map default
 FCoE CoS: 3
 FCoE Provisioned
 Default CoS 0
 Interface trust cos
          In-CoS:  0  1  2  3  4  5  6  7
   ------------------------------------------------------
   Out-CoS/TrafficClass: 0/6 1/6 2/6 3/3 4/6 5/6 6/6 0/7
 Per-Traffic Class Tail Drop Threshold (bytes)
      TC:   0   1   2   3   4   5   6   7
   ------------------------------------------------------------------
```

```
  Threshold:  252  252  252 75284  252  252 57456  9576
Flow control mode PFC
  CoS3 TX on, RX on
Multicast Packet Expansion Rate Limit 3000000 pkt/s, max burst 4096 pkts
Multicast Packet Expansion Tail Drop Threshold (packets)
  TrafficClass:  0  1  2  3  4  5  6  7
  ------------------------------------------------
   Threshold:  64  64  64  64  64  64  64  64
Traffic Class Scheduler configured for 1 Strict Priority queues
  TrafficClass:  0  1  2  3  4  5  6  7
  ------------------------------------------
   DWRRWeight:  0  0  0 40  0  0 60 ---
Multicast Packet Expansion Traffic Class Scheduler
  TrafficClass:  0  1  2  3  4  5  6  7
  ------------------------------------------------
   DWRRWeight:  12  13  12  13  12  13  12  13
```

6．QoS を再設定します。239 ページの『20 QoS の設定』を参照下さい。

(2) データパスの確認

この手順では、ファブリックの一貫性が破棄されたパケットの原因かどうかをチェックします。

1．エンドデバイスへのパスをテストするために'ping'コマンドを入力します。

```
switch# ping 10.24.81.2
PING 10.24.81.2 (10.24.81.2): 56 octets data
64 octets from 10.24.81.2: icmp_seq=0 ttl=128 time=9.4 ms
64 octets from 10.24.81.2: icmp_seq=1 ttl=128 time=0.3 ms
64 octets from 10.24.81.2: icmp_seq=2 ttl=128 time=0.3 ms
64 octets from 10.24.81.2: icmp_seq=3 ttl=128 time=0.3 ms
64 octets from 10.24.81.2: icmp_seq=4 ttl=128 time=0.3 ms


---10.24.81.2 ping statistics --5
packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/2.1/9.4 ms
```

2．パケットが到達したかエラーで破棄されたかを確認するために、'show interface'コマンドを入力します。特に、次の例に示す受信統計情報のパケット数、バイト数やエラーパケットの数値が重要です。

```
switch# show interface tengigabitethernet 66/0/60
TenGigabitEthernet 66/0/60 is up, line protocol is up (connected)
Hardware is Ethernet, address is 0005.3367.26d8
  Current address is 0005.3367.26d8
Pluggable media present
Interface index (ifindex) is 283874428169
MTU 2500 bytes
LineSpeed Actual  : 10000 Mbit
LineSpeed Configured : Auto, Duplex: Full
Flowcontrol rx: off, tx: off
Last clearing of show interface counters: 22:07:59
Queueing strategy: fifo
Receive Statistics:
  15254 packets, 1395269 bytes
  Unicasts: 10641, Multicasts: 2637, Broadcasts: 1976
  64-byte pkts: 10874, Over 64-byte pkts: 3294, Over 127-byte pkts: 117
  Over 255-byte pkts: 969, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
  Over 1518-byte pkts(Jumbo): 0
  Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
  Errors: 0, Discards: 0
Transmit Statistics:
  12633 packets, 1155963 bytes
  Unicasts: 18, Multicasts: 12615, Broadcasts: 0
  Underruns: 0
```

```
  Errors: 0, Discards: 0
Rate info (interval 299 seconds):
  Input 0.000128 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 1d00h40m
```

3．光モジュールが Brocade 製かをチェックするため'show media interface'コマンドを入力します。Vendor Name フィールドをチェックします。また、TX Power と RX Power フィールドがゼロでないことを確認します。

```
switch# show media interface tengigabitethernet 66/0/60
 Interface   TenGigabitEthernet 66/0/60
 Identifier   3 SFP
 Connector   7 LC
 Transceiver     0000000000000010 10_GB/s
 Name      id
 Encoding    6
 Baud Rate   103 (units 100 megabaud)
 Length 9u   0 (units km)
 Length 9u   0 (units 100 meters)
 Length 50u   8 (units 10 meters)
 Length 62.5u  3 (units 10 meters)
 Length Cu   0 (units 1 meter)
 Vendor Name  BROCADE
 Vendor OUI   00:05:1e
 Vendor PN   57-0000075-01
 Vendor Rev   A
 Wavelength   850 (units nm)
 Options    001a
 BR Max     0
 BR Min     0
 Serial No   AAA209282044472
 Date Code   090709
 Temperature  35 Centigrade
 Voltage    3356.4 (mVolts)
 Current    5.564 (mAmps)
 TX Power    568.9 (uWatts)
 RX Power    549.9 (uWatts)
```

4．MAC アドレステーブルが新しい値を学習しているかを確認するため、'show mac-address-table'コマンドを入力します。新しい MAC アドレスはここに現れます。

```
switch# show mac-address-table
VlanId   Mac-address       Type    State    Ports
1002     0efc.0042.7300    FPMA    Active   Te 66/0/55
1002     0efc.0042.7302    FPMA    Active   Te 66/0/55
1002     0efc.0042.7800    FPMA    Active   Te 66/0/60
Total MAC addresses : 3
```

5．LLDP が全ての隣接スイッチを報告するか確認するために、'show lldp neighbors'コマンドを入力します。

```
switch# show lldp neighbors
Local Intf Dead Interval Remaining Life Remote Intf Chassis ID Tx
Rx
Te 66/0/55 120 101 port1 0005.1e78.f004 3000
2948
Te 66/0/60 120 117 port0 0005.1e55.16c8 2999
2945
```

もし、コマンド出力が全ての隣接スイッチを表示しない場合、サポート窓口か保守員に連絡してください。

6．イーサネットネームサーバの機能確認と、他の VCS ファブリックスイッチから学習済み MAC ア

ドレスが存在するかを確認するため、'show mac-address-table'コマンドを入力します。
それらのスイッチがこの MAC アドレスを参照できるかを確認するため、ファブリック内の他のスイッチ上で、このコマンドを入力します。

```
switch# show mac-address-table
VlanId   Mac-address       Type    State    Ports
1002     0efc.0042.7300    FPMA    Active   Te 66/0/55
1002     0efc.0042.7302    FPMA    Active   Te 66/0/55
1002     0efc.0042.7800    FPMA    Active   Te 66/0/60
Total MAC addresses : 3
```

7．データパスのファブリック一貫性を検査するため、'l2traceroute'コマンドを入力します。
動的に学習されたソース MAC アドレスとデータパスに対するデスティネーション MAC アドレスを入力します。
拡張コマンドの中から、IP,SIP,DIP,TCP,Scr Port,Dest Port コマンドを使います。
Traceroute パケットが特定の ECMP リンクを通過するように IP コマンドパラメータを入力します。
'l2traceroute'コマンドを使用する上での詳細は、330 ページの『25.5.1 Layer 2 traceroute』を参照下さい。

(3) オプティカルラインのノイズをチェック
オプティカルラインの過度のノイズは、CRC エラー、NIC 相互接続性エラーやその他状況により結果としてパケット破棄となります。

1．'show interface'コマンドを入力して、CRC エラーや TX 破棄をチェックします。次の例の Errors フィールドや Discards フィールドをチェックします。

```
switch# show interface tengigabitethernet 66/0/55
TenGigabitEthernet 66/0/55 is up, line protocol is up (connected)
Hardware is Ethernet, address is 0005.3367.26d3
 Current address is 0005.3367.26d3
Pluggable media present
Interface index (ifindex) is 283874100484
MTU 2500 bytes
LineSpeed Actual   : 10000 Mbit
LineSpeed Configured : Auto, Duplex: Full
Flowcontrol rx: off, tx: off
Last clearing of show interface counters: 21:51:35
Queueing strategy: fifo
Receive Statistics:
  15433457505 packets, 32164575799774 bytes
  Unicasts: 15433454934, Multicasts: 2571, Broadcasts: 0
  64-byte pkts: 11357, Over 64-byte pkts: 242664576, Over 127-byte pkts: 0
  Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
  Over 1518-byte pkts(Jumbo): 15190781568
  Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
  Errors: 0, Discards: 0
Transmit Statistics:
  21456965161 packets, 32549136821934 bytes
  Unicasts: 15313174675, Multicasts: 6143790486, Broadcasts: 0
  Underruns: 0
  Errors: 0, Discards: 0
Rate info (interval 299 seconds):
  Input 3345.136864 Mbits/sec, 200572 packets/sec, 33.45% of line-rate
  Output 3386.493904 Mbits/sec, 281345 packets/sec, 33.86% of line-rate
Time since last interface status change: 1d00h24m
```

2．もし先の手順でエラーが報告されていれば、SFP トランシーバーやケーブルをチェックします。
   a．各スイッチ上で'show media interface'コマンドを入力し、オプティックスが Brocade 製か確認するため Vender Name フィールドをチェックします。
   非 Brocade 製 SFP トランシーバは交換します。
   b．SFP トランシーバを交換してみます
   c．ケーブルを交換してみます。

25.4.8　Ping 失敗

もし、Ping が正常にスイッチを通らない場合、次の操作を試してください。

1．パケットの流れをトレースして、ARP か ICMP パケットが破棄されるかどうかをチェックします
2．インタフェースの統計情報を使って何れの方向が失敗するかトレースします。
3．パケットを破棄しているデバイスを探します。
4．デバイス上でどのエラーカウンタが増加するかを調査します。
5．MAC アドレスが正しいポート/port-channel で学習されるかどうかを判断するため MAC アドレステーブルをチェックします。

25.4.9　tail drops の原因となる QoS 設定

Tail-drop キューイングは輻輳制御の最も基本的な形です。全てのバッファーが尽きるまで、普通の動作は FIFO です。その後、新たなフレームが破棄されます。'qos rcv-queue multicast threshold'コマンドを使って CoS 優先度の閾値を設定することにより、このような破棄の影響を低減することが出来ます。『20 QoS の設定』を参照下さい。

25.4.10 QoS は正しくパケットをマーキング・取り扱わない

QoS がパケットを正しくマーキングして取り扱うかをチェックするため、入出力ポートをミラーする Switched Port Analyzer (SPAN)機能を使います。『22 スイッチドポートアナライザ(SPAN)設定』を参照してください。

25.4.11 RBridge ID の重複

同じ RBridge ID を持つスイッチは、同一 VCS ファブリッククラスタ内に共存できません。存在するクラスタスイッチとして同じ RBridge ID を持つスイッチに対する試みは全て失敗します。２つのスイッチ間の ISL は、形成されませんし、セグメントされます。

1．新しいスイッチ上で、RBridge ID を決定するために、'show vcs'コマンドを入力します。

```
switch2# show vcs
Config Mode : Local-Only
VCS Mode       : Fabric Cluster
VCS ID         : 1
Total Number of Nodes           : 1
Rbridge-Id  WWN                           Management IP   VCS Status       Fabric
Status        HostName
-------------------------------------------------------------------------------
------------------------------
66          >10:00:00:05:33:A4:ED:F3*  192.168.0.76    Online           Online
switch
```

2．動作している VCS ファブリッククラスタ内のどのスイッチ上でも、クラスタ内の全ての RBridge

ID を参照するため、'show vcs'コマンドを入力します。

```
switch1# show vcs
Config Mode : Local-Only
VCS Mode       : Fabric Cluster
VCS ID         : 1
Total Number of Nodes           : 2
Rbridge-Id   WWN                           Management IP   VCS Status       Fabric
Status        HostName
-------------------------------------------------------------------------------
------------------------------
60           >10:00:00:05:33:FF:CA:BC*  192.168.0.78    Online           Online
switch1
66            10:00:00:05:33:A4:E3:33   192.168.0.77    Online           Online
switch2
```

3．もし新しいスイッチがクラスタ内に存在するいずれかのスイッチと同じ RBridge ID を持っていれば、特権実行モードにて、RBridge ID をユニークな値に変更するため、'vcs rbridge-id'コマンドを入力します。

```
switch2# vcs rbridge-id 77
```

25.4.12 SNMP MIB の不正値報告

もし、SNMP MIB が不正な値を報告した場合は、次の手順を実行してください。

1．サポートされた MIB ブラウザを使っているかを確認します。
2．問題は一貫して発生しているか確認します。
3．SNMP 設定が正しいか確認します。
4．もし、MIB ブラウザがサポートされたものであり、SNMP 設定が正しく、一貫して問題が発生しているならば、サポート窓口や保守員に連絡してください。

25.4.13 SNMP trap 通知の失敗

もし SNMP trap 通知が失敗するなら、次の手順を実行してください。

1．正しい SNMP 設定が行われているか確認します。『8 SNMP 管理』を参照してください。
2．SNMP ホストがリーチャブルか確認します。
3．もし問題が依然として継続するなら、サポート窓口や保守員に連絡してください。

Workaround として、syslog メッセージに対して trap 設定をしてください。

25.4.14 スイッチへの telnet 失敗

正しい IP アドレスと正しいログイン情報を想定しても、telnet を使ったスイッチへのアクセス失敗は次の理由のいずれかのためです。

- 管理インタフェースへのアクセスが ACL で拒否されている。325 ページの『25.4.14 (1) 拒否 ACL の確認』を参照してください。
- スイッチ CPU が過負荷である。326 ページの『25.4.14 (2) CPU 過負荷の確認』を参照してください。

(1) 拒否 ACL の確認

システムコンソール上で、'show running-config ip access-list'コマンドを入力して、ACL が管理ポートのアクセスを拒否していないかを判断するため、出力を確認してください。

(2) CPU 過負荷の確認

スイッチ CPU の過負荷は、telnet アクセスを阻害します。313 ページの『25.4.2 不意の CPU 利用率高騰』を参照してください。

25.4.15 Trunk メンバ未使用

もし、trunk メンバポートが使用されていないと疑われるなら、次の手順を実行してください。

1．どのインタフェースでトランキングが有効になっているかを判断するため、'show running-config interface'コマンドを入力します。

```
switch# show running-config interface
interface Vlan 1
!
interface Management 66/0
 no tcp burstrate
 ip icmp unreachable
 ip icmp echo-reply
 no ip address dhcp
 ip address 192.168.0.77/24
 ipv6 icmpv6 unreachable
 ipv6 icmpv6 echo-reply
 no ipv6 address autoconfig
 no ipv6 address dhcp
!
interface TenGigabitEthernet 66/0/1
 fabric isl enable
 fabric trunk enable
 no shutdown
!
interface TenGigabitEthernet 66/0/2
 fabric isl enable
 fabric trunk enable
 no shutdown
!
interface TenGigabitEthernet 66/0/3
 fabric isl enable
 fabric trunk enable
 no shutdown
!
```

- (出力省略)

2．ISL ポートとリンクの状態を検証します。

ａ．ISL がアップしているかどうか検証するため、'show fabric isl'コマンドを入力します。

ｂ．各ポートの状態を検査するため、'show fabric islports'コマンドを入力します。

詳細と修正のため操作は、315 ページの『25.4.5 (1)ISL ステータスの確認』を参照してください。

3．それぞれのトランクリンクに対して、'show interface'コマンドを入力し、トランクのインタフェースのトラフィックが均一に分配されているかをチェックするため、レート情報を精査します。

```
switch# show interface tengigabitethernet 66/0/12
TenGigabitEthernet 66/0/12 is up, line protocol is down (link protocol down)
Hardware is Ethernet, address is 0005.3367.26a8
  Current address is 0005.3367.26a8
Pluggable media not present
Interface index (ifindex) is 283871281409
MTU 2500 bytes
LineSpeed Actual   : Nil
LineSpeed Configured : Auto, Duplex: Full
Flowcontrol rx: off, tx: off
```

```
Last clearing of show interface counters: 1d00h42m
Queueing strategy: fifo
Receive Statistics:
  0 packets, 0 bytes
  Unicasts: 0, Multicasts: 0, Broadcasts: 0
  64-byte pkts: 0, Over 64-byte pkts: 0, Over 127-byte pkts: 0
  Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
  Over 1518-byte pkts(Jumbo): 0
  Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
  Errors: 0, Discards: 0
Transmit Statistics:
  0 packets, 0 bytes
  Unicasts: 0, Multicasts: 0, Broadcasts: 0
  Underruns: 0
  Errors: 0, Discards: 0
Rate info (interval 299 seconds):
  Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 1d03h16m
```

4. 他のトランクメンバはビジーであるのにトラフィックが発生していないトランクメンバが見られる場合、同じ'show interface'コマンドの出力から、インタフェースの状態、設定、エラー統計情報などをチェックします。
   もし、インタフェースが無効化されていたら、'no shutdown'コマンドで有効化します
   もし、設定ミスがあるなら、ファブリックトランクの設定方法については、『9 ファブリック管理』を参照してください。
   もし、エラー統計情報に極端なエラーが見られるならば、エラーによっては、SFP トランシーバやケーブルをチェックしてください。
   a. 'show media interface'コマンドを各スイッチ上で入力して、Brocade 製のモジュールかを確認するため Vender Name をチェックしてください。
      非 Brocade 製 SFP トランシーバは交換してください。
   b. SFP トランシーバを交換してみます。
   c. ケーブルを交換してみます。

25.4.16 アップデート失敗

ファームウェアのアップデート中に問題が発生したら、次の手順を実行します。

1. 以前のファームウェアバージョンに戻します。
2. アップデートを再試行することが適切かどうかを確認するため、サポート窓口や保守員に連絡してください。

25.4.17 VCS ファブリックが形成されない

VCS ファブリックがいくつかの理由で形成に失敗することがあります。

- 必要なライセンスが有効化されてない。328 ページの『25.4.17 (1) VCS Fabric licenses の確認』を参照下さい。
- VCS ファブリック設定が正しくない。次の構成上の問題は VCS ファブリックの形成を阻害します。
  - VCS ファブリックモードが有効になってない。
  - 構成するスイッチの VCS ID が一致してない。
  - スイッチに接続している ISL ポートがアップしてない。

  328 ページの『25.4.17 (2) VCS ファブリック設定の確認』を参照してください。

(1) VCS Fabric licenses の確認

もし、VCS ファブリッククラスタが１台ないしは２台のスイッチから構成されるならば、VCS Fabric license は必要ありません。Network OS v3.0.0 以前の場合、VCS ファブリッククラスタに３台以上のスイッチが存在する場合、VCS Fabric license をインストールしなければなりません。

1．必要な VCS Fabric license がインストールされているかどうかをチェックするため、'show license'コマンドを入力します。

```
switch# show license
rbridge-id: 66
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
       FCoE Base license
       Feature name:FCOE_BASE
       License is valid
```

2．'show license'コマンドの出力に VCS Fabric license が表示されない場合、ライセンスを有効化するため'license add licstr'コマンドを入力します。

```
switch# license add licstr "*B
r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANFav5W:gWx3hH2:9RsMv3BHfeC
RFM2gj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#"

Adding license [*B
r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvvl3Strvw1:fUjANFav5W:gWx3hH2:9RsMv3BHfeC
RFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#]
```

3．ライセンスが追加されたか確認するため、'show license'コマンドを入力します。

NOTE

VCS Fabric license を有効化するため、スイッチをリブートする必要はありません。

```
switch# show license
Rbridge-Id: 66
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
       FCoE Base license
       Feature name:FCOE_BASE
       License is valid
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
       VCS Fabric license
       Feature name:VCS_FABRIC
       License is valid
```

ライセンス管理の更に詳細情報については、99 ページの『7 ライセンスの管理』を参照下さい。

(2) VCS ファブリック設定の確認

VCS ファブリック設定を確認するために、次の手順を実行してください。

1．VCS ファブリックモードが有効か、各スイッチの VCS ID が一致しているか、RBridge ID が異なっているかを確認するため、各スイッチ上で'show vcs'コマンドを入力する。

2．ISL がアップしているかどうかを確認するため、'show fabric isl'コマンドを実行する。

3．各ﾎﾟｰﾄの状態を精査するため、'show fabric islports'コマンドを実行する。

詳細と修正のための操作については、315 ページの『25.4.5 ISL が動作しない』を参照下さい。

25.4.18 vLAG が形成されない

vLAG トランクが幾つかの理由で形成に失敗することがあります。

- VCS ファブリックスイッチ間のリンクが存在しない。329 ページの『25.4.18 (1) VCS ファブリックスイッチ間の接続確認』を参照下さい。

- LACPDU の異常な送受信による接続不良。329 ページの『25.4.18 (2) LACPDU を確認する』を参照下さい。
- VCS ファブリックスイッチ上で port-channel 番号の不一致。329 ページの『25.4.18 (3) vLAG 設定の確認』を参照下さい。
- スイッチ間で異なる LACP モード(static/dynamic)。330 ページの『25.4.18 (4) 各スイッチの LACP モードの確認』を参照下さい。
- 1G port-channel 時の設定漏れ。330 ページの『25.4.18 (5) 1G port-channel の明示的なスピード設定』を参照下さい。

(1) VCS ファブリックスイッチ間の接続確認

スイッチ間の接続が様々な理由のため切断されていることがあります。

- ポートが有効化されてない。
- ISL トランクがセグメントされている。
- VCS ファブリックが正しく形成されていない。
- CPU 過負荷

問題の検出と修正に関する詳細は、315 ページの『25.4.5 ISL が動作しない』を参照下さい。

(2) LACPDU を確認する

LACPDU は vLAG の両端で送受信されなければなりません。この手順では、問題が発生したか、及び PDU のエラーかどうかをチェックする方法を示します。

1．両スイッチ上で、LACPDU を送受信しているか、エラーPDU は無いかを確認するため、'show lacp counter'コマンドを入力します。

```
switch# show lacp counter 10
% Traffic statistics
Port       LACPDUs          Marker            Pckt err
          Sent    Recv     Sent    Recv     Sent    Recv
% Aggregator  Po 10 1000000
Te0/1      65       0        0        0        0        0
Te0/2      64       0        0        0        0        0
Te0/3      64       0        0        0        0        0
Te0/4      0        0        0        0        0        0
```

このケースでは、LACPDU はスイッチにより送信されているが、受信されていません。

2．コマンド出力結果から LACPDU が正しく送受信されていない、または、パケットエラーを示している場合、サポート窓口か保守員に連絡下さい。

(3) vLAG 設定の確認

port-channel 番号は、全ての vLAG メンバスイッチに渡って一致しなければなりません。そうでなければ、vLAG は形成されません。

1．各 vLAG メンバスイッチ上で、特権実行モードにおいて、'show port-channel'コマンドを入力します。

```
switch# show port-channel summary
Static Aggregator: Po 15
Aggregator type: Standard
Member ports on rbridge-id 60
   Te 60/0/1
   Te 60/0/2
   Te 60/0/3
   Te 60/0/4
```

2．Port-channel が両スイッチ上に表示されない場合、表示されないスイッチ上で、グローバルコンフィグレーションモードにて、port-channel を生成するために'interface port-channel'コマンドを入力します。

```
switch2(config)# interface port-channel 15
```

詳細は、『16 リンクアグリゲーションの設定』を参照下さい。

(4) 各スイッチの LACP モードの確認

vLAG は vLAG の両端のスイッチ上で静的または動的に設定されなければなりません。詳細は、『16 リンクアグリゲーションの設定』を参照下さい。

(5) 1G port-channel の明示的なスピード設定

Network OS では、1Gbps のポートスピードの vLAG は、ポートスピードをコンフィグで明示的に指定しなければ形成されません。デフォルトのポートスピードは、10Gbps です。1Gbps のポートスピードをもつ LAG 及び vLAG は、次のマイグレーション手順で形成されます。

1Gbps のポートスピードを設定するために、次の手順を実行してください。

1．インタフェースコンフィグレーションモードにて、port-channel を shutdown します。

```
switch(config-Port-channel-2)# shutdown
```

2．port-channel スピードを 1Gbps に設定します。

```
switch(config-Port-channel-2)# speed 1000
```

3．port-channel で、全てのメンバを再有効化します。

```
switch(config-Port-channel-2)# no shutdown
```

25.5　トラブルシューティングと診断ツール

この章では、Network OS 3.0 以降で使用できる様々なトラブルシューティングと診断ツールについての解説と、それらを使用する場合のガイドラインを示します。

- 330 ページの『25.5.1 Layer 2 traceroute』
- 336 ページの『25.5.2 show コマンド』
- 338 ページの『25.5.3 Debug コマンド』
- 338 ページの『25.5.4 SPAN ポート及びトラフィックミラーリング』
- 339 ページの『25.5.5 ハードウェア診断』
- 339 ページの『'show fabric route pathinfo'コマンドによる経路情報の参照』

また、300 ページの『25.2 問題解決情報の収集』を参照下さい。そこでは、Network OS の supportsave についての情報を提供しています。

25.5.1　Layer 2 traceroute

TRILL OAM はファブリックパスの一貫性を検証するため、'l2traceroute'コマンドを提供しています。'l2traceroute'コマンドを拡張オプション付で使用すると、レイヤ 2traceroute パケットが通過するレイヤ 2 パス上で細やかな制御が可能となります。

(1) レイヤ 2 traceroute パケット

レイヤ 2traceroute ツールを使用するために、リクエストフレームかレスポンスフレームかワイヤ上で

観測できるレイヤ 2traceroute パケットの構造を理解する必要があります。
図 25-1 は、通常のレイヤ 2 パケットがレイヤ 2traceroute を適用しない状態でイーサネットファブリックを通過する時どのように見えるかを示しています。

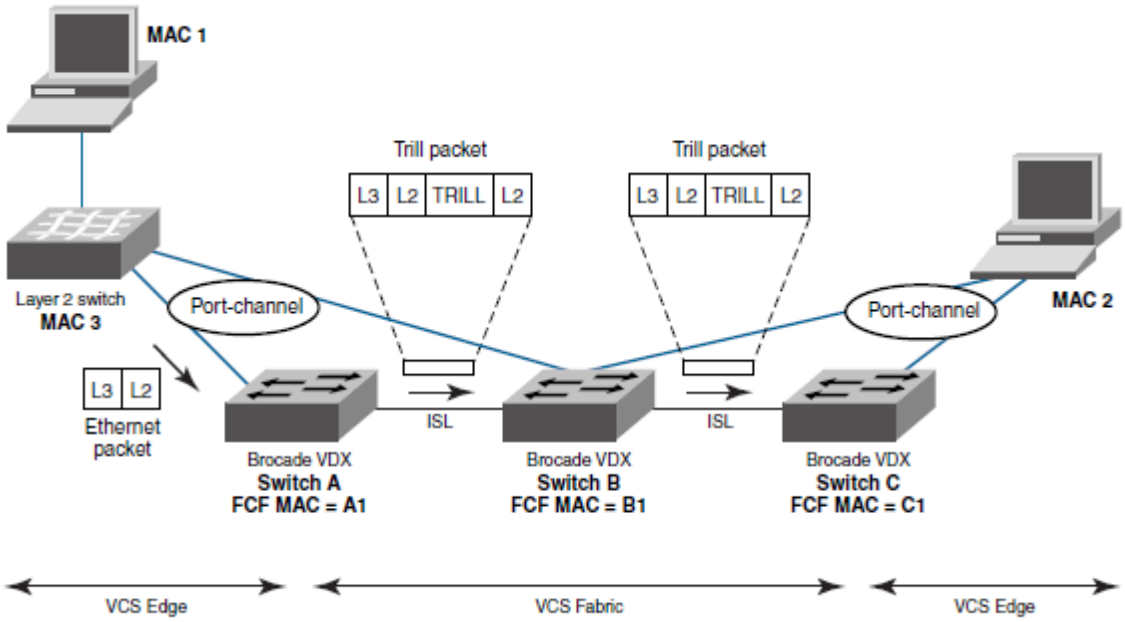

図 25-1　VCS ファブリックを通過する通常のレイヤ 2 パケット

図 25-1 では、イーサネットパケットが MAC1 から VCS ファブリックのエッジに到達しています。TRILL ヘッダの情報は、VCS ファブリックを通過する際に追加されます。TRILL 情報は VCS ファブリックを抜ける時に削除され、通常のイーサネットパケットが MAC2 に到着します。表 25-3 は、レイヤ 2 パケットヘッダの詳細を示しています。

表 25-3　VCS ファブリックを通過するレイヤ 2 パケットのヘッダ詳細

イーサネットパケット	TRILL パケットー最初のホップ	TRILL パケットー２番目のポップ
L2 DA = MAC 2	Outer L2 DA = B1	Outer L2 DA = C1
L2 SA = MAC 1	Outer L2 SA = A1	Outer L2 SA = B1
	Outer 802.1q tag	Outer 802.1q tag
	Outer etype = TRILL	Outer etype = TRILL
	TRILL destination RBridge ID = C	TRILL destination RBridge ID = C
	TRILL source RBridge ID = A	TRILL source RBridge ID = A
	TRILL flags	TRILL flags
	Inner L2 DA = MAC 2	Inner L2 DA = MAC 2
	Inner L2 SA = MAC 1	Inner L2 SA = MAC 1
	Inner 802.1q tag	Inner 802.1q tag
	Inner etype = 0x800	Inner etype = 0x800

'l2traceroute'コマンドを使ってパケットを見るとき、それらが VCS ファブリックを通過する際パケットに付加された TRILL OAM ヘッダ情報が見られます。Switch A 上でトレースを開始すると、TRILL OAM は、隣接スイッチ、この場合は Switch B、とのパスの一貫性を最初に確認します。これは、図 25-2 に示すとおり、TRILL 属性の time-to-live (TTL)を"1"に設定したレイヤ 2traceroute リクエストパケットを送信することで行われます。Switch B は next hop を読み出した到達可能情報と共にレスポンスを返します。

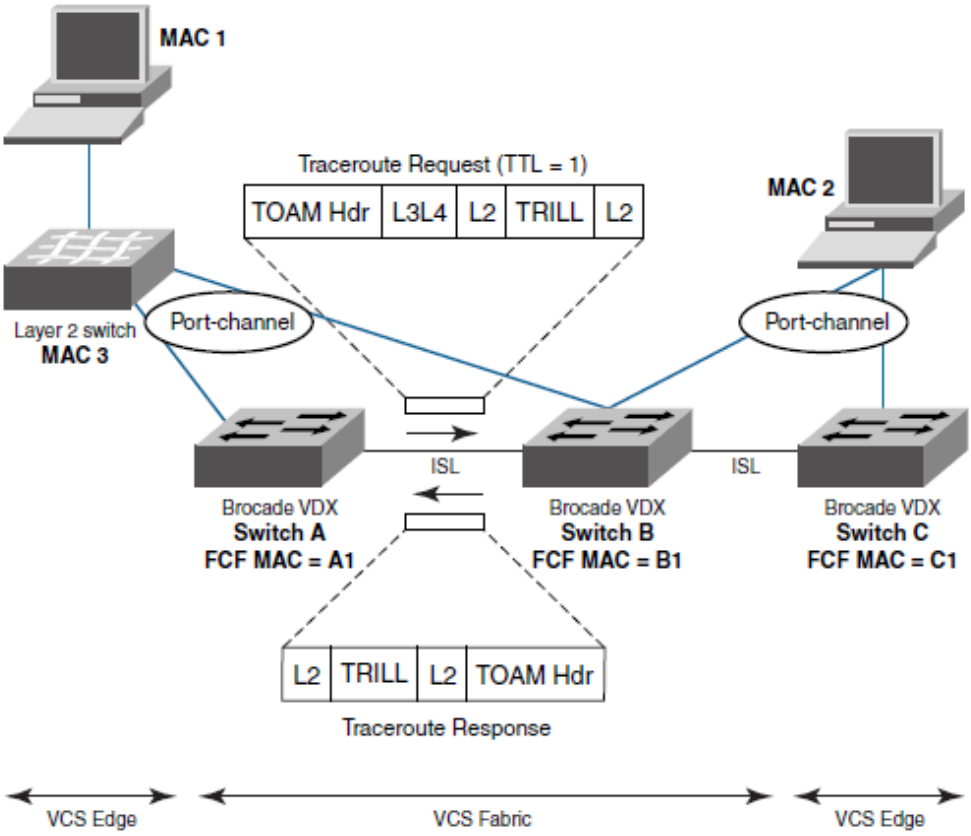

図 25-2　隣接スイッチとのパス一貫性の検証

表 25-4 は、リクエスト及びレスポンスのパケットヘッダ情報を示します。追加された TRILL OAM 情報は、太字で示されます。

表 25-4　レイヤ 2traceroute の第一ホップのパケットヘッダ詳細

traceroute 要求パケットのヘッダー	traceroute 応答パケットのヘッダー
Outer L2 DA = B1	Outer L2 DA = B1
Outer L2 SA = A1	Outer L2 SA = A1
Outer 802.1q tag	Outer 802.1q tag
Outer etype = TRILL	Outer etype = TRILL
TRILL destination RBridge ID = C	TRILL destination RBridge ID = A
TRILL source RBridge ID = A	TRILL source RBridge ID = B
TRILL flags: TTL = 1	TRILL flags: TTL = MAX (63)
Inner L2 DA = MAC 2	Inner L2 DA = A1
Inner L2 SA = MAC 1	Inner L2 SA = B1
Inner 802.1q tag	Inner 802.1q tag
Inner etype = 0x800	Inner etype = TRILL OAM
TOAM Opcode = 5 (request)	TOAM Opcode = 4 (reply)
	C reachable

隣接スイッチ(Switch B)と継続的にパケットが交換されることと Switch C への到達性を確立することは、レイヤ 2traceroute 機能が TTL を"2"に設定することで別のリクエストを作り出します。
Switch B は、TTL カウントを減じて Switch C にパケットを転送します。そして、Swith A にレスポンスを返します。図 25-3 を参照してください。

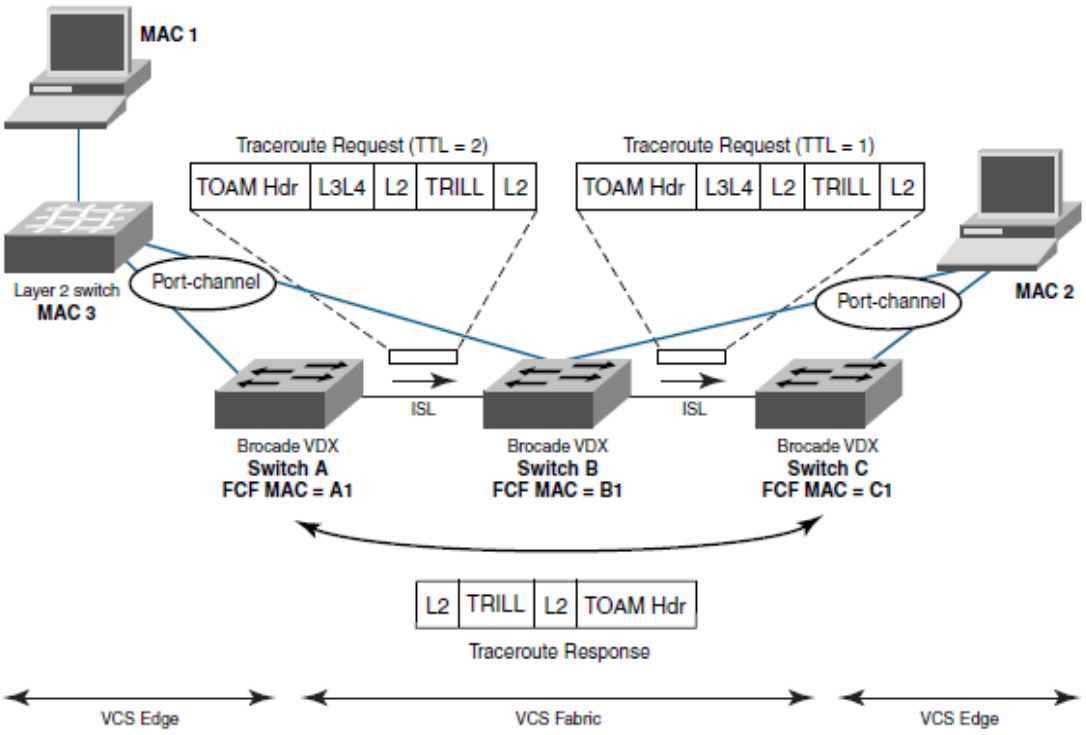

図 25-3　第２ホップへのパス一貫性の検証

表 25-5 は、リクエストとレスポンスのパケットヘッダ情報を示します。レイヤ 2traceroute 機能固有の情報は、太字で示されます。

表 25-5　レイヤ 2traceroute の第２ホップへのパケットヘッダ詳細

Traceroute 要求ー最初のホップ (TTL = 2)	Traceroute 要求ー２番目のホップ (TTL = 1)	Traceroute 応答
Outer L2 DA = B1	Outer L2 DA = C1	Outer L2 DA = B1->A1
Outer L2 SA = A1	Outer L2 SA = B1	Outer L2 SA = C1->B1
Outer 802.1q tag	Outer 802.1q tag	Outer 802.1q tag
Outer etype = TRILL	Outer etype = TRILL	Outer etype = TRILL
TRILL destination RBridge ID = C	TRILL destination RBridge ID = C	TRILL destination RBridge ID = A
TRILL source RBridge ID = A	TRILL source RBridge ID = A	TRILL source RBridge ID = C
TRILL flags: TTL = 2	TRILL flags: TTL = 1	TRILL flags: TTL = MAX (63)
Inner L2 DA = MAC 2	Inner L2 DA = MAC 2	Inner L2 DA = A1
Inner L2 SA = MAC 1	Inner L2 SA = MAC 1	Inner L2 SA = B1
Inner 802.1q tag	Inner 802.1q tag	Inner 802.1q tag
Inner etype = 0x800	Inner etype = 0x800	Inner etype = TRILL OAM
TOAM Opcode = 5 (request)	TOAM Opcode = 5 (request)	TOAM Opcode = 4 (reply)

(2) l2traceroute コマンドを使ったトレース情報

次の例では、'l2traceroute'コマンドがポート 3/0/1(ソース MAC: 0050.5685.0003)とポート 2/0/9(ソース MAC: 0024.3878.3720)の間のパスを検証しています。

1．ネットワーク上の全ての MAC アドレスを表示するため、'show mac-address-table'コマンドを入力します。

```
switch# show mac-address-table
VlanId  Mac-address    Type   State   Ports
100   0024.3878.e720  Dynamic Active  Po 11
100   0050.5685.0001  Dynamic Active  Po 1
101   0000.0000.0003  Dynamic Active  Po 1
101   0024.3878.e720  Dynamic Active  Po 11
101   0050.5685.0003  Dynamic Active  Po 1
Total MAC addresses  : 5
```

出力結果から、ソースとデスティネーション MAC アドレスを選択します。

・Source MAC: 0050.5685.0003

・Destination MAC: 0024.3878.e720

2．'l2traceroute'コマンドを入力します

```
switch2# l2traceroute
Source mac address            : 0050.5685.0003
Destination mac address       : 0024.3878.e720
Vlan [1-3962]                 : 101
Edge rbridge-id [1-239]       : 3
Extended commands [Y/N]?      : y
Protocol Type [IP]            : IP
Source IP address             : 101.101.101.10
Destination IP address        : 101.101.101.101
IP Protocol Type [TCP/UDP]    : TCP
Source port number [0-65535]  : 3000
Dest port number [0-65535]    : 22
Rbridge  Ingress                  Egress                    Rtt(usec)
-------------------------------------------------------------------------------
3        Te 3/0/1(std-lag, Po 1)  Te 3/0/20(isl) 0
2        Te 2/0/20(isl)           Te 2/0/9(std-lag, Po 11)  34041
```

以下の点をご承知おきください。

・MAC アドレスは MAC address-table に存在しなければならない(dynamic or static)

・'l2traceroute'コマンドは VCS ファブリックモードでのみ使用可能

・パス選択に影響する"IP"パラメータを使用してください

25.5.2　show コマンド

表 25-6 は、トラブルシュートでしばしば使用される'show'コマンドをリストしています。全ての'show'コマンドの詳細については、『Network OS Command Reference』を参照して下さい。

表 25-6　トラブルシュートに使われる show コマンド

コマンドグループ	コマンド	特定のフィールドまたは目的
システムコマンド	show system	
	show license	
	show running-config	
	show startup-config	
	show logging raslog	
	show version	
	show chassis	
	show environment	
	show vlan brief	
	show mac-address-table	
	show process cpu	
	show process memory	
	show firmwaredownloadstatus	
インタフェースコマンド	show interface	
	show media	
	show ip int brief	
	show qos flowcontrol interface	ポーズフレームをチェックします。
	show qos queue interface	CoS 統計情報をチェックします。
	show qos rcv-queue interface	パケットドロップ、バッファ消費、リアルタイムのキュー統計をチェックします。
	show qos int	インタフェース上での QoS 設定をチェックします。
診断コマンド	show diags status	
	show diags post results detailed	
	show diag burninerrshow	
	show diag burninstatus	
機能コマンド	show port-channel detail	
	show lacp counter	
	show port-profile status	
	show lldp neighbors detail	
	show lldp statistics	
	show qos interface all	

VCS ファブリック コマンド	show vcs	
	show fabric trunk all	
	show fabric all	
	show fabric isl	
	show fabric islports	
	show fabric route linkinfo	
	show fabric route multicast	
	show fabric route neighbor-state	
	show fabric route pathinfo	
	show fabric route topology	
	show name-server detail	

25.5.3 Debug コマンド

デバッグ機能に関連した次の操作を実行することが出来ます。

- デバッグ機能を有効にするため、'debug'コマンドを使います。

```
debug <feature> <required-keywords>
```

- デバッグ機能が有効かどうかを確認するため、'show debug'コマンドを使います。

```
show debug <feature>
```

- デバッグ機能を無効化するため、'no debug'コマンドを使います。

```
no debug <feature> <required-keywords>
```

リアルタイムデバッギングは CPU に負担を掛けますので、運用環境でのリアルタイムデデバッグする際は注意を払ってください。まず、テスト機でデバッグ出力をチェックして、結果が許容できるならば実運用環境で更にデータ収集するためデバッグ機能を有効化してください。加えて、CPU 負荷を軽減するために、「詳細」や「全て」といった包括的なオプションより、デバッグ機能の範囲を限定する特定イベントや「要約」のようなオプションを使用することを推奨します。

デバッグ機能の操作は、主に LACP や LLDP のようなコントロールプレーンをデバッグするために使います。例えば、コンソールで LLDP パケットの受信を確認するために、次のコマンドを使用します。

```
switch# debug lldp packet all rx
```

スイッチが telnet でアクセスされているなら、ターミナルモニタを有効化します。次の例は、最もよく使われる'debug'コマンドの例です。

- ・debug lldp packet interface [rx | tx | both]
- ・debug lacp pdu [rx | tx] all
- ・debug spanning-tree bpdu [rx | tx] all – スタンドアロンモードのみ
- ・debug dot1x packet all – スタンドアロンモードのみ

25.5.4 SPAN ポート及びトラフィックミラーリング

あるインスタンスにおいて、特定ポートのトラフィックパターンを理解するためにリンクを通過するパケットを調査する必要があるかもしれません。このような状況では、アナライザを接続したミラーポートに特定のイーサネットポートのトラフィックをコピーするため、Switched Port Analyzer (SPAN)を設定することが出来ます。アナライザによりキャプチャされたパケットを分析することが可能になります。

```
switch(config)# monitor session 1
switch(config-mon-sess-1)# source tengigabitethernet 1/0/10 destination
tengigabitethernet 1/0/15 direction both
switch(config-session-1)# end
switch# show monitor 1
Session :1
Description : [None]
State :Enabled
Source interface : 1/0/10 (Up)
Destination interface : 1/0/15 (Up)
Direction :Both
```

デスティネーションポートを、ISL,レイヤ 2, レイヤ 3, QoS, ACL, 802.1x, LAG メンバ, LLDP, port-profile ポートにすることは出来ません。ソースポートを ISL ポートにすることはできません。VCS ファブリックモードでは、エッジポートだけがミラーリング可能です。

25.5.5　ハードウェア診断

現状、次の診断タイプがあります。

- Power-on self-test (POST)

(1) POST 診断

POST はブート時に実行され、結果は格納されます。格納された結果を参照するために、'show diag post results'コマンドを使います。

POST を有効にするために、'diag post [rbridge-id] [rbridge-id] enable'コマンドを使います。

25.5.6　'show fabric route pathinfo'コマンドによる経路情報の参照

'show fabric route pathinfo'コマンドは、ローカルスイッチ上のソースポートインデックスから、VCS ファブリッククラスタや、異なる VCS ファブリッククラスタや、接続された Fabric OS の backbone fabric や、エッジファブリックにある別のスイッチ上のデスティネーションポートインデックスまでの経路を情報を表示します。この経路情報は、全てのファブリック内のスイッチを含むこれらのポート間を通過するデータストリームのフルパス情報を示しています。

経路及び統計情報は、現在のルーティングテーブル情報とリアルタイムに継続的に集計される統計情報に基づき、パスに沿った全てのスイッチによって提供されます。各スイッチは、1 hop を表します。

'show fabric route pathinfo'コマンドをリモートファブリックに跨り使用するためには、リモートスイッチの VCS ID(または Fabric ID)と RBridge ID(ドメイン ID)の両方を指定しなければなりません。リモートファブリックにまたがってパス情報を入手する時、デスティネーションスイッチは RBridge ID またはドメイン ID により特定されます。名称や WWN によりスイッチを特定することは、受け付けられません。

'show fabric route pathinfo'コマンドの詳細は、『Network OS Command Reference』を参照してください。

26 サポートされているタイムゾーンと地域

Network Time Protocol(NTP)によってサポートされているタイムゾーンと地域を次の表に示します。

- アフリカ(Africa)－340 ページの表 26-1 に示します。
- アメリカ(America)－342 ページの表 26-2 に示します。
- 南極大陸(Antarctica)－344 ページの表 26-3 に示します。
- 北極(Arctic)－344 ページの表 26-4 に示します。
- アジア(Asia)－344 ページの表 26-5 に示します。
- 大西洋(Atlantic)－346 ページの表 26-6 に示します。
- オーストラリア(Australia)－346 ページの表 26-7 に示します。
- ヨーロッパ(Europe)－346 ページの表 26-8 に示します。
- インド(Indian)－348 ページの表 26-9 に示します。
- 太平洋(Pacific)－348 ページの表 26-10 に示します。

26.1 アフリカ(Africa)

表 26-1 アフリカの地域/都市タイムゾーン

Africa/Ouagadougou	Africa/Conakry	Africa/Sao_Tome
Africa/Bujumbura	Africa/Malabo	Africa/Mbabane
Africa/Porto-Novo	Africa/Bissau	Africa/Ndjamena
Africa/Gaborone	Africa/Nairobi	Africa/Lome
Africa/Kinshasa	Africa/Monrovia	Africa/Tunis
Africa/Lubumbashi	Africa/Maseru	Africa/Dar_es_Salaam
Africa/Bangui	Africa/Tripoli	Africa/Kampala
Africa/Brazzaville	Africa/Casablanca	Africa/Johannesburg
Africa/Abidjan	Africa/Bamako	Africa/Lusaka
Africa/Douala	Africa/Nouakchott	Africa/Harare
Africa/Djibouti	Africa/Blantyre	
Africa/Algiers	Africa/Maputo	
Africa/Cairo	Africa/Windhoek	
Africa/El_Aaiun	Africa/Niamey	
Africa/Asmara	Africa/Lagos	
Africa/Ceuta	Africa/Kigali	
Africa/Addis_Ababa	Africa/Khartoum	
Africa/Libreville	Africa/Freetown	
Africa/Accra	Africa/Dakar	

26.2　アメリカ(America)

表 26-2　アメリカの地域/都市タイムゾーン

America/Antigua	America/Guatemala	America/Edmonton
America/Anguilla	America/Guyana	America/Cambridge_Bay
America/Curacao	America/Tegucigalpa	America/Yellowknife
America/Argentina/Buenos_Aires	America/Port-au-Prince	America/Inuvik
America/Argentina/Cordoba	America/Guadeloupe	America/Dawson_Creek
America/Argentina/San_Luis	America/Jamaica	America/Vancouver
America/Argentina/Jujuy	America/St_Kitts	America/Whitehorse
America/Argentina/Tucuman	America/Cayman	America/Thunder_Bay
America/Argentina/Catamarca	America/St_Lucia	America/Iqaluit
America/Argentina/La_Rioja	America/Marigot	America/Pangnirtung
America/Argentina/San_Juan	America/Adak	America/Resolute
America/Argentina/Mendoza	America/Martinique	America/Rankin_Inlet
America/Argentina/Rio_Gallegos	America/Montserrat	America/Winnipeg
America/Argentina/Ushuaia	America/Mexico_City	America/Rainy_River
America/Aruba	America/Cancun	America/Regina
America/Barbados	America/Merida	America/Montevideo
America/St_Barthelemy	America/Monterrey	America/St_Vincent
America/La_Paz	America/Mazatlan	America/Caracas
America/Noronha	America/Chihuahua	America/Tortola
America/Belem	America/Hermosillo	America/St_Thomas
America/Fortaleza	America/Tijuana	America/New_York
America/Recife	America/Managua	America/Detroit
America/Araguaina	America/Panama	America/Kentucky/Monticello
America/Maceio	America/Lima	America/Indiana/Indianapolis
America/Bahia	America/Miquelon	America/Indiana/Vincennes
America/Sao_Paulo	America/Puerto_Rico	America/Indiana/Knox
America/Campo_Grande	America/Asuncion	America/Indiana/Winamac
America/Cuiaba	America/Paramaribo	America/Indiana/Marengo
America/Santarem	America/El_Salvador	America/Indiana/Vevay
America/Porto_Velho	America/Grand_Turk	America/Chicago
America/Boa_Vista	America/Swift_Current	America/Indiana/Tell_City
America/Manaus	America/Dawson	America/Indiana/Petersburg
America/Eirunepe	America/Santiago	America/Menominee
America/Rio_Branco	America/Bogota	America/North_Dakota/Center
America/Nassau	America/Costa_Rica	America/North_Dakota/New_Salem

America/Belize	America/Havana	America/Denver
America/St_Johns	America/Dominica	America/Boise
America/Halifax	America/Santo_Domingo	America/Shiprock
America/Glace_Bay	America/Guayaquil	America/Phoenix
America/Moncton	America/Grenada	America/Los_Angeles
America/Goose_Bay	America/Cayenne	America/Anchorage
America/Blanc-Sablon	America/Godthab	America/Juneau
America/Montreal	America/Danmarkshavn	America/Yakutat
America/Toronto	America/Scoresbysund	America/Nome
America/Nipigon	America/Thule	America/Port_of_Spain

26.3　南極大陸(Antarctica)

表 26-3　南極大陸の地域/都市タイムゾーン

Antarctica/McMurdo	Antarctica/Mawson	Antarctica/Vostok
Antarctica/South_Pole	Antarctica/Davis	Antarctica/DumontDUrville
Antarctica/Rothera	Antarctica/Casey	Antarctica/Syowa

26.4　北極(Arctic)

表 26-4　北極の地域/都市タイムゾーン

Arctic/Longyearbyen

26.5　アジア(Asia)

表 26-5　アジアの地域/都市タイムゾーン

Asia/Dubai	Asia/Tokyo	Asia/Gaza
Asia/Kabul	Asia/Bishkek	Asia/Qatar
Asia/Yerevan	Asia/Phnom_Penh	Asia/Yekaterinburg
Asia/Baku	Asia/Pyongyang	Asia/Omsk
Asia/Dhaka	Asia/Seoul	Asia/Novosibirsk
Asia/Bahrain	Asia/Kuwait	Asia/Krasnoyarsk
Asia/Brunei	Asia/Almaty	Asia/Irkutsk
Asia/Thimphu	Asia/Qyzylorda	Asia/Yakutsk
Asia/Shanghai	Asia/Aqtobe	Asia/Vladivostok
Asia/Harbin	Asia/Aqtau	Asia/Sakhalin
Asia/Chongqing	Asia/Oral	Asia/Magadan
Asia/Urumqi	Asia/Vientiane	Asia/Kamchatka
Asia/Kashgar	Asia/Beirut	Asia/Anadyr
Asia/Nicosia	Asia/Colombo	Asia/Riyadh
Asia/Tbilisi	Asia/Rangoon	Asia/Singapore
Asia/Hong_Kong	Asia/Ulaanbaatar	Asia/Damascus
Asia/Jakarta	Asia/Hovd	Asia/Bangkok
Asia/Pontianak	Asia/Choibalsan	Asia/Dushanbe
Asia/Makassar	Asia/Macau	Asia/Dili
Asia/Jayapura	Asia/Kuala_Lumpur	Asia/Ashgabat
Asia/Jerusalem	Asia/Kuching	Asia/Taipei

Asia/Kolkata	Asia/Katmandu	Asia/Samarkand
Asia/Baghdad	Asia/Muscat	Asia/Tashkent
Asia/Tehran	Asia/Manila	Asia/Ho_Chi_Minh
Asia/Amman	Asia/Karachi	Asia/Aden

26.6　大西洋(Atlantic)

表 26-6　大西洋の地域/都市タイムゾーン

Atlantic/Bermuda	Atlantic/Faroe	Atlantic/Azores
Atlantic/Cape_Verde	Atlantic/South_Georgia	Atlantic/St_Helena
Atlantic/Canary	Atlantic/Reykjavik	
Atlantic/Stanley	Atlantic/Madeira	

26.7　オーストラリア(Australia)

表 26-7　オーストラリアの地域/都市タイムゾーン

Australia/Lord_Howe	Australia/Sydney	Australia/Darwin
Australia/Hobart	Australia/Brisbane	Australia/Perth
Australia/Currie	Australia/Lindeman	Australia/Eucla
Australia/Melbourne	Australia/Adelaide	

26.8　ヨーロッパ(Europe)

表 26-8　ヨーロッパの地域/都市タイムゾーン

Europe/Andorra	Europe/Gibraltar	Europe/Warsaw
Europe/Tirane	Europe/Athens	Europe/Lisbon
Europe/Vienna	Europe/Zagreb	Europe/Bucharest
Europe/Mariehamn	Europe/Budapest	Europe/Belgrade
Europe/Sarajevo	Europe/Dublin	Europe/Kaliningrad
Europe/Brussels	Europe/Isle_of_Man	Europe/Moscow
Europe/Sofia	Europe/Rome	Europe/Volgograd
Europe/Minsk	Europe/Jersey	Europe/Samara
Europe/Zurich	Europe/Vaduz	Europe/Stockholm
Europe/Prague	Europe/Vilnius	Europe/Ljubljana
Europe/Berlin	Europe/Luxembourg	Europe/Bratislava
Europe/Copenhagen	Europe/Riga	Europe/San_Marino
Europe/Tallinn	Europe/Monaco	Europe/Istanbul
Europe/Madrid	Europe/Chisinau	Europe/Kiev
Europe/Helsinki	Europe/Podgorica	Europe/Uzhgorod
Europe/Paris	Europe/Skopje	Europe/Zaporozhye
Europe/London	Europe/Malta	Europe/Simferopol

Europe/Guernsey	Europe/Amsterdam	Europe/Vatican
Europe/Oslo		

26.9　インド(Indian)

表 26-9　インドの地域/都市タイムゾーン

Indian/Cocos	Indian/Antananarivo	Indian/Mahe
Indian/Christmas	Indian/Mauritius	Indian/Kerguelen
Indian/Chagos	Indian/Maldives	Indian/Mayotte
Indian/Comoro	Indian/Reunion	

26.10　太平洋(Pacific)

表 26-10　太平洋の地域/都市タイムゾーン

Pacific/Pago_Pago	Pacific/Kwajalein	Pacific/Palau
Pacific/Rarotonga	Pacific/Saipan	Pacific/Guadalcanal
Pacific/Easter	Pacific/Noumea	Pacific/Fakaofo
Pacific/Galapagos	Pacific/Norfolk	Pacific/Tongatapu
Pacific/Fiji	Pacific/Nauru	Pacific/Funafuti
Pacific/Truk	Pacific/Niue	Pacific/Johnston
Pacific/Ponape	Pacific/Auckland	Pacific/Midway
Pacific/Kosrae	Pacific/Chatham	Pacific/Wake
Pacific/Guam	Pacific/Tahiti	Pacific/Honolulu
Pacific/Tarawa	Pacific/Marquesas	Pacific/Efate
Pacific/Enderbury	Pacific/Gambier	Pacific/Wallis
Pacific/Kiritimati	Pacific/Port_Moresby	Pacific/Apia
Pacific/Majuro	Pacific/Pitcairn	