レイヤ 2/3 コンフィギュレーション ガイド、Cisco IOS XE リリース 3.6E（Catalyst 3850 スイッチ）

初版：2014 年 06 月 27 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Text Part Number: OL-32601-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

© 2014 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xi

表記法 xi

関連資料 xiii

マニュアルの入手方法およびテクニカル サポート xiii

スパニングツリー プロトコルの設定 1

機能情報の確認 1

STP の制約事項 1

スパニング ツリー プロトコルに関する情報 2

スパニングツリー プロトコル 2

スパニングツリー トポロジと BPDU 3

ブリッジ ID、デバイス プライオリティ、および拡張システム ID 5

ポート プライオリティとパス コスト 6

スパニングツリー インターフェイス ステート 7

ブロッキング ステート 9

リスニング ステート 9

ラーニング ステート 9

フォワーディング ステート 10

ディセーブル ステート 10

Switch またはポートがルート Switchまたはルート ポートになる仕組み 10

スパニングツリーおよび冗長接続 11

スパニングツリー アドレスの管理 12

接続を維持するためのエージング タイムの短縮 12

スパニングツリー モードおよびプロトコル 13

サポートされるスパニングツリー インスタンス 14

スパニングツリーの相互運用性と下位互換性 14

STP および IEEE 802.1Q トランク 15

VLAN ブリッジ スパニングツリー 15
スパニング ツリーとSwitch スタック 15
スパニングツリー機能のデフォルト設定 16
スパニングツリー機能の設定方法 17
スパニングツリー モードの変更 17
スパニング ツリーのディセーブル化 19
ルート Switchの設定 20
セカンダリ ルート デバイスの設定 22
ポート プライオリティの設定 23
パス コストの設定 25
VLAN のデバイス プライオリティの設定 26
hello タイムの設定 28
VLAN の転送遅延時間の設定 28
VLAN の最大エージング タイムの設定 30
転送保留カウントの設定 31
スパニングツリー ステータスのモニタリング 32
スパニング ツリー プロトコルに関する追加情報 32
STP の機能情報 33
複数のスパニング ツリー プロトコルの設定 35
機能情報の確認 35
MSTP の前提条件 35
MSTP の制約事項 36
MSTP について 37
MSTP の設定 37
MSTP 設定時の注意事項 38
ルート スイッチ 39
MST リージョン 40
IST、CIST、CST 40
MST リージョン内の動作 41
MST リージョン間の動作 42
IEEE 802.1s の用語 42
MST リージョンの図 43

ホップ カウント 44
境界ポート 45
IEEE 802.1s の実装 46
ポートの役割名の変更 46
レガシーおよび規格Switchesの相互運用 46
単一方向リンク障害の検出 47
MSTP およびSwitch スタック 48
IEEE 802.1D STP との相互運用性 48
RSTP 概要 48
ポートの役割およびアクティブ トポロジー 49
高速コンバージェンス 50
ポート ロールの同期 51
ブリッジ プロトコル データ ユニットの形式および処理 52
優位 BPDU 情報の処理 53
下位 BPDU 情報の処理 53
トポロジの変更 54
プロトコル移行プロセス 54
MSTP のデフォルト設定 55
MSTP 機能の設定方法 56
MST リージョン設定の指定と MSTP のイネーブル化 56
ルート Switchの設定 59
セカンダリ ルートの設定Switch 60
ポート プライオリティの設定 62
パス コストの設定 64
Switch プライオリティの設定 65
hello タイムの設定 67
転送遅延時間の設定 68
最大エージング タイムの設定 70
最大ホップ カウントの設定 71
高速移行を確実にするためのリンク タイプの指定 72
ネイバー タイプの設定 73
プロトコルの移行プロセスの再開 75

MST の設定およびステータスのモニタリング 76
MSTP に関する追加情報 77
MSTP の機能情報 78
オプションのスパニングツリー機能の設定 79
機能情報の確認 79
オプションのスパニング ツリー機能の制約事項 79
オプションのスパニングツリー機能について 80
PortFast 80
BPDU ガード 81
BPDU フィルタリング 81
UplinkFast 82
クロススタック UplinkFast 84
クロススタック UplinkFast の動作 84
高速コンバージェンスを発生させるイベント 86
BackboneFast 87
EtherChannel ガード 89
ルート ガード 90
ループ ガード 91
オプションのスパニングツリー機能の設定方法 91
PortFast のイネーブル化 91
BPDU ガードのイネーブル化 93
BPDU フィルタリングのイネーブル化 95
冗長リンクで使用するための UplinkFast のイネーブル化 97
UplinkFast のディセーブル化 98
BackboneFast をイネーブル化 99
EtherChannel ガードのイネーブル化 101
ルート ガードのイネーブル化 102
ループ ガードのイネーブル化 103
スパニングツリー ステータスのモニタリング 105
オプションのスパニング ツリー機能に関する追加情報 106
オプションのスパニングツリー機能の機能情報 107
EtherChannel の設定 109
機能情報の確認 109

EtherChannel の制約事項 109
EtherChannel について 110
EtherChannel の概要 110
EtherChannel のモード 111
Switches上の EtherChannel 112
EtherChannel リンクのフェールオーバー 114
チャネル グループおよびポートチャネル インターフェイス 114
ポート集約プロトコル 116
PAgP モード 116
サイレント モード 118
PAgP 学習方式およびプライオリティ 118
PAgP と他の機能との相互作用 119
Link Aggregation Control Protocol 120
LACP モード 120
LACP とリンクの冗長性 121
LACP と他の機能との相互作用 121
EtherChannel の On モード 122
ロードバランシングおよび転送方式 122
MAC アドレス転送 122
IP アドレス転送 123
ロードバランシングの利点 124
EtherChannel およびSwitch スタック 125
Switch スタックおよび PAgP 126
Switch スタックおよび LACP 126
EtherChannel のデフォルト設定 126
EtherChannel 設定時の注意事項 128
レイヤ 2 EtherChannel 設定時の注意事項 129
レイヤ 3 EtherChannel 設定時の注意事項 130
EtherChannel の設定方法 131
レイヤ 2 EtherChannel の設定 131
レイヤ 3 EtherChannel の設定 134
EtherChannel ロードバランシングの設定 136

EtherChannel 拡張ロードバランシングの設定 138
PAgP 学習方式およびプライオリティの設定 139
LACP ホット スタンバイ ポートの設定 140
LACP 最大バンドル機能の設定 141
ポート チャネル最小リンク機能の設定 142
LACP システム プライオリティの設定 143
LACP ポート プライオリティの設定 145
EtherChannel、PAgP、および LACP ステータスのモニタ 146
EtherChannel の設定例 147
レイヤ 2 EtherChannel の設定：例 147
レイヤ 3 EtherChannel の設定：例 148
LACP ホット スタンバイ ポートの設定：例 149
EtherChannels の追加リファレンス 149
EtherChannels の機能情報 150
Flex Link および MAC アドレス テーブル移動更新機能の設定 153
機能情報の確認 153
Flex Link および MAC アドレス テーブル移動更新設定の制約事項 154
Flex Link および MAC アドレス テーブル移動更新に関する情報 155
Flex Link 155
Flex Link の設定 155
VLAN Flex Link ロード バランシングおよびサポート 156
Flex Link フェールオーバーによるマルチキャスト高速コンバージェンス 157
その他の Flex Link ポートを mrouter ポートとして学習 157
IGMP レポートの生成 158
IGMP レポートのリーク 158
MAC アドレス テーブル移動更新 159
Flex Link の VLAN ロード バランシング設定時の注意事項 162
MAC アドレス テーブル移動更新設定時の注意事項 162
デフォルトの Flex Link および MAC アドレス テーブル移動更新の設定 162
Flex Link および MAC アドレス テーブル移動更新機能の設定方法 163
Flex Link の設定 163
Flex Link ペアのプリエンプション方式の設定 164

Flex Link の VLAN ロード バランシングの設定 166
MAC アドレス テーブル移動更新の設定 167
MAC アドレス テーブル移動更新メッセージの取得および処理用のSwitch設定 169
Flex Link、マルチキャスト高速コンバージェンス、および MAC アドレス テーブル移動更新のモニタ 170
Flex Link の設定例 171
Flex Link の設定：例 171
Flex Link における VLAN ロード バランシングの設定：例 171
MAC アドレス テーブル移動更新の設定：例 173
Flex Link フェールオーバーによるマルチキャスト高速コンバージェンスの設定: 例 173
Flex Link および MAC アドレス テーブル移動更新の追加リファレンス 176
Flex Link および MAC アドレス テーブル移動更新の機能情報 177
単方向リンク検出の設定 179
機能情報の確認 179
UDLD 設定の制約事項 179
UDLD について 180
動作モード 180
通常モード 180
アグレッシブ モード 181
単一方向の検出方法 181
ネイバー データベース メンテナンス 182
イベントドリブン検出およびエコー 182
UDLD リセット オプション 182
UDLD のデフォルト設定 183
UDLD の設定方法 184
UDLD のグローバルなイネーブル化 184
インターフェイスでの UDLD のイネーブル化 185
UDLD のモニタおよびメンテナンス 187
UDLD の追加リファレンス 187
UDLD の機能情報 188

はじめに

- 表記法，xi ページ
- 関連資料，xiii ページ
- マニュアルの入手方法およびテクニカル サポート，xiii ページ

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。たとえば、**^D** または **Ctrl+D** というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します （ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。
bold フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字**フォントで示しています。
Italic フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*italic* フォントで示しています。
`courier` フォント	システムが表示するターミナル セッションおよび情報は、`courier` フォントで示しています。
`太字の courier` フォント	太字の **`courier`** フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。

表記法	説明
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x | y]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

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

ヒント 「問題解決に役立つ情報」です。

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

ワンポイント アドバイス　時間を節約する方法です。 ここに紹介している方法で作業を行うと、時間を短縮できます。

警告　IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

関連資料

（注）　switchをインストールまたはアップグレードする前に、switchのリリース ノートを参照してください。

- 次の URL にある Cisco Catalyst 3850 スイッチ のマニュアル：
  http://www.cisco.com/go/cat3850_docs
- 次の URL にある Cisco SFP および SFP+ モジュールのマニュアル（互換性マトリクスを含む）：
  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html
- 次の URL にある Cisco Validated Design（CVD）のマニュアル：
  http://www.cisco.com/go/designzone
- 次の URL にあるエラー メッセージ デコーダ：
  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

マニュアルの入手方法およびテクニカル サポート

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

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定するこ

ともできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

スパニングツリー プロトコルの設定

- 機能情報の確認，1 ページ
- STP の制約事項，1 ページ
- スパニング ツリー プロトコルに関する情報，2 ページ
- スパニングツリー機能の設定方法，17 ページ
- スパニングツリー ステータスのモニタリング，32 ページ
- スパニング ツリー プロトコルに関する追加情報，32 ページ
- STP の機能情報，33 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

STP の制約事項

- ルート switchとしてswitchを設定しようとする場合、ルート switchにするために必要な値が 1 未満だと、失敗します。
- ネットワークが、拡張システム ID をサポートするswitchesとサポートしないものの両方で構成されている場合、拡張システム ID をサポートするswitchがルート switchになる可能性は低

くなります。 古いソフトウェアを実行している接続switchesのプライオリティより VLAN 番号が大きい場合は常に、拡張システム ID によってswitch プライオリティ値が増加します。

- 各スパニングツリー インスタンスのルート switchは、バックボーンまたはディストリビューション switchでなければなりません。 アクセス switchをスパニングツリー プライマリ ルートとして設定しないでください。
- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

関連トピック

ルート Switchの設定, （20 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID, （5 ページ）
スパニングツリー トポロジと BPDU, （3 ページ）
接続を維持するためのエージング タイムの短縮, （12 ページ）

スパニング ツリー プロトコルに関する情報

スパニングツリー プロトコル

スパニングツリー プロトコル（STP）は、ネットワーク内のループを回避しながらパスを冗長化するためのレイヤ 2 リンク管理プロトコルです。 レイヤ 2 イーサネット ネットワークが正常に動作するには、任意の 2 つのステーション間で存在できるアクティブ パスは 1 つだけです。 エンド ステーション間に複数のアクティブパスがあると、ネットワークにループが生じます。 このループがネットワークに発生すると、エンド ステーションにメッセージが重複して到着する可能性があります。 Switchesは、複数のレイヤ 2 インターフェイスのエンド ステーション MAC アドレスを学習する可能性もあります。 このような状況によって、ネットワークが不安定になります。 スパニングツリーの動作は透過的であり、エンド ステーション側で、単一 LAN セグメントに接続されているのか、複数セグメントからなるスイッチドLANに接続されているのかを検出することはできません。

STP は、スパニングツリー アルゴリズムを使用し、スパニングツリーのルートとして冗長接続ネットワーク内のswitchを 1 つ選択します。 アルゴリズムは、次に基づき、各ポートにロールを割り当て、スイッチド レイヤ 2 ネットワークを介して最良のループフリー パスを算出します。 アクティブ トポロジでのポートの役割：

- ルート：スパニングツリー トポロジに対して選定される転送ポート
- 指定：各スイッチド LAN セグメントに対して選定される転送ポート
- 代替：スパニングツリーのルート ブリッジへの代替パスとなるブロック ポート
- バックアップ：ループバック コンフィギュレーションのブロック ポート

すべてのポートに役割が指定されているswitch、またはバックアップの役割が指定されているスイッチはルート switchです。 少なくとも *1* つのポートに役割が指定されているswitchは、指定switchを意味します。

冗長データ パスはスパニングツリーによって、強制的にスタンバイ（ブロックされた）ステートにされます。 スパニングツリーのネットワーク セグメントでエラーが発生したときに冗長パスが存在する場合は、スパニングツリーアルゴリズムがスパニングツリー トポロジを再計算し、スタンバイ パスをアクティブにします。 Switchesは、スパニングツリー フレーム （ブリッジ プロトコル データ ユニット（BPDU）と呼ばれる）を定期間隔で送受信します。 switchesはこのフレームを転送しませんが、このフレームを使用してループフリー パスを構築します。 BPDU には、switchおよび MAC アドレス、switchの優先順位、ポートの優先順位、およびパス コストを含む、送信側switchとそのポートに関する情報が含まれます。 スパニングツリーはこの情報を使用して、スイッチド ネットワーク用のルート switchおよびルート ポートを選定し、さらに、各スイッチド セグメントのルート ポートおよび指定ポートを選定します。

switchの 2 つのポートがループの一部である場合、 スパニングツリー および、パス コスト設定は、どのポートがフォワーディング ステートになるか、およびどのポートがブロッキング ステートになるかを制御します。 スパニングツリー ポート プライオリティ値は、ネットワーク トポロジにおけるポートの位置とともに、トラフィック転送におけるポートの位置がどれだけ適切であるかを表します。 The パス コスト値は、メディア速度を表します。

（注） デフォルトではswitchは、Small Form-Factor Pluggable（SFP）モジュールを備えていないインターフェイスにだけ、（接続が稼働していることを確認するために）キープアライブ メッセージを送信します。 [**no**] **keepalive** インターフェイス コンフィギュレーション コマンドをキーワードなしで入力すると、インターフェイスのデフォルトを変更できます。

スパニングツリー トポロジと BPDU

スイッチド ネットワーク内の安定したアクティブ スパニングツリー トポロジは、次の要素によって制御されます。

- switch上の各 VLAN に関連付けられた一意のブリッジ ID（switch プライオリティおよびMAC アドレス）。 switch スタックでは、ある特定のスパニングツリー インスタンスに対して、すべてのswitchesが同一のブリッジ ID を使用します。
- ルート switchに対するスパニングツリー パス コスト。
- 各レイヤ 2 インターフェイスに対応付けられたポート ID（ポート プライオリティおよびMAC アドレス）。

ネットワーク内のswitchesに電源が入ると、各機能はルート switchとして機能します。 各switchは、そのすべてのポートからコンフィギュレーション BPDU を送信します。 BPDU によって通信が行われ、スパニングツリー トポロジが計算されます。 各設定 BPDUには、次の情報が含まれています。

- 送信switchがルート switch として識別するswitchの一意のブリッジ ID。

- ルートまでのスパニングツリー パス コスト
- 送信switch のブリッジ ID。
- メッセージ エージ
- 送信側インターフェイス ID
- hello タイマー、転送遅延タイマー、および max-age プロトコル タイマーの値

switchは、優位な情報（より小さいブリッジ ID、より低いパス コストなど）が含まれているコンフィギュレーション BPDU を受信すると、そのポートに対する情報を保存します。 この BPDU をswitchのルート ポート上で受信した場合、そのswitchが指定switchとなっているすべての接続 LAN に、更新したメッセージを付けて BPDU を転送します。

switchは、そのポートに現在保存されている情報よりも下位の情報を含むコンフィギュレーション BPDU を受信した場合は、その BPDU を廃棄します。 switchが下位 BPDU を受信した LAN の指定switchである場合、そのポートに保存されている最新情報を含む BPDU をその LAN に送信します。 このようにして下位情報は廃棄され、優位情報がネットワークで伝播されます。

BPDU の交換によって、次の処理が行われます。

- ネットワーク内の 1 つのswitchがとして選択されます。 ルート switch（スイッチドネットワークのスパニングツリー トポロジーの論理的な中心）。 箇条書きの項目の下の図を参照してください。

  VLAN ごとに、switch プライオリティが最も高い（最も小さい数字の優先順位の値）switch がルート switchとして選択されます。 すべてのswitchesがデフォルトのプライオリティ（32768）で設定されている場合、VLAN 内で MAC アドレスの最も小さいswitchがルート switchになります。 switchのプライオリティ値は、次の図のようにブリッジ ID の最上位ビットを占めます。

- switchごとに（ルート switchを除く）、ルート ポートが 1 つ選択されます。 このポートは、switchからルート switchにパケットを転送するときに最適パス（最小コスト）を提供します。

  switch スタックのルート ポートを選択する場合には、スパニング ツリーは次の順序に従います。

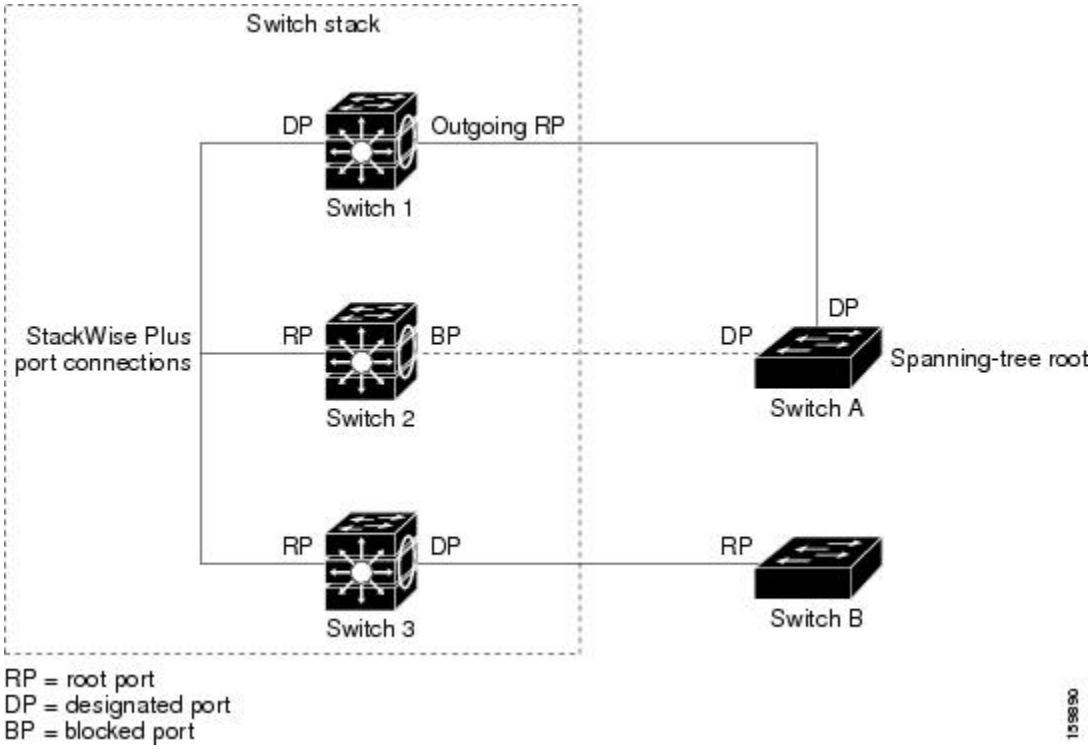
  - 最も低いルート ブリッジ ID を選択
  - ルート switch への最も低いパス コストを選択
  - 最も低い代表ブリッジ ID を選択
  - 最も低い代表パス コストを選択
  - 最も低いポート ID を選択

- スタック ルート switch上の 1 つの発信ポートだけが、ルート ポートとして選択されます。 スタック内の残りのswitchesは、次の図に示すように指定switchesになります（Switch 2 およびSwitch 3）。
- ルート switchへの最短距離は、パス コストに基づいてswitchごとに計算されます。

- LANセグメントごとに指定switchが選択されます。 指定switchは、そのLANからルートswitchにパケットを転送するときの最小パス コストを提供します。 DPは、指定switchがLANに接続されているポートです。

1つのスタック メンバーがスタック ルートswitchとして選択されます。 スタック ルートswitchには出力ルート ポート（Switch1）が含まれます。

図 *1*：*Switch* スタックのスパニング ツリー ポート ステート



スイッチド ネットワーク上のいずれの地点からもルートswitchに到達する場合に必要のないパスはすべて、スパニングツリー ブロッキング モードになります。

関連トピック

ルート Switchの設定，（20 ページ）
STP の制約事項，（1 ページ）

ブリッジ ID、デバイス プライオリティ、および拡張システム ID

IEEE 802.1D 標準では、それぞれのswitchに固有の ルートswitchの選択を制御するブリッジ識別子（ブリッジ ID）が必要です。 各 VLAN は PVST+ と Rapid PVST+ によって異なる論理ブリッジと見なされるので、同一のswitchは設定された各 VLAN とは異なるブリッジ ID を保有している必要があります。 switch上の各 VLAN には一意の 8 バイト ブリッジ ID が設定されます。 上位の 2 バイトはswitch プライオリティに使用され、残りの 6 バイトがswitchの MAC アドレスから取得されます。

switchでは IEEE 802.1t スパニングツリー拡張機能がサポートされ、従来はswitch プライオリティに使用されていたビットの一部がVLAN IDとして使用されるようになりました。 その結果、switchに割り当てられる MAC アドレスが少なくなり、より広い範囲の VLAN ID をサポートできるようになり、しかもブリッジ ID の一意性を損なうこともありません。

従来はswitch プライオリティに使用されていた2バイトが、4ビットのプライオリティ値と12ビットの拡張システム ID 値（VLAN ID と同じ）に割り当てられています。

表 *1*：デバイス プライオリティ値および拡張システム *ID*

プライオリティ値				拡張システム ID（VLAN ID と同設定）										
ビット 16	ビット 15	ビット 14	ビット 13	ビット 12	ビット 11	ビット 10	ビット 9	ビット 8	ビット 7	ビット 6	ビット 5	ビット 4	ビット 3	ビット 2	ビット 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

スパニングツリーは、ブリッジ ID を VLAN ごとに一意にするために、拡張システム ID、switch プライオリティ、および割り当てられたスパニングツリー MAC アドレスを使用します。 switch スタックは他のネットワークからは単一のswitchとして認識されるため、スタック内のすべてのswitchesは、指定のスパニングツリーに対して同一のブリッジ ID を使用します。 スタック マスターに障害が発生した場合、スタック メンバは新しいスタック マスターの新しい MAC アドレスに基づいて、実行中のすべてのスパニングツリーのブリッジ ID を再計算します。

拡張システム ID のサポートにより、ルート switch、セカンダリ ルート switch、および VLAN の switch プライオリティの手動での設定方法に影響が生じます。 たとえば、switchのプライオリティ値を変更すると、switchがルート switchとして選定される可能性も変更されることになります。 大きい値を設定すると可能性が低下し、値が小さいと可能性が増大します。

指定された VLAN のルート switchに 24576 に満たないswitch プライオリティが設定されている場合は、switchはその VLAN について、自身のプライオリティを最小のswitch プライオリティより 4096 だけ小さい値に設定します4096は、表に示すように4ビットswitch スイッチプライオリティ値の最下位ビットの値です。

関連トピック

ルート Switchの設定, （20 ページ）
STP の制約事項, （1 ページ）
ルート Switchの設定, （59 ページ）
ルート スイッチ, （39 ページ）
MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）

ポート プライオリティとパス コスト

ループが発生した場合、スパニングツリーはポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。 最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプラ

イオリティ値（高い数値）を割り当てることができます。 すべてのインターフェイスに同じプライオリティ値が与えられている場合、スパニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

スパニングツリー パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。 ループが発生した場合、スパニングツリーはコストを使用して、フォワーディング ステートにするインターフェイスを選択します。 最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択されるインターフェイスには高いコスト値を割り当てることができます。 すべてのインターフェイスに同じコスト値が与えられている場合、スパニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

switchがswitch スタックのメンバーの場合は、最初に選択させたいインターフェイスには小さいコスト値を与え、最後に選択させたいインターフェイスには（ポート プライオリティを調整せずに）大きいコスト値を与えます。 詳細については、関連項目を参照してください。

関連トピック

ポート プライオリティの設定, （23 ページ）
パス コストの設定, （25 ページ）

スパニングツリー インターフェイス ステート

プロトコル情報がスイッチド LAN を通過するとき、伝播遅延が生じることがあります。 その結果、スイッチドネットワークのさまざまな時点および場所でトポロジーの変化が発生します。 インターフェイスがスパニングツリートポロジに含まれていない状態からフォワーディング ステートに直接移行すると、一時的にデータ ループが形成されることがあります。 インターフェイスは新しいトポロジ情報がスイッチドLAN上で伝播されるまで待機し、フレーム転送を開始する必要があります。 インターフェイスはさらに、古いトポロジで使用されていた転送フレームのフレーム存続時間を満了させることも必要です。

スパニングツリーを使用しているswitchの各レイヤ2インターフェイスは、次のいずれかのステートになります。

- ブロッキング：インターフェイスはフレーム転送に関与しません。
- リスニング：インターフェイスをフレーム転送に関与させることをスパニングツリーが決定した場合、ブロッキング ステートから最初に移行するステートです。
- ラーニング：インターフェイスはフレーム転送に関与する準備をしている状態です。
- フォワーディング：インターフェイスはフレームを転送します。
- ディセーブル：インターフェイスはスパニングツリーに含まれません。シャットダウン ポートであるか、ポート上にリンクがないか、またはポート上でスパニングツリー インスタンスが稼働していないためです。

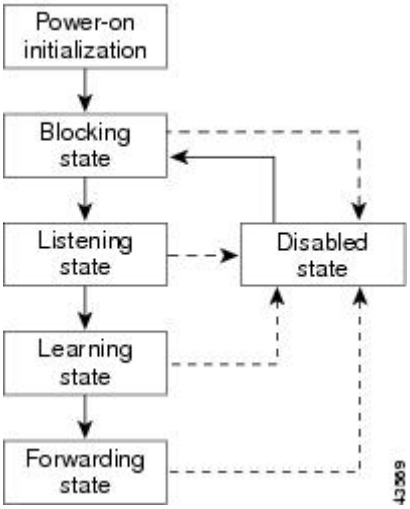
インターフェイスは次のように、ステートを移行します。

- 初期化からブロッキング

- ブロッキングからリスニングまたはディセーブル
- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

インターフェイスはこれらのステート間を移動します。

図 *2*: スパニングツリー インターフェイス ステート



デフォルト設定では、switchを起動するとスパニングツリーがイネーブルになります。その後、switchの各インターフェイス、VLAN、ネットワークがブロッキング ステートからリスニングおよびラーニングという移行ステートを通過します。スパニングツリーは、フォワーディング ステートまたはブロッキング ステートで各インターフェイスを安定させます。

スパニングツリー アルゴリズムがレイヤ 2 インターフェイスをフォワーディング ステートにする場合、次のプロセスが発生します。

1. スパニングツリーがインターフェイスをブロッキング ステートに移行させるプロトコル情報を待つ間、インターフェイスはリスニング ステートになります。
2. スパニングツリーは転送遅延タイマーの満了を待ち、インターフェイスをラーニング ステートに移行させ、転送遅延タイマーをリセットします。
3. ラーニング ステートの間、switchが転送データベースのエンド ステーションの位置情報を学習しているとき、インターフェイスはフレーム転送をブロックし続けます。
4. 転送遅延タイマーが満了すると、スパニングツリーはインターフェイスをフォワーディング ステートに移行させ、このときラーニングとフレーム転送の両方が可能になります。

ブロッキング ステート

ブロッキング ステートのレイヤ 2 インターフェイスはフレームの転送に関与しません。 初期化後、switchの各インターフェイスに BPDU が送信されます。 switchは最初、他のswitchesと BPDU を交換するまで、ルートとして動作します。 この交換により、ネットワーク内でどのswitchがルートまたはルート switchになるかが確立されます。 ネットワーク内にswitchが 1 つしかない場合は交換は行われず、転送遅延タイマーが満了し、インターフェイスがリスニング ステートになります。 インターフェイスはswitchの初期化後、必ずブロッキング ステートになります。

ブロッキング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

リスニング ステート

リスニング ステートは、ブロッキング ステートを経て、レイヤ2インターフェイスが最初に移行するステートです。 インターフェイスがリスニング ステートになるのは、スパニングツリーによってそのインターフェイスのフレーム転送への関与が決定された場合です。

リスニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

ラーニング ステート

ラーニング ステートのレイヤ 2 インターフェイスは、フレームの転送に関与できるように準備します。 インターフェイスはリスニング ステートからラーニング ステートに移行します。

ラーニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習します。
- BPDU を受信します。

フォワーディング ステート

フォワーディング ステートのレイヤ 2 インターフェイスは、フレームを転送します。 インターフェイスはラーニング ステートからフォワーディング ステートに移行します。

フォワーディング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上でフレームを受信して転送します。
- 他のインターフェイスからスイッチングされたフレームを転送します。
- アドレスを学習します。
- BPDU を受信します。

ディセーブル ステート

ブロッキング ステートのレイヤ 2 インターフェイスは、フレームの転送やスパニングツリーに関与しません。 ディセーブル ステートのインターフェイスは動作不能です。

ディセーブル インターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信しません。

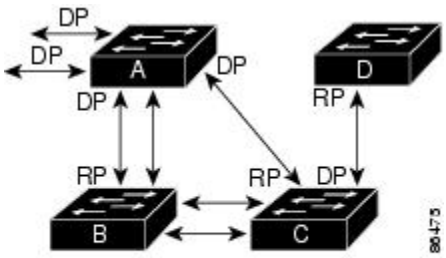
Switch またはポートがルート Switchまたはルート ポートになる仕組み

ネットワーク上のすべてのswitchesがデフォルトのスパニングツリー設定でイネーブルになっている場合、最小の MAC アドレスを持つswitchがルート switchになります。

Switch A はルート switchとして選択されます。すべてのswitchesのswitchのプライオリティがデフォルト（32768）に設定されており、Switch A の MAC アドレスが最も小さいためです。 ただし、トラフィック パターン、転送インターフェイスの数、またはリンク タイプによっては、Switch A が最適なルート switchとは限りません。 ルート switchになるように、最適なswitchのプライオリティ

を引き上げる（数値を引き下げる）と、スパニングツリーの再計算が強制的に行われ、最適なswitchをルートとした新しいトポロジが形成されます。

図 *3*：スパニングツリー トポロジ



RP = Root Port
DP = Designated Port

スパニングツリー トポロジがデフォルトのパラメータに基づいて算出された場合、スイッチドネットワークの送信元エンドステーションから宛先エンドステーションまでのパスが最適にならない場合があります。たとえば、ルートポートよりプライオリティの高いインターフェイスに高速リンクを接続すると、ルートポートが変更される可能性があります。最高速のリンクをルートポートにすることが重要です。

たとえば、Switch B のあるポートがギガビット イーサネット リンクで、Switch上の別のポート（10/100 リンク）がルート ポートであると仮定します。 ネットワーク トラフィックはギガビット イーサネット リンクに流す方が効率的です。 ギガビット イーサネット ポートのスパニングツリー ポート プライオリティをルート ポートより高くする（数値を小さくする）と、ギガビット イーサネット ポートが新しいルート ポートになります。

関連トピック

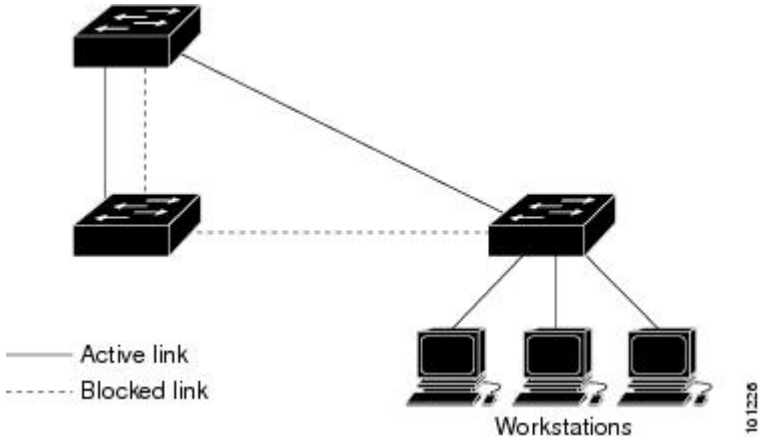
ポート プライオリティの設定, （23 ページ）

スパニングツリーおよび冗長接続

2 つのswitch インターフェイスを別の 1 台のデバイス、または 2 台の異なるデバイスに接続することにより、スパニングツリーを使用して冗長バックボーンを作成できます。 スパニングツリーは一方のインターフェイスを自動的にディセーブルにし、他方でエラーが発生した場合にはそのディセーブルにしていた方をイネーブルにします。 一方のリンクが高速で、他方が低速の場合、必

ず、低速の方のリンクがディセーブルになります。 速度が同じ場合、ポート プライオリティとポートIDが加算され、値の小さいリンクがスパニングツリーによってディセーブルにされます。

図 *4*：スパニングツリーおよび冗長接続



EtherChannel グループを使用して、switches間に冗長リンクを設定することもできます。

スパニングツリー アドレスの管理

IEEE 802.1D では、各種ブリッジ プロトコルに使用させるために、0x00180C2000000 ～ 0x0180C2000010 の範囲で 17 のマルチキャスト アドレスが規定されています。 これらのアドレスは削除できないスタティック アドレスです。

スパニングツリー ステートに関係なく、スタック内の各switchは 0x0180C2000000 ～ 0x0180C2000000 のアドレス宛てのパケットを受信しますが、転送は行いません。

スパニングツリーがイネーブルの場合、switchまたはスタック内の各switchの CPU は 0x0180C2000000 および 0x0180C2000010 宛てのパケットを受信します。 スパニングツリーがディセーブルの場合は、switchまたはスタック内の各switchは、それらのパケットを不明のマルチキャスト アドレスとして転送します。

接続を維持するためのエージング タイムの短縮

ダイナミック アドレスのエージング タイムはデフォルトで 5 分です。これは、**mac-address-table aging-time** グローバル コンフィギュレーション コマンドのデフォルトの設定です。 ただし、スパニングツリーの再構成により、多数のステーションの位置が変更されることがあります。 このようなステーションは、再構成中、5分以上にわたって到達できないことがあるので、アドレステーブルからステーション アドレスを削除し、改めて学習できるように、アドレス エージング タイムが短縮されます。 スパニングツリー再構成時に短縮されるエージングタイムは、転送遅延パラメータ値（**spanning-tree vlan** *vlan-id* **forward-time** *seconds* グローバル コンフィギュレーション コマンド）と同じです。

各 VLAN はそれぞれ独立したスパニングツリー インスタンスであるため、switchは VLAN 単位でエージング タイムを短縮します。 ある VLAN でスパニングツリーの再構成が行われると、その

VLAN で学習されたダイナミック アドレスがエージング タイム短縮の対象になります。 他の VLAN のダイナミック アドレスは影響を受けず、switchで設定されたエージング間隔がそのまま保持されます。

関連トピック

ルート Switchの設定, （20 ページ）
STP の制約事項, （1 ページ）

スパニングツリー モードおよびプロトコル

このswitchでサポートされるモードおよびプロトコルは、次のとおりです。

- PVST+：このスパニングツリー モードは、IEEE 802.1D 標準およびシスコ独自の拡張機能に準拠します。 すべてのイーサネット ポートベースの VLAN で使用されるスパニングツリーのデフォルト モードです。 PVST+ はswitch上の各 VLAN でサポートされる最大数まで動作し、各 VLAN にネットワーク上でのループフリー パスを提供します。

  PVST+ は、対象となる VLAN にレイヤ 2 ロード バランシングを提供します。 ネットワーク上のVLANを使用してさまざまな論理トポロジを作成し、特定のリンクに偏らないようにすべてのリンクを使用できるようにします。 VLAN 上の PVST+ インスタンスごとに、それぞれ 1 つのルート switchがあります。 このルート switchは、その VLAN に対応するスパニングツリー情報を、ネットワーク上の他のすべてのswitchesに伝送します。 このプロセスにより、各switchがネットワークに関する共通の情報を持つため、ネットワーク トポロジが確実に維持されます。

- Rapid PVST+：このスパニングツリー モードは、IEEE 802.1w 標準に準拠した高速コンバージェンスを使用する以外は PVST+ と同じです。 高速コンバージェンスを行うため、Rapid PVST+ はトポロジ変更を受信すると、ポート単位でダイナミックに学習した MAC アドレス エントリをただちに削除します。 このような場合、PVST+ では、ダイナミックに学習した MAC アドレス エントリには短いエージング タイムが使用されます。

  Rapid PVST+ は PVST+ と同じ設定を使用しているので（特に明記する場合を除く）、switch で必要なことは最小限の追加設定のみです。 Rapid PVST+ の利点は、大規模な PVST+ のインストール ベースを Rapid PVST+ に移行する際に、複雑なマルチ スパニングツリー プロトコル（MSTP）設定の学習やネットワーク再設定の必要がないことです。 Rapid PVST+ モードでは、各 VLAN は独自のスパニングツリー インスタンスを最大数実行します。

- MSTP：このスパニングツリー モードは IEEE 802.1s 標準に準拠しています。 複数の VLAN を同一のスパニングツリー インスタンスにマッピングし、多数の VLAN をサポートする場合に必要となるスパニングツリーインスタンスの数を減らすことができます。 MSTP は高速スパニングツリー プロトコル（RSTP）（IEEE 802.1w 準拠）上で実行され、転送遅延を解消し、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行することにより、スパニングツリーの高速コンバージェンスを可能にします。 switch スタックでは、クロススタック高速移行（CSRT）機能が RSTP と同じ機能を実行します。 RSTP も CSRT もなしに MSTP を実行することはできません。

関連トピック

スパニングツリー モードの変更, （17 ページ）

サポートされるスパニングツリー インスタンス

PVST+ または Rapid PVST+ モードでは、switchまたはswitch スタックは最大 128 のスパニングツリー インスタンスをサポートします。

MSTP モードでは、switchまたはswitch スタックは最大 65 の MST インスタンスをサポートします。 特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。

関連トピック

スパニング ツリーのディセーブル化, （19 ページ）
スパニングツリー機能のデフォルト設定, （16 ページ）
MSTP のデフォルト設定, （55 ページ）

スパニングツリーの相互運用性と下位互換性

MSTP および PVST+ が混在したネットワークでは、Common Spanning-Tree（CST）のルートは MST バックボーンの内側に配置する必要があり、PVST+ switchを複数の MST リージョンに接続することはできません。

ネットワーク内に Rapid PVST+ を実行しているswitchesと PVST+ を実行しているswitchesが存在する場合、Rapid PVST+ switchesと PVST+ switchesを別のスパニングツリー インスタンスに設定することを推奨します。 Rapid PVST+ スパニングツリー インスタンスでは、ルート switchは Rapid PVST+ switchでなければなりません。 PVST+ インスタンスでは、ルート switchは PVST+ switchでなければなりません。 PVST+ switchesはネットワークのエッジに配置する必要があります。

すべてのスタック メンバーが、同じバージョンのスパニングツリーを実行します（すべて PVST+、すべて Rapid PVST+、またはすべて MSTP）。

表 *2*：*PVST+*、*MSTP*、*Rapid PVST+* の相互運用性と互換性

	PVST+	MSTP	Rapid PVST+
PVST+	あり	あり（制限あり）	あり（PVST+ に戻る）
MSTP	あり（制限あり）	あり	あり（PVST+ に戻る）
Rapid PVST+	あり（PVST+ に戻る）	あり（PVST+ に戻る）	あり

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）
MSTP 設定時の注意事項, （38 ページ）

MST リージョン，（40 ページ）

STP および IEEE 802.1Q トランク

VLAN トランクに関する IEEE 802.1Q 規格は、ネットワークのスパニングツリー ストラテジに一定の制限を設けています。 この規格では、トランク上で使用できるすべての VLAN に対して、1 つのスパニングツリー インスタンスしか認められません。 ただし、IEEE 802.1Q トランクを介して接続される Cisco switchesのネットワークにおいて、switchesはトランク上で許容される VLAN ごとに 1 つのスパニングツリー インスタンスを維持します。

IEEE 802.1Q トランクを介して Cisco switchを他社製のデバイスに接続する場合、Cisco switchは PVST+ を使用してスパニングツリーの相互運用性を実現します。 Rapid PVST+ がイネーブルの場合、switchは PVST+ ではなく Rapid PVST+ を使用します。 switchは、トランクの IEEE 802.1Q VLAN のスパニングツリー インスタンスと他社の IEEE 802.1Q switchのスパニングツリー インスタンスを結合します。

ただし、PVST+ または Rapid PVST+ の情報はすべて、他社製の IEEE 802.1Q switchesからなるクラウドにより分離された Cisco switchesによって維持されます。 Cisco switchesを分離する他社製の IEEE 802.1Q クラウドは、switches間の単一トランク リンクとして扱われます。

PVST+ は IEEE 802.1Q トランクで自動的にイネーブルになるので、ユーザ側で設定する必要はありません。 アクセス ポートおよびISL（スイッチ間リンク）トランク ポートでの外部スパニングツリーの動作は、PVST+ の影響を受けません。

VLAN ブリッジ スパニングツリー

シスコ VLANブリッジスパニングツリーは、フォールバック ブリッジング機能（ブリッジ グループ）で使用し、DECnet などの IP 以外のプロトコルを 2 つ以上の VLAN ブリッジ ドメインまたはルーテッド ポート間で伝送します。 VLAN ブリッジ スパニングツリーにより、ブリッジ グループは個々の VLAN スパニングツリーの上部にスパニングツリーを形成できるので、VLAN 間で複数の接続がある場合に、ループが形成されないようにします。 また、ブリッジングされている VLAN からの個々のスパニングツリーが単一のスパニングツリーに縮小しないようにする働きもします。

VLANブリッジスパニングツリーをサポートするには、一部のスパニングツリー タイマーを増やします。 フォールバック ブリッジング機能を使用するには、switchでIPサービス フィーチャ セットをイネーブルにする必要があります。

スパニング ツリーとSwitch スタック

switch スタックが PVST+ または Rapid PVST+ モードで動作している場合：

- switch スタックは、ネットワークのその他の部分に対しては単一のスパニングツリー ノードに見え、すべてのスタック メンバーが与えられたスパニングツリーに同一のブリッジ ID を使用します。 ブリッジ ID は、active switchの MAC アドレスから取得されます。
- 新しいswitchがスタックに加わると、そのスイッチは、active switchのブリッジ ID を自分のブリッジ ID として設定します。 新しく追加されたswitchの ID が最も小さく、ルート パス コス

トがすべてのスタック メンバー間で同じ場合は、新しく追加されたswitchがスタック ルートになります。

- スタック メンバがスタックから除外されると、スタック内でスパニングツリーの再コンバージェンスが発生します（スタック外で発生する場合もあります）。 残っているスタック メンバのうち最も低いスタック ポート ID を持つスタック メンバが、スタック ルートになります。
- switch スタックがスパニング ツリー ルートで、active switchで障害が発生した、またはスタックから外れた場合、スタンバイ スイッチが新しいアクティブ スイッチになり、ブリッジ ID は同じままで、スパニング ツリーの再コンバージェンスが発生する可能性があります。
- switch スタック外にあるネイバー switchに障害が発生したか、またはその電源が停止した場合、通常のスパニングツリー処理が発生します。 スパニングツリーの再コンバージェンスは、アクティブなトポロジ内のswitchが失われたことにより発生する場合もあります。
- switch スタック外にある新しい switchがネットワークに追加された場合、通常のスパニングツリー処理が発生します。 スパニングツリーの再コンバージェンスは、ネットワークにswitchが追加されたことにより発生する場合もあります。

スパニングツリー機能のデフォルト設定

表 *3*：スパニングツリー機能のデフォルト設定

機能	デフォルト設定
イネーブル ステート	VLAN 1 上でイネーブル
スパニングツリー モード	PVST+ （Rapid PVST+ と MSTP はディセーブル）
Switch プライオリティ	32768
スパニングツリー ポート プライオリティ（インターフェイス単位で設定可能）	128
スパニングツリー ポート コスト（インターフェイス単位で設定可能）	1000 Mb/s：4 100 Mb/s：19 10 Mb/s：100
スパニングツリーVLANポートプライオリティ（VLAN単位で設定可能）	128

機能	デフォルト設定
スパニングツリーVLANポートコスト（VLAN単位で設定可能）	1000 Mb/s：4 100 Mb/s：19 10 Mb/s：100
スパニングツリー タイマー	hello タイム：2 秒 転送遅延時間：15 秒 最大エージング タイム：20 秒 転送保留カウント：6 BPDU

関連トピック

スパニング ツリーのディセーブル化，（19 ページ）
サポートされるスパニングツリー インスタンス，（14 ページ）

スパニングツリー機能の設定方法

スパニングツリー モードの変更

スイッチは次の 3 つのスパニングツリー モードをサポートします。Per-VLAN Spanning-Tree Plus（PVST+）、Rapid PVST+、またはマルチ スパニングツリー プロトコル（MSTP）。 デフォルトで、switchは PVST+ プロトコルを実行します。

デフォルト モード以外のモードをイネーブルにする場合、この手順は必須です。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree mode** {**pvst** | **mst** | **rapid-pvst**}
4. **interface** *interface-id*
5. **spanning-tree link-type point-to-point**
6. **end**
7. **clear spanning-tree detected-protocols**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mode** {**pvst** | **mst** | **rapid-pvst**} 例： `Switch(config)# spanning-tree mode pvst`	スパニングツリー モードを設定します。 すべてのスタック メンバーは、同じバージョンのスパニング ツリーを実行します。 • **pvst** を指定して、PVST+ をイネーブルにします（デフォルト設定）。 • **mst** を指定して、MSTP（および RSTP）をイネーブルにします。 • **rapid-pvst** を指定して、Rapid PVST+ をイネーブルにします。
ステップ 4	**interface** *interface-id* 例： `Switch(config)# interface GigabitEthernet1/0/1`	（Rapid PVST+ モードの場合のみ推奨）設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスとしては、物理ポート、VLAN、ポート チャネルなどがあります。 VLAN ID の範囲は 1 ～ 4094 です。 ポート チャネル範囲は 1 ～ 48 です。
ステップ 5	**spanning-tree link-type point-to-point** 例： `Switch(config-if)# spanning-tree link-type point-to-point`	（Rapid PVST+ モードの場合のみ推奨）このポートのリンク タイプをポイントツーポイントに指定します。 このポート（ローカル ポート）をポイントツーポイント リンクでリモート ポートと接続し、ローカル ポートが指定ポートになると、switchはリモート ポートとネゴシエーションし、ローカル ポートをフォワーディング ステートにすばやく変更します。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**clear spanning-tree detected-protocols** 例： `Switch# clear spanning-tree detected-protocols`	（Rapid PVST+ モードの場合のみ推奨）switch上の任意のポートがIEEE 802.1D 準拠のレガシー switchのポートと接続されている場合に、このコマンドはswitch全体でプロトコル移行プロセスを再開します。 このステップは、このswitchで Rapid PVST+ が稼働していることを指定switchが検出する場合のオプションです。

関連トピック

スパニングツリー モードおよびプロトコル，（13 ページ）

スパニング ツリーのディセーブル化

スパニングツリーはデフォルトで、VLAN 1 およびスパニングツリー限度を上限として新しく作成されたすべての VLAN 上でイネーブルです。 スパニングツリーをディセーブルにするのは、ネットワーク トポロジにループがないことが確実な場合だけにしてください。

注意 スパニングツリーがディセーブルでありながら、トポロジにループが存在していると、余分なトラフィックが発生し、パケットの重複が無限に繰り返されることによって、ネットワークのパフォーマンスが大幅に低下します。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **no spanning-tree vlan** *vlan-id*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no spanning-tree vlan** *vlan-id* 例： `Switch(config)# no spanning-tree vlan 300`	*vlan-id* に指定できる範囲は 1 ～ 4094 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

サポートされるスパニングツリー インスタンス, （14 ページ）
スパニングツリー機能のデフォルト設定, （16 ページ）

ルート Switchの設定

特定の VLAN でswitchをルートとして設定するには、**spanning-tree vlan** *vlan-id* **root** グローバル コンフィギュレーション コマンドを使用して、switch プライオリティをデフォルト値（32768）から、それより大幅に小さい値に変更します。このコマンドを入力すると、ソフトウェアが各 VLAN について、ルート switchesのswitch プライオリティを確認します。 拡張システム ID をサポートするため、switchは指定された VLAN の自身のプライオリティを 24576 に設定します。この値によって、このswitchを指定された VLAN のルートに設定できます。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間の最大switch ホップ カウント）を指定するには、**diameter** キーワードを指定します。ネットワーク直径を指定すると、switchはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に設定します。その結果、コンバージェンスに要する時間が大幅に短縮されます。 **hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree vlan** *vlan-id* **root primary** [**diameter** *net-diameter*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan** *vlan-id* **root primary** [**diameter** *net-diameter* 例： `Switch(config)# spanning-tree vlan 20-24 root primary diameter 4`	指定された VLAN のルートになるように、switchを設定します。 • *vlan-id* には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 •（任意）**diameter** *net-diameter* には、任意の 2 つのエンドステーション間の最大switches数を指定します。 指定できる範囲は 2 ～ 7 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

次の作業

ルート switchとしてswitchを設定した後で、**spanning-tree vlan** *vlan-id* **hello-time**、**spanning-tree vlan** *vlan-id* **forward-time**、および **spanning-tree vlan** *vlan-id* **max-age** グローバル コンフィギュレーショ

ン コマンドを使用して、hello タイム、転送遅延時間、および最大エージング タイムを手動で設定することは推奨できません。

関連トピック

ブリッジ ID、デバイス プライオリティ、および拡張システム ID, （5 ページ）
スパニングツリー トポロジと BPDU, （3 ページ）
接続を維持するためのエージング タイムの短縮, （12 ページ）
STP の制約事項, （1 ページ）

セカンダリ ルート デバイスの設定

switchをセカンダリ ルートとして設定すると、switch プライオリティがデフォルト値（32768）から 28672 に変更されます。 このプライオリティでは、switchがプライマリ ルート switchが失敗した場合の、指定された VLAN のルートswitchになる可能性があります。 ここでは、その他のネットワーク switchesが、デフォルトのswitch プライオリティの 32768 を使用しているためにルートswitchになる可能性が低いことが前提となっています。

このコマンドを複数のswitchに対して実行すると、複数のバックアップ ルート switchesを設定できます。 **spanning-tree vlan** *vlan-id* **root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート switchを設定したときと同じネットワーク直径およびhello タイム値を使用してください。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree vlan** *vlan-id* **root secondary** [**diameter** *net-diameter*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**spanning-tree vlan** *vlan-id* **root secondary** [**diameter** *net-diameter* 例： `Switch(config)# spanning-tree vlan 20-24 root secondary diameter 4`	指定された VLAN のセカンダリ ルートになるように、switchを設定します。 • *vlan-id* には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 •（任意）**diameter** *net-diameter* には、任意の 2 つのエンドステーション間の最大switches数を指定します。 指定できる範囲は 2 ～ 7 です。 プライマリ ルート switchを設定したときと同じネットワーク直径を使用してください。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

ポート プライオリティの設定

（注） switchがswitch スタックのメンバである場合、**spanning-tree** [**vlan** *vlan-id*] **port-priority** *priority* インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree** [**vlan** *vlan-id*] **cost** *cost* インターフェイス コンフィギュレーション コマンドを使用して、フォワーディング ステートにするインターフェイスを選択する必要があります。 最初に選択させるインターフェイスには、低いコスト値を割り当て、最後に選択させるインターフェイスには高いコスト値を割り当てます。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **spanning-tree port-priority** *priority*
5. **spanning-tree vlan** *vlan-id* **port-priority** *priority*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスは、物理ポートおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）です。
ステップ 4	**spanning-tree port-priority** *priority* 例： `Switch(config-if)# spanning-tree port-priority 0`	インターフェイスのポート プライオリティを設定します。 *priority* に指定できる範囲は 0 ～ 240 で、16 ずつ増加します。デフォルトは 128 です。 有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。 その他の値はすべて拒否されます。 値が小さいほど、プライオリティが高くなります。
ステップ 5	**spanning-tree vlan** *vlan-id* **port-priority** *priority* 例： `Switch(config-if)# spanning-tree vlan 20-25 port-priority 0`	VLAN のポート プライオリティを設定します。 • *vlan-id* には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 • *priority* に指定できる範囲は 0 ～ 240 で、16 ずつ増加します。デフォルトは 128 です。 有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。 その他の値はすべて拒否されます。 値が小さいほど、プライオリティが高くなります。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

ポート プライオリティとパス コスト，（6 ページ）
Switch またはポートがルート Switchまたはルート ポートになる仕組み，（10 ページ）

パス コストの設定

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **spanning-tree cost** *cost*
5. **spanning-tree vlan** *vlan-id* **cost** *cost*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。有効なインターフェイスは、物理ポートおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）です。
ステップ 4	**spanning-tree cost** *cost* 例： `Switch(config-if)# spanning-tree cost 250`	インターフェイスのコストを設定します。 ループが発生した場合、スパニングツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。 低いパス コストは高速送信を表します。

	コマンドまたはアクション	目的
		cost の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 5	**spanning-tree vlan** *vlan-id* **cost** *cost* 例： `Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300`	VLAN のコストを設定します。 ループが発生した場合、スパニングツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。 低いパス コストは高速送信を表します。 • *vlan-id* には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 • *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

show spanning-tree interface *interface-id* 特権 EXEC コマンドで情報が表示されるのは、リンクアップ動作可能の状態にあるポートに限られます。 そうでない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

関連トピック

ポート プライオリティとパス コスト, （6 ページ）

VLAN のデバイス プライオリティの設定

switch プライオリティを設定して、スタンドアロン switchまたはスタックにあるswitchがルートswitchとして選択される可能性を高めることができます。

（注） このコマンドの使用には注意してください。 switchのプライオリティを変更する場合は通常、**spanning-tree vlan** *vlan-id* **root primary** および **spanning-tree vlan** *vlan-id* **root secondary** グローバル コンフィギュレーション コマンドを使用することを推奨します。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree vlan** *vlan-id* **priority** *priority*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan** *vlan-id* **priority** *priority* 例： `Switch(config)# spanning-tree vlan 20 priority 8192`	VLAN のswitch プライオリティの設定 • *vlan-id* には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 • *priority* の範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。 この値が低いほど、switchがルート switch として選択される可能性が高くなります。 有効なプライオリティ値は 4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。 その他の値はすべて拒否されます。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

hello タイムの設定

hello タイムはルート switchによって設定メッセージが生成されて送信される時間の間隔です。

この手順は任意です。

手順の概要

1. **enable**
2. **spanning-tree vlan** *vlan-id* **hello-time** *seconds*
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**spanning-tree vlan** *vlan-id* **hello-time** *seconds* 例： `Switch(config)# spanning-tree vlan 20-24 hello-time 3`	VLAN の hello タイムを設定します。 hello タイムはルート switch によって設定メッセージが生成されて送信される時間の間隔です。このメッセージは、switchが活動中であることを表します。 • *vlan-id* には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 3	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

VLAN の転送遅延時間の設定

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree vlan** *vlan-id* **forward-time** *seconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan** *vlan-id* **forward-time** *seconds* 例： `Switch(config)# spanning-tree vlan 20,25 forward-time 18`	VLAN の転送時間を設定します。 転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、インターフェイスが待機する秒数です。 • *vlan-id* には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 4 ～ 30 です。デフォルトは 15 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

VLAN の最大エージング タイムの設定

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree vlan** *vlan-id* **max-age** *seconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree vlan** *vlan-id* **max-age** *seconds* 例： `Switch(config)# spanning-tree vlan 20 max-age 30`	VLAN の最大エージング タイムを設定します。 最大エージング タイムは、switchが再設定を試す前にスパニングツリー設定メッセージを受信せずに待機する秒数です。 • *vlan-id* には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。 指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

転送保留カウントの設定

転送保留カウント値を変更することで、BPDU のバースト サイズを設定できます。

（注） このパラメータをより高い値に変更すると、（特に Rapid PVST+ モードで）CPU の使用率に大きく影響します。 逆に、この値を低く設定すると、セッションによってはコンバージェンスを抑えることができます。 この値は、デフォルト設定で使用することを推奨します。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree transmit hold-count** *value*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree transmit hold-count** *value* 例： `Switch(config)# spanning-tree transmit hold-count 6`	1 秒間停止する前に送信できる BPDU 数を設定します。 *value* に指定できる範囲は 1 ～ 20 です。デフォルト値は 6 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

スパニングツリー ステータスのモニタリング

表 *4*：スパニングツリー ステータス表示用のコマンド

show spanning-tree active	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree vlan *vlan-id*	指定した VLAN のスパニング ツリー情報を表示します。
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree interface *interface-id* **portfast**	指定したインターフェイスのスパニングツリー portfast 情報を表示します。
show spanning-tree summary [**totals**]	インターフェイス ステートのサマリーを表示します。またはSTP ステートセクションのすべての行を表示します。

スパニングツリー カウンタをクリアするには、**clear spanning-tree** [**interface** *interface-id*] 特権 EXEC コマンドを使用します。

スパニング ツリー プロトコルに関する追加情報

関連資料

関連項目	マニュアル タイトル
スパニング ツリー プロトコル コマンド	*LAN Switching Command Reference, Cisco IOS XE Release 3SE（Catalyst 3850 Switches）*

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

STP の機能情報

リリース	変更内容
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	この機能が導入されました。

第 2 章

複数のスパニングツリープロトコルの設定

- 機能情報の確認，35 ページ
- MSTP の前提条件，35 ページ
- MSTP の制約事項，36 ページ
- MSTP について，37 ページ
- MSTP 機能の設定方法，56 ページ
- MST の設定およびステータスのモニタリング，76 ページ
- MSTP に関する追加情報，77 ページ
- MSTP の機能情報，78 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

MSTP の前提条件

- 2 つ以上のswitchesを同じマルチ スパニングツリー（MST）リージョンに設定するには、その 2 つに同じ VLAN/インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。

- 2 つ以上のスタック スイッチを同じ MST リージョンに設定するには、その複数のスイッチに同じ VLAN/インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定する必要があります。
- ネットワーク内の冗長パスでロード バランシングを機能させるには、すべての VLAN/インスタンスマッピングの割り当てが一致している必要があります。一致していないと、すべてのトラフィックが 1 つのリンク上で伝送されます。 パス コストを手動で設定することで、switch スタック全体にわたりロード バランシングを実現できます。
- Per-VLAN Spanning-Tree Plus（PVST+）と MST クラウドの間、または Rapid- PVST+ と MST クラウドの間でロード バランシングが機能するためには、すべての MST 境界ポートがフォワーディングでなければなりません。 MST クラウドの内部スパニング ツリー（IST）マスターが共通スパニング ツリー（CST）のルートである場合、MST境界ポートはフォワーディングです。 MST クラウドが複数の MST リージョンから構成されている場合、いずれかの MST リージョンに CST ルートを含める必要があり、その他すべての MST リージョンに、PVST+ クラウドまたは高速 PVST+ クラウドを通るパスよりも、MST クラウド内に含まれるルートへのパスが良くする必要があります。 クラウド内のswitchesを手動で設定しなければならない場合もあります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）
MSTP 設定時の注意事項, （38 ページ）
MST リージョン, （40 ページ）

MSTP の制約事項

- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。
- switch スタックは最大 65 の MST インスタンスをサポートします。 特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。
- PVST+、Rapid PVST+、および MSTP はサポートされますが、アクティブにできるのは 1 つのバージョンだけです （たとえば、すべての VLAN で PVST+ を実行する、すべての VLAN で Rapid PVST+ を実行する、またはすべての VLAN で MSTP を実行します）。
- すべてのスタック メンバーは同一のスパニングツリー バージョンを実行する必要があります（すべての PVST+、Rapid PVST+、または MSTP）。
- MST コンフィギュレーションの VLAN トランキング プロトコル（VTP）伝搬はサポートされません。 ただし、コマンドライン インターフェイス（CLI）または簡易ネットワーク管理プロトコル（SNMP）サポートを通じて、MST リージョン内の各switchで MST コンフィギュレーション（リージョン名、リビジョン番号、およびVLANとインスタンスのマッピング）を手動で設定することは可能です。

- ネットワークを多数のリージョンに分割することは推奨できません。ただし、どうしても分割せざるを得ない場合は、スイッチド LAN をルータまたは非レイヤ 2 デバイスで相互接続された小規模な LAN に分割することを推奨します。
- リージョンは、同じ MST コンフィギュレーションを持つ 1 つまたは複数のメンバーで構成されます。リージョンの各メンバーは高速スパニングツリー プロトコル（RSTP）ブリッジ プロトコルデータユニット（BPDU）を処理する機能を備えている必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリー インスタンスの数は 65 までです。 VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。
- switchをルート switchとして設定した後に、**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、および **spanning-tree mst max-age** グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、最大エージング タイムを手動で設定することは推奨できません。

表 *5*：*PVST+*、*MSTP*、*Rapid PVST+* の相互運用性と互換性

	PVST+	MSTP	Rapid PVST+
PVST+	あり	あり（制限あり）	あり（PVST+ に戻る）
MSTP	あり（制限あり）	あり	あり（PVST+ に戻る）
Rapid PVST+	あり（PVST+ に戻る）	あり（PVST+ に戻る）	あり

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化，（56 ページ）
MSTP 設定時の注意事項，（38 ページ）
MST リージョン，（40 ページ）
ルート Switchの設定，（59 ページ）
ルート スイッチ，（39 ページ）
MST リージョン設定の指定と MSTP のイネーブル化，（56 ページ）

MSTP について

MSTP の設定

高速コンバージェンスのために RSTP を使用する MSTP では、複数の VLAN をグループ化して同じスパニングツリーインスタンスにマッピングすることが可能で、多くの VLAN をサポートするのに必要なスパニングツリーインスタンスの数を軽減できます。 MSTP は、データ トラフィックに複数の転送パスを提供し、ロードバランシングを実現して、多数の VLAN をサポートするのに

必要なスパニングツリー インスタンスの数を減らすことができます。 MSTP を使用すると、1 つのインスタンス（転送パス）で障害が発生しても他のインスタンス（転送パス）は影響を受けないので、ネットワークのフォールトトレランスが向上します。

（注） マルチ スパニングツリー（MST）実装は IEEE 802.1s 標準に準拠しています。

MSTP を導入する場合、最も一般的なのは、レイヤ 2 スイッチド ネットワークのバックボーンおよびディストリビューション レイヤへの導入です。 MSTP の導入により、サービス プロバイダー環境に求められる高可用性ネットワークを実現できます。

switchが MST モードの場合、IEEE 802.1w 準拠の RSTP が自動的にイネーブルになります。 RSTP は、IEEE 802.1D の転送遅延を軽減し、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行する明示的なハンドシェイクによって、スパニングツリーの高速コンバージェンスを実現します。

MSTP と RSTP は、既存のシスコ独自の Multiple Instance STP（MISTP）、および既存の Cisco PVST+ と Rapid Per-VLAN Spanning-Tree plux（Rapid PVST+）を使用して、スパニングツリーの動作を改善し、（オリジナルの）IEEE 802.1D スパニング ツリーに準拠した機器との下位互換性を保持しています。

switch スタックは、ネットワークのその他の部分に対しては単一のスパニングツリー ノードに見え、すべてのスタック メンバーが同一のswitch ID を使用します。

MSTP 設定時の注意事項

- **spanning-tree mode mst** グローバル コンフィギュレーション コマンドを使用して、MST をイネーブルにすると、RSTP が自動的にイネーブルになります。
- UplinkFast、BackboneFast、クロススタック UplinkFast の設定のガイドラインについては、関連項目のセクションの該当するセクションを参照してください。
- switchが MST モードの場合は、パス コスト値の計算に、ロング パス コスト計算方式（32 ビット）が使用されます。 ロング パス コスト計算方式では、次のパス コスト値がサポートされます。

速度	パス コスト値
10 Mb/s	2,000,000
100 Mb/s	200,000
1 Gb/s	20,000
10 Gb/s	2,000
100 Gb/s	200

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）
MSTP の前提条件, （35 ページ）
MSTP の制約事項, （36 ページ）
スパニングツリーの相互運用性と下位互換性, （14 ページ）
オプションのスパニングツリー設定時の注意事項
BackboneFast, （87 ページ）
UplinkFast, （82 ページ）

ルート スイッチ

switchは、マッピングされている VLAN グループのスパニングツリー インスタンスを保持しています。 switch ID は、switchのプライオリティおよびswitchの MAC アドレスで構成されており、各インスタンスに関連付けられます。 VLAN のグループでは、最小のswitch ID をもつswitchがルート switchになります。

switchをルートとして設定する場合は、switch プライオリティをデフォルト値（32768）からそれより大幅に低い値に変更し、switchが、指定したスパニング ツリー インスタンスのルート switchになるようにします。 このコマンドを入力すると、switchはルート switchesのswitch プライオリティをチェックします。 拡張システム ID をサポートしているため、24576 という値でswitchesが指定したスパニングツリー インスタンスのルートとなる場合、そのswitchは指定したインスタンスに対する自身のプライオリティを 24576 に設定します。

指定されたインスタンスのルート switchに 24576 に満たないswitch プライオリティが設定されている場合は、switchは自身のプライオリティを最小のswitch プライオリティより 4096 だけ小さい値に設定します （4096 は 4 ビット switch プライオリティの最下位ビットの値です）。 詳細については、関連項目の「Bridge ID, Switch Priority, and Extended System ID」リンクを参照してください。

ネットワークが、拡張システム ID をサポートするswitchesとサポートしないものの両方で構成されている場合、拡張システム ID をサポートするswitchがルート switchになる可能性は低くなります。 古いソフトウェアを実行している接続switchのプライオリティより VLAN 番号が大きい場合は常に、拡張システム ID によってスイッチ プライオリティ値が増加します。

各スパニングツリー インスタンスのルート switchは、バックボーンまたはディストリビューション switchでなければなりません。 アクセス switchをスパニングツリー プライマリ ルートとして設定しないでください。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間の最大switch ホップ カウント）を指定するには、**diameter** キーワード（MST インスタンスが 0 の場合のみ使用できる）を指定します。 ネットワーク直径を指定すると、switchはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に設定します。その結果、コンバージェンスに要する時間が大幅に短縮されます。 **hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

関連トピック

ルート Switchの設定, （59 ページ）
MSTP の制約事項, （36 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID, （5 ページ）

MST リージョン

スイッチを MST インスタンスに加入させるには、同じ MST コンフィギュレーション情報を使用して矛盾のないようにスイッチを設定する必要があります。 同じ MST 設定の相互接続スイッチの集まりによって MST リージョンが構成されます。

MST 設定では、それぞれのswitchが属する MST リージョンが制御されます。 この設定には、領域の名前、バージョン番号、MST VLAN とインスタンスの割り当てマップが含まれます。 その中で MST リージョンの設定を指定することにより、リージョンのswitchを設定します。 MST インスタンスに VLAN をマッピングし、リージョン名を指定して、リビジョン番号を設定できます。手順と例については、関連項目の「MST リージョンの設定の指定と MSTP のイネーブル化」リンクをクリックします。

リージョンには、同一の MST コンフィギュレーションを持った 1 つまたは複数のメンバが必要です。 さらに、各メンバは、RSTP ブリッジ プロトコル データ ユニット（BPDU）を処理できる必要があります。 ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリーインスタンスの数は65までです。 インスタンスは、0～4094 の範囲の任意の番号で識別できます。 VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。

関連トピック

MST リージョンの図, （43 ページ）
MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）
MSTP の前提条件, （35 ページ）
MSTP の制約事項, （36 ページ）
スパニングツリーの相互運用性と下位互換性, （14 ページ）
オプションのスパニングツリー設定時の注意事項
BackboneFast, （87 ページ）
UplinkFast, （82 ページ）

IST、CIST、CST

すべてのスパニングツリーインスタンスが独立している PVST+ および Rapid PVST+ とは異なり、MSTP は次の 2 つのタイプのスパニングツリーを確立して保持しています。

- Internal Spanning-Tree（IST）は、1 つの MST リージョン内で稼働するスパニングツリーです。

各 MST リージョン内の MSTP は複数のスパニングツリー インスタンスを維持しています。インスタンス 0 は、リージョンの特殊なインスタンスで、IST と呼ばれています。 その他すべての MSTI には、1 ～ 4094 の番号が付きます。

IST は、BPDU を送受信する唯一のスパニングツリー インスタンスです。 他のスパニングツリーの情報はすべて、MSTP BPDU 内にカプセル化されている M レコードに格納されています。 MSTP BPDU はすべてのインスタンスの情報を伝送するので、複数のスパニングツリー インスタンスをサポートする処理が必要な BPDU の数を大幅に減少できます。

同一リージョン内の すべての MST インスタンスは同じプロトコル タイマーを共有しますが、各 MST インスタンスは独自のトポロジ パラメータ（ルート switch ID、ルート パス コストなど）を持っています。 デフォルトでは、すべての VLAN が IST に割り当てられます。

MSTI はリージョンにローカルです。たとえばリージョン A およびリージョン B が相互接続されていても、リージョン A の MSTI 1 は、リージョン B の MSTI 1 に依存しません。

- Common and Internal Spanning-Tree（CIST）は、各 MST リージョン内の IST と、MST リージョンおよびシングル スパニングツリーを相互接続する Common Spanning-Tree（CST）の集合です。

  1 つのリージョン内で計算されたスパニングツリーは、スイッチド ドメイン全体を網羅する CST のサブツリーと見なされます。 CIST は、IEEE 802.1w、IEEE 802.1s、および IEEE 802.1D 標準をサポートするスイッチ間で実行されるスパニングツリーアルゴリズムによって形成されます。 MST リージョン内の CIST は、リージョン外の CST と同じです。

MST リージョン内の動作

IST は 1 つのリージョン内のすべての MSTP スイッチを接続します。 IST が収束すると、IST のルートは、CIST リージョナル ルート（IEEE 802.1s 標準が実装される以前は *IST* マスターと呼ばれた）になります。 これは、リージョン内で最も小さいswitch ID、および CIST ルートに対するパス コストをもつswitchです。 ネットワークに領域が 1 つしかない場合、CIST リージョナル ルートは CIST ルートにもなります。 CIST ルートがリージョンの外部にある場合、リージョンの境界に位置する MSTP スイッチの 1 つが CIST リージョナル ルートとして選択されます。

MSTP switchは初期化時に、自身が CIST のルートおよび CIST リージョナル ルートであることを主張するために CIST ルートと CIST リージョナル ルートへのパス コストがいずれもゼロに設定された BPDU を送信します。 switchはすべての MSTI を初期化し、そのすべてのルートであることを主張します。 switchは、ポート用に現在保存されているものより上位の MST ルート情報（低いswitch ID、低いパス コストなど）を受信した場合、CIST リージョナル ルートとしての主張を放棄します。

リージョンには、初期化中に多くのサブ リージョンが含まれて、それぞれに独自の CIST リージョナル ルートが含まれることがあります。 スイッチは、優位の IST 情報を受信すると、古いサブリージョンを脱退して、真の CIST リージョナル ルートが含まれている新しいサブリージョンに加入します。 真の CIST リージョナル ルートが含まれている以外のサブリージョンは、すべて縮小します。

正常な動作のためには、MST リージョン内のすべてのスイッチが同じ CIST リージョナル ルートを承認する必要があります。 共通の CIST リージョナル ルートに収束する場合、そのリージョン

内にある 2 つのスイッチは、1 つの MST インスタンスに対するポートの役割のみを同期させます。

関連トピック

MST リージョンの図, （43 ページ）

MST リージョン間の動作

ネットワーク内に複数のリージョンまたはレガシー IEEE 802.1D switchesが混在している場合、MSTP は、ネットワーク内のすべての MST リージョンとすべてのレガシー STP switchesから構成される CST を構築して保持します。 MSTI は、リージョンの境界にある IST と組み合わさり、CST になります。

IST はリージョン内のすべての MSTP switchesを接続し、スイッチド ドメイン全体を囲む CIST のサブツリーとして認識されます。 サブツリーのルートは CIST リージョナル ルートです。 MST リージョンは、隣接する STP switchおよびMST リージョンへの仮想switchesとして認識されます。

CST インスタンスのみが BPDU を送受信し、MST インスタンスはスパニングツリー情報を BPDU に追加して隣接するswitchesと相互作用し、最終的なスパニングツリートポロジーを算出します。そのため、BPDU 送信に関連したスパニングツリー パラメータ（たとえば hello タイム、転送時間、最大エージング タイム、最大ホップ数など）は、CST インスタンスのみで設定されますが、すべての MST インスタンスに影響します。 スパニングツリー トポロジに関連するパラメータ（switch プライオリティ、ポート VLAN コスト、ポート VLAN プライオリティなど）は、CST インスタンスと MST インスタンスの両方で設定できます。

MSTP switchesは、バージョン 3 RSTP BPDU または IEEE 802.1D STP BPDU を使用して、レガシー IEEE 802.1D switchesと通信します。 MSTP switchesは、MSTP BPDU を使用して MSTP switchesと通信します。

関連トピック

MST リージョンの図, （43 ページ）

IEEE 802.1s の用語

シスコの先行標準実装で使用される一部の MST 命名規則は、一部の内部パラメータまたはリージョンパラメータを識別するように変更されました。 これらのパラメータは、ネットワーク全体に関連している外部パラメータと違い、MST リージョン内でのみ影響があります。 CIST はネットワーク全体を網羅するスパニングツリーインスタンスのため、CISTパラメータのみ、内部修飾子やリージョナル修飾子ではなく外部修飾子が必要です。

- CIST ルートは、ネットワーク全体を網羅する一意のインスタンスのためのルート switchです。
- CIST 外部ルート パス コストは、CIST ルートまでのコストです。 このコストは MST 領域内で変化しません。 MST リージョンは、CIST への単一switchと見なすことに注意してください。 CIST 外部ルート パス コストは、これらの仮想switches、およびどのリージョンにも属さないswitchesの間で算出されるルート パス コストです。

- CIST リージョナル ルートは、準規格の実装で IST マスターと呼ばれていました。 CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。 CIST ルートがリージョン内にない場合、CIST リージョナル ルートは、リージョン内の CIST ルートに最も近い switchです。 CIST リージョナル ルートは、IST のルート switchとして動作します。
- CIST 内部ルート パス コストは、領域内の CIST リージョナル ルートまでのコストです。 このコストは、IST つまりインスタンス 0 だけに関連します。

表 *6*：準規格と規格の用語

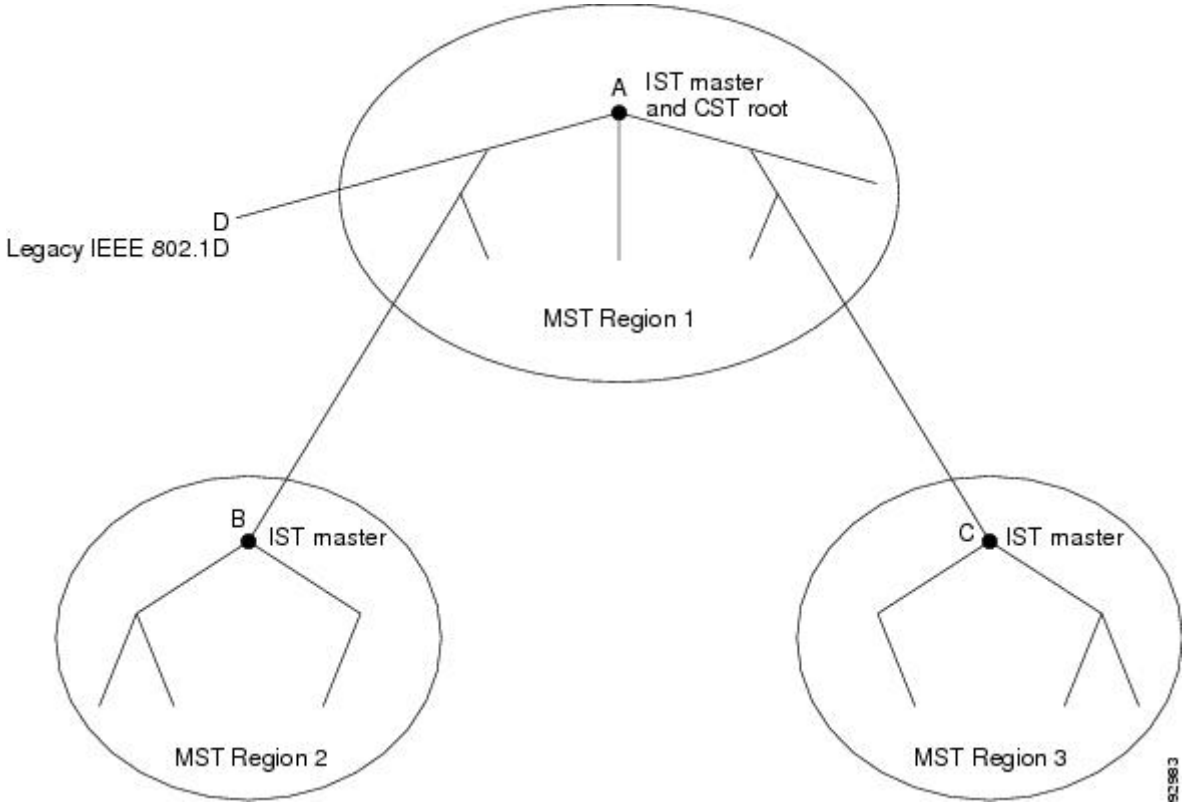
IEEE 標準	シスコ先行標準	シスコ標準
CIST リージョナル ルート	IST マスター	CIST リージョナル ルート
CIST 内部ルート パス コスト	IST マスター パス コスト	CIST 内部パス コスト
CIST 外部ルート パス コスト	ルート パス コスト	ルート パス コスト
MSTI リージョナル ルート	インスタンス ルート	インスタンス ルート
MSTI 内部ルート パス コスト	ルート パス コスト	ルート パス コスト

MST リージョンの図

この図は、3 個の MST リージョンとレガシー IEEE 802.1D switch（D）を示しています。 リージョン 1 の CIST リージョナル ルート（A）は、CIST ルートでもあります。 リージョン 2 の CIST リー

ジョナル ルート（B）、およびリージョン 3 の CIST リージョナル ルート（C）は、CIST 内のそれぞれのサブツリーのルートです。 RSTP はすべてのリージョンで稼働しています。

図 *5* : ***MST*** リージョン、***CIST*** マスター、および ***CST*** ルート



関連トピック

MST リージョン, （40 ページ）
MST リージョン内の動作, （41 ページ）
MST リージョン間の動作, （42 ページ）

ホップ カウント

IST および MST インスタンスは、スパニングツリー トポロジの計算に、コンフィギュレーション BPDU のメッセージ有効期間と最大エージング タイムの情報を使用しません。 その代わりに、IP Time To Live（TTL）メカニズムに似た、ルートまでのパス コストおよびホップ カウント メカニズムを使用します。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用することにより、リージョン内の最大ホップを設定し、その値をリージョン内の IST インスタンスとすべての MST インスタンスに適用できます。 ホップ カウントを設定すると、メッセージ エージ情報を設定するのと同様の結果が得られます（再構成の開始時期を決定します）。 インスタンスのルート switch

は、コストが 0 でホップ カウントが最大値に設定されている BPDU（M レコード）を常に送信します。 switchは、この BPDU を受信すると、受信した残りのホップ カウントから 1 を引き、生成する BPDU で残りのホップ カウントとしてこの値を伝播します。 カウントがゼロに達すると、switchは BPDU を廃棄し、ポート用に維持されている情報を期限切れにします。

BPDUのRSTP部分に格納されているメッセージ有効期間と最大エージング タイムの情報は、リージョン全体で同じままであり、そのリージョンの境界に位置する指定ポートによって同じ値が伝播されます。

境界ポート

シスコ先行標準の実装では、境界ポートは、RSTP が稼働する単一のスパニングツリー リージョン、PVST+ または Rapid PVST+ が稼働する単一のスパニングツリー リージョン、または異なる MST コンフィギュレーションを持つ別の MST リージョンに MST リージョンを接続します。 境界ポートは、LAN、単一のスパニングツリーswitchまたはMST設定が異なるswitchの指定switchにも接続します。

IEEE 802.1s 標準では、境界ポートの定義はなくなりました。 IEEE 802.1Q-2002 標準では、ポートが受信できる 2 種類のメッセージを識別します。

- 内部（同一リージョンから）
- 外部（別のリージョンから）

メッセージが内部の場合、CIST の部分はCIST によって受信されるので、各 MST インスタンスは個々の M レコードだけを受信します。

メッセージが外部である場合、CIST だけが受信します。 CIST の役割がルートや代替ルートの場合、または外部BPDUのトポロジが変更された場合は、MSTインスタンスに影響する可能性があります。

MST リージョンには、switchesおよび LAN の両方が含まれます。 セグメントは、DP のリージョンに属します。 そのため、セグメントの指定ポートではなく異なるリージョンにあるポートは境界ポートになります。 この定義では、リージョン内部の 2 つのポートが、別のリージョンに属するポートとセグメントを共有し、内部メッセージおよび外部メッセージの両方を 1 つのポートで受信できるようになります。

シスコ先行標準の実装との主な違いは、STP 互換モードを使用している場合、指定ポートが境界ポートとして定義されない点です。

（注） レガシー STP switchがセグメントに存在する場合、メッセージは常に外部と見なされます。

シスコ先行標準の実装から他に変更された点は、送信switch ID を持つ RSTP またはレガシー IEEE 802.1Q switchの部分に、CIST リージョナル ルート switch ID フィールドが加えられたことです。リージョン全体は、一貫した送信者switch ID をネイバー switchesに送信し、単一仮想switchのように動作します。 この例では、A または B がセグメントに指定されているかどうかに関係なく、ルートの一貫した送信者switch ID が同じである BPDU をswitch C が受信します。

IEEE 802.1s の実装

シスコの IEEE MST 標準の実装には、標準の要件を満たす機能だけでなく、すでに公開されている標準には含まれていない一部の（要望されている）先行標準の機能が含まれています。

ポートの役割名の変更

境界の役割は最終的にMST標準に含まれませんでしたが、境界の概念自体はシスコの実装に投影されています。 ただし、リージョン境界にある MST インスタンスのポートは、対応する CIST ポートのステートに必ずしも従うわけではありません。 現在、2 つの境界の役割が存在しています。

- 境界ポートが CIST リージョナル ルートのルート ポートである場合：CIST インスタンス ポートを提案されて同期中の場合、対応するすべての MSTI ポートの同期を取り終わった後であれば（その後フォワーディングします）、その場合のみ合意を返信してフォワーディング ステートに移行できます。 MSTI ポートには、特別なマスターの役割があります。
- 境界ポートが CIST リージョナル ルートのルート ポートでない：MSTI ポートは、CIST ポートのステートおよび役割に従います。 標準では提供される情報が少ないため、MSTI ポートが BPDU（M レコード）を受信しない場合、MSTI ポートが BPDU を代わりにブロックできる理由がわかりにくい場合があります。 この場合、境界の役割自体は存在していませんが、**show** コマンドで見ると、出力される *type* カラムで、ポートが境界ポートとして認識されていることがわかります。

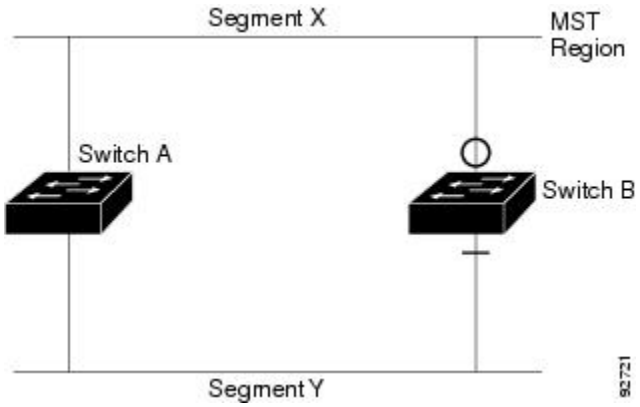
レガシーおよび規格Switchesの相互運用

準規格switchesの自動検出はエラーになることがあるので、インターフェイス コンフィギュレーション コマンドを使用して準規格ポートを識別できます。 switchの規格と準規格の間にリージョンを形成することはできませんが、CISTを使用して相互運用することができます。 このような特別な方法を採用しても、失われる機能は、異なるインスタンス上のロード バランシングだけです。 ポートが先行標準の BPDU を受信すると、CLI（コマンドライン インターフェイス）にはポートの設定に応じて異なるフラグが表示されます。 switchが準規格 BPDU 送信用に設定されていないポートで準規格 BPDU を初めて受信したときは、Syslog メッセージも表示されます。

A が規格のswitchで、B が準規格のswitchとして、両方とも同じリージョンに設定されているとします。 A が CIST のルート switchで、B はセグメント X 上にルート ポート（BX）を、セグメント Y 上に代替ポート（BY）を保持しています。 セグメント Y がフラップして BY のポートが代替になってから 1 つの準規格 BPDU を送信すると、準規格switchが Y に接続されていることを AY は検出できず、規格 BPDU の送信を続けます。 ポート BY は境界に固定され、A と B の間での

ロードバランスは不可能になります。 セグメント X にも同じ問題がありますが、B は TC を送信することがあります。

図 *6*：規格および準規格の*Switch*の相互運用



（注） 規格 MST 実装と準規格 MST 実装間の相互作用を最低限に抑えることを推奨します。

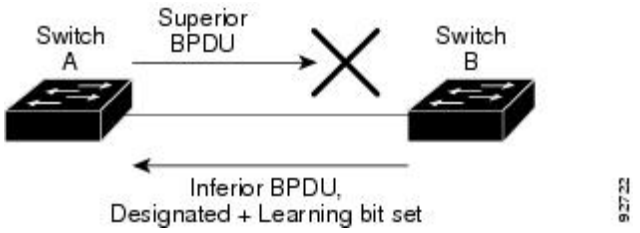
単一方向リンク障害の検出

IEEE MST 標準にはこの機能が存在していませんが、Cisco IOS Release には加えられています。ソフトウェアを使用することで、受信したBPDUからポートの役割とステートの一貫性を確認し、単一方向リンクが失敗してブリッジ処理のループを引き起こしていないかどうかを検証できます。

指定ポートは、矛盾を検出すると、そのロールを維持しますが、廃棄ステートに戻ります。一貫性がない場合は、接続を中断した方がブリッジング ループを解決できるからです。

次の図に、ブリッジング ループの一般的な原因となる単方向リンク障害を示します。 Switch A はルート switchであり、switch B へのリンクで BPDU は失われます。 RSTP および MST BPDU には、送信側ポートの役割とステートが含まれます。 switch A はこの情報を使用し、ルータ A が送信する上位 BPDU にswitch B が反応しないこと、およびswitch B がルート switchではなく指定ブリッジであることを検出できます。 この結果、switch A は、そのポートをブロックし（またはブロックし続け）、ブリッジング ループが防止されます。

図 *7*：単一方向リンク障害の検出



MSTP およびSwitch スタック

switch スタックは、ネットワークのその他の部分に対しては単一のスパニングツリー ノードに見え、すべてのスタック メンバーが与えられたスパニングツリーに同一のブリッジ ID を使用します。 ブリッジ ID は、active switchの MAC アドレスから取得されます。

スタックがネットワークのルートで、スタック内でルートの選択が行われていない場合は、active switchがスタック ルートになります。

switch スタックがスパニング ツリー ルートで、active switchで障害が発生した、またはスタックから外れた場合、スタンバイ スイッチが新しいアクティブ スイッチになり、ブリッジ ID は同じままで、スパニング ツリーの再コンバージェンスが発生する可能性があります。

MSTP をサポートしていないswitchが、MSTP またはリバースをサポートしているswitch スタックに追加されると、switchはバージョンが不一致の状態になります。 可能な場合、switchは、switch スタックで実行中のソフトウェアと同じバージョンに自動的にアップグレードまたはダウングレードされます。

IEEE 802.1D STP との相互運用性

MSTP が稼働しているswitchは、IEEE 802.1D 準拠のレガシー switchesとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。 このswitchは、レガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定されている BPDU）を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。 また、MSTP switchは、レガシー BPDU、別のリージョンに関連付けられている MSTP BPDU（バージョン 3）、または RSTP BPDU（バージョン 2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、switchが IEEE 802.1D BPDU を受信していない場合は、自動的に MSTP モードに戻りません。これはレガシー switchが指定switchでない限り、レガシー switchがリンクから削除されたかどうか検出できないためです。 このswitchが接続するswitchがリージョンに加入していると、switch はポートに境界の役割を割り当て続ける場合があります。 プロトコル移行プロセスを再開するには（強制的にネイバー switchesと再びネゴシエーションするには）、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

リンク上のすべてのレガシー switchesが RSTP switchesであれば、これらのスイッチは、RSTP BPDU 同様に MSTP BPDU を処理できます。 したがって、MSTP switchesは、バージョン 0 コンフィギュレーションと TCN BPDU またはバージョン 3 MSTP BPDU のいずれかを境界ポートで送信します。境界ポートは、LAN、単一スパニングツリー switchまたは MST 設定が異なるswitchのいずれかの指定のswitchに接続します。

RSTP 概要

RSTP は、ポイントツーポイントの配線を利用して、スパニングツリーの高速コンバージェンスを実現します。 また、1 秒未満の間に、スパニングツリーを再構成できます（IEEE 802.1D スパニングツリーのデフォルトに設定されている 50 秒とは異なります）。

ポートの役割およびアクティブ トポロジー

RSTPは、ポートに役割を割り当てて、アクティブ トポロジを学習することによって高速コンバージェンスを実現します。 RSTP はswitch をルート switchとして最も高いswitch プライオリティ（プライオリティの数値が一番小さい）に選択するために、IEEE 802.1D STP 上に構築されます。 RSTP は、次のうちいずれかのポートの役割をそれぞれのポートに割り当てます。

- ルート ポート：switch がルートswitch にパケットを転送するとき、最適なパス（最低コスト）を提供します。
- 指定ポート：指定switchに接続し、その LAN からルート switchにパケットを転送するとき、パス コストを最低にします。 DP は、指定switchが LAN に接続されているポートです。
- 代替ポート：現在のルート ポートが提供したパスに代わるルート switchへの代替パスを提供します。
- バックアップ ポート：指定ポートが提供した、スパニングツリーのリーフに向かうパスのバックアップとして機能します。 バックアップ ポートは、2 つのポートがループバック内でポイントツーポイント リンクによって接続されるか、共有 LAN セグメントとの複数の接続がswitchにある場合に限って存在できます。
- ディセーブル ポート：スパニングツリーの動作において何も役割が与えられていません。

ルート ポートまたは DP の役割があるポートは、アクティブ トポロジーに組み込まれます。 代替ポートまたはバックアップ ポートのロールがあるポートは、アクティブ トポロジから除外されます。

ネットワーク全体のポートの役割に矛盾のない安定したトポロジでは、RSTP は、すべてのルート ポートおよび指定ポートがただちにフォワーディング ステートに移行し、代替ポートとバックアップ ポートが必ず廃棄ステート（IEEE 802.1D のブロッキング ステートと同じ）になるように保証します。 ポートのステートにより、転送処理および学習処理の動作が制御されます。

表 7: ポート ステートの比較

動作ステータス	STP ポート ステート（IEEE 802.1D）	RSTP ポート ステート	ポートがアクティブ トポロジに含まれているか
イネーブル	ブロッキング	廃棄	いいえ
イネーブル	リスニング	廃棄	いいえ
イネーブル	ラーニング	ラーニング	はい
イネーブル	フォワーディング	フォワーディング	はい
ディセーブル	ディセーブル	廃棄	いいえ

Cisco STP の実装との一貫性を保つため、このマニュアルでは、ポート ステートを廃棄ではなくブロッキングとして定義します。 DP はリスニング ステートから開始します。

高速コンバージェンス

RSTP は、switch、switch ポート、LAN のうちいずれかの障害のあと、接続の高速回復を提供します。 エッジ ポート、新しいルート ポート、ポイントツーポイント リンクで接続したポートに、高速コンバージェンスが次のように提供されます。

- エッジ ポート：**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して RSTP switchでエッジ ポートとしてポートを設定した場合、エッジ ポートはフォワーディング ステートにすぐに移行します。 エッジ ポートは Port Fast 対応ポートと同じであり、単一エンドステーションに接続しているポートだけでイネーブルにする必要があります。
- ルート ポート：RSTP は、新しいルート ポートを選択した場合、古いルート ポートをブロックし、新しいルート ポートをフォワーディング ステートにすぐに移行します。
- ポイントツーポイント リンク：ポイントツーポイント リンクで別のポートにポートを接続し、ローカル ポートが DP になると、提案と合意のハンドシェークを使用して別のポートと高速移行がネゴシエーションされ、ループがないトポロジーが確保されます。

  Switch A がSwitch B にポイントツーポイント リンクで接続され、すべてのポートはブロッキング ステートになっています。 Switch A のプライオリティの数値が、Switch B のプライオリティより小さいとします。 Switch A は提案メッセージ（提案フラグを設定した設定 BPDU）をSwitch B に送信し、指定switchとして自分自身を提案します。

  Switch B は、提案メッセージの受信後、提案メッセージを受信したポートを新しいルート ポートとして選択し、エッジ以外のすべてのポートを強制的にブロッキング ステートにして、新しいルート ポートを介して合意メッセージ（合意フラグを設定した BPDU）を送信します。

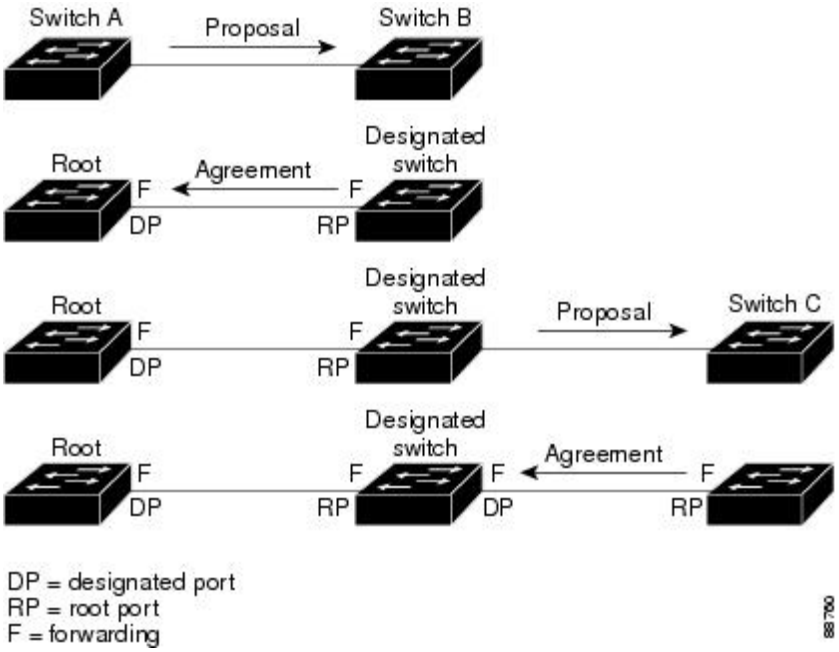
  Switch A も、Switch B の合意メッセージの受信後、指定ポートをフォワーディング ステートにすぐに移行します。 Switch B はすべてのエッジ以外のポートをブロックし、Switches A およびルータ B の間にポイントツーポイント リンクがあるので、ネットワークにループは形成されません。

  Switch C がSwitch B に接続すると、同様のセットのハンドシェーク メッセージが交換されます。 Switch C はSwitch B に接続されているポートをルート ポートとして選択し、両端がフォワーディング ステートにすぐに移行します。 このハンドシェーク処理を繰り返して、もう 1 つのswitchがアクティブ トポロジーに加わります。 ネットワークが収束すると、この提案/合意ハンドシェイクがルートからスパニングツリーのリーフへと進みます。

  switch スタックでは、Cross-Stack Rapid Transition（CSRT）機能を使用すると、ポートがフォワーディング ステートに移行する前に、スタック メンバで、提案/合意ハンドシェイク中にすべてのスタック メンバーから確認メッセージを受信できます。 switchが MST モードの場合、CSRT は自動的にイネーブルにされます。

switchはポートのデュプレックス モードによってリンク タイプを学習します。全二重ポートはポイントツーポイント接続と見なされ、半二重接続は共有接続と見なされます。**spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを使用すると、デュプレックス設定によって制御されるデフォルト設定を無効にすることができます。

図 *8*：高速コンバージェンスの提案と合意のハンドシェーク



ポート ロールの同期

switchがそのルータのポートの 1 つで提案メッセージを受信し、そのポートが新しいルート ポートとして選択されると、RSTP によってその他すべてのポートが新しいルートの情報と強制的に同期化します。

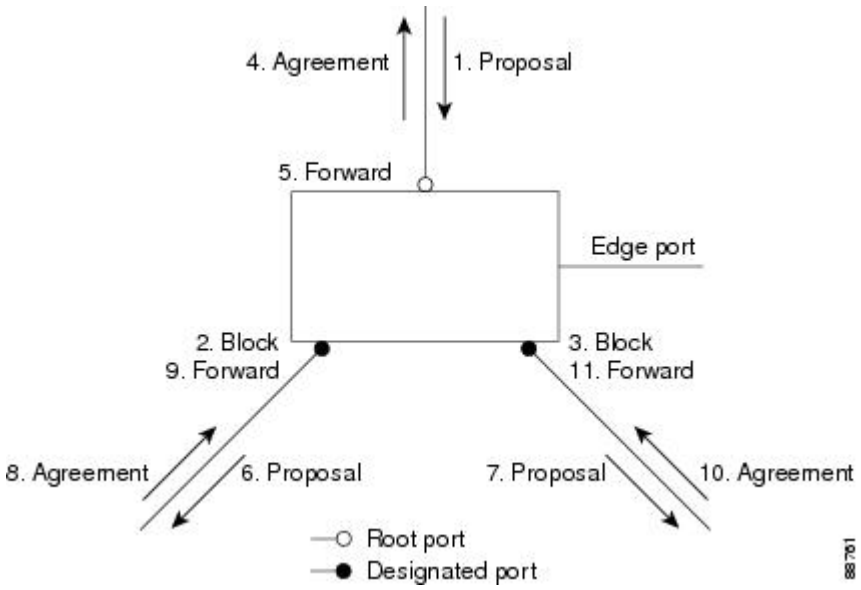
その他すべてのポートが同期化されている場合、switchはルート ポートで受信した上位ルート情報で同期化されます。 switchのそれぞれのポートは、次のような場合に同期化します。

- ブロッキング ステートである場合
- エッジ ポートである場合（ネットワークのエッジとして設定されているポート）

DP は、フォワーディング ステートになっていてエッジ ポートとして設定されていない場合、RSTP によって DP が強制的に新しいルート情報で同期化すると、DP がブロッキング ステートに移行します。 一般的に RSTP がルート情報でポートを強制的に同期化し、ポートが上の条件を満たしていない場合、そのポート ステートはブロッキングに設定されます。

switchは、すべてのポートが同期化されたことを確認した後で、ルート ポートに対応する指定switchに合意メッセージを送信します。 ポイントツーポイント リンクで接続されたswitchesがポートの役割で合意すると、RSTP はポート ステートをフォワーディングにすぐに移行します。

図 *9*：高速コンバージェンス中のイベントのシーケンス



ブリッジ プロトコル データ ユニットの形式および処理

RSTP BPDU のフォーマットは、プロトコル バージョンが 2 に設定されている点を除き、IEEE 802.1D BPDU のフォーマットと同じです。 新しい 1 バイトのバージョン 1 の Length フィールドは 0 に設定されます。これはバージョン 1 のプロトコルの情報がないことを示しています。

表 *8*：*RSTP BPDU* フラグ

ビット	機能
0	トポロジーの変化（TC）
1	提案
2 ～ 3: 00 01 10 11	ポートの役割： 不明 代替ポート ルート ポート 指定ポート
4	ラーニング

ビット	機能
5	フォワーディング
6	合意
7	トポロジー変更確認応答（TCA）

送信側switchはRSTP BPDUの提案フラグを設定し、そのLANの指定switchとして自分自身を提案します。 提案メッセージのポートの役割は、常にDPに設定されます。

送信側switchは、RSTP BPDUの合意フラグを設定して以前の提案を受け入れます。 合意メッセージのポートの役割は、常にルート ポートに設定されます。

RSTPには個別のトポロジ変更通知（TCN）BPDUはありません。 TCフラグが使用されて、TCが示されます。 ただし、IEEE 802.1D switchesとの相互運用性を保つために、RSTP switchはTCN BPDUの処理と生成を行います。

ラーニング フラグおよびフォワーディング フラグは、送信側ポートのステートに従って設定されます。

優位 BPDU 情報の処理

ポートに現在保存されているルート情報よりも優位のルート情報（小さいswitch ID、低いパス コストなど）をポートが受け取ると、RSTPは再構成を開始します。 ポートが新しいルート ポートとして提案されて選択されると、RSTPは強制的にその他すべてのポートを同期化します。

受信したBPDUが、提案フラグが設定されているRSTP BPDUである場合、switchはその他すべてのポートが同期化されてから合意メッセージを送信します。 BPDUがIEEE 802.1D BPDUの場合、switchは提案フラグを設定せずに、そのポートの転送遅延タイマーを起動します。 新しいルート ポートでは、フォワーディング ステートに移行するために、2倍の転送遅延時間が必要となります。

ポートで優位の情報が受信されたために、そのポートがバックアップ ポートまたは代替ポートになる場合、RSTPはそのポートをブロッキング ステートに設定し、合意メッセージは送信しません。 DPは、転送遅延タイマーが失効するまで、提案フラグを設定してBPDUを送信し続け、転送遅延タイマーの失効時に、ポートはフォワーディング ステートに移行します。

下位 BPDU 情報の処理

指定ポートの役割を持つ下位BPDU（そのポートに現在保存されている値より大きいswitch ID 、高いパス コストなど）を指定ポートが受信した場合、その指定ポートはただちに現在の自身の情報で応答します。

トポロジの変更

ここでは、スパニングツリー トポロジの変更処理について、RSTP と IEEE 802.1D の相違を説明します。

- 検出：IEEE 802.1D では、どのようなブロッキング ステートとフォワーディング ステートとの間の移行でもトポロジの変更が発生しますが、RSTP でトポロジの変更が発生するのは、ブロッキング ステートからフォワーディング ステートに移行する場合だけです（トポロジの変更と見なされるのは、接続数が増加する場合だけです）。エッジポートにおけるステート変更は、TC の原因になりません。 RSTP switchは、TC を検出すると、TCN を受信したポートを除く、エッジ以外のすべてのポートで学習した情報を削除します。
- 通知：IEEE 802.1D は TCN BPDU を使用しますが、RSTP は使用しません。 ただし、IEEE 802.1D との相互運用性を保つために、RSTP switchは TCN BPDU の処理と生成を行います。
- 確認：RSTP switchは、指定ポートで IEEE 802.1D switchから TCN メッセージを受信した場合、TCA ビットが設定された IEEE 802.1D コンフィギュレーション BPDU で応答します。ただし、IEEE 802.1D switchに接続されたルート ポートで TC 時間タイマー（IEEE 802.1D のトポロジ変更タイマーと同じ）がアクティブであり、TCA ビットが設定されたコンフィギュレーション BPDU が受信された場合、TC 時間タイマーはリセットされます。

  この処理は、IEEE 802.1D switchesをサポートする目的でのみ必要とされます。 RSTP BPDU は TCA ビットが設定されていません。
- 伝播：RSTP switchは、DP またはルート ポートを介して別のswitchから TC メッセージを受信すると、エッジ以外のすべての DP、およびルート ポート（TC メッセージを受信したポートを除く）に変更を伝播します。 switchはこのようなすべてのポートで TC-while タイマーを開始し、そのポートで学習した情報を消去します。
- プロトコルの移行：IEEE 802.1D switchesとの下位互換性を保つため、RSTP は IEEE 802.1D コンフィギュレーション BPDU および TCN BPDU をポート単位で必要に応じて送信します。

  ポートが初期化されると、移行遅延タイマーが開始され（RSTP BPDU が送信される最低時間を指定）、RSTP BPDU が送信されます。 このタイマーがアクティブである間、switchはそのポートで受信したすべての BPDU を処理し、プロトコル タイプを無視します。

  switchはポートの移行遅延タイマーが満了した後に IEEE 802.1D BPDU を受信した場合、IEEE 802.1D switchに接続されていると想定し、IEEE 802.1D BPDU のみの使用を開始します。 ただし、RSTP switchが 1 つのポートで IEEE 802.1D BPDU を使用していて、タイマーが満了した後に RSTP BPDU を受信した場合、タイマーが再起動し、そのポートで RSTP BPDU の使用が開始されます。

プロトコル移行プロセス

MSTP が稼働しているswitchは、IEEE 802.1D 準拠のレガシー switchesとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。 このswitchは、レガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定されている BPDU）を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。 また、MST switchは、レガシー

BPDU、別のリージョンに関連付けられている MSTP BPDU（バージョン 3）、または RST BPDU（バージョン 2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、switchが IEEE 802.1D BPDU を受信していない場合は、自動的に MSTP モードに戻りません。これはレガシー switchが指定switchでない限り、レガシー switchがリンクから削除されたかどうか検出できないためです。また、接続するswitchがリージョンに加入していると、switchはポートに境界の役割を割り当て続ける場合があります。

関連トピック

プロトコルの移行プロセスの再開，（75 ページ）

MSTP のデフォルト設定

表 *9*：*MSTP* のデフォルト設定

機能	デフォルト設定
スパニングツリー モード	MSTP
Switch プライオリティ（CIST ポートごとに設定可能）	32768
スパニングツリー ポート プライオリティ（CIST ポート単位で設定可能）	128
スパニングツリー ポート コスト（CIST ポート単位で設定可能）	1000 Mb/s：20000 100 Mb/s：20000 10 Mb/s：20000 1000 Mb/s：20000 100 Mb/s：20000 10 Mb/s：20000
hello タイム	3 秒
転送遅延時間	20 秒
最大エージング タイム	20 秒
最大ホップ カウント	20 ホップ

関連トピック

サポートされるスパニングツリー インスタンス，（14 ページ）

MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）

MSTP 機能の設定方法

MST リージョン設定の指定と MSTP のイネーブル化

2 つ以上のスイッチを同じ MST リージョンに設定するには、その 2 つのスイッチに同じ VLAN/インスタンスマッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。

リージョンには、MST 設定が同一である、1 つ以上のメンバーを含めることができます。各メンバーでは、RSTP BPDU を処理できる必要があります。 ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリーインスタンスの数は65までです。 VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree mst configuration**
4. **instance** *instance-id* **vlan** *vlan-range*
5. **name** *name*
6. **revision** *version*
7. **show pending**
8. **exit**
9. **spanning-tree mode mst**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**spanning-tree mst configuration** 例： `Switch(config)# spanning-tree mst configuration`	MST コンフィギュレーション モードを開始します。
ステップ 4	**instance** *instance-id* **vlan** *vlan-range* 例： `Switch(config-mst)# instance 1 vlan 10-20`	VLAN を MSTI にマップします。 • *instance-id* に指定できる範囲は、0 ～ 4094 です。 • **vlan** *vlan-range* に指定できる範囲は、1 ～ 4094 です。 VLAN を MSTI にマップする場合、マッピングは増加され、コマンドに指定した VLAN は、以前マッピングした VLAN に追加されるか、そこから削除されます。 VLAN の範囲を指定するには、ハイフンを使用します。たとえば **instance 1 vlan 1-63** では、VLAN 1 ～ 63 が MSTI 1 にマップされます。 一連の VLAN を指定するには、カンマを使用します。たとえば **instance 1 vlan 10, 20, 30** と指定すると、VLAN 10、20、30 が MSTI 1 にマップされます。
ステップ 5	**name** *name* 例： `Switch(config-mst)# name region1`	コンフィギュレーション名を指定します。 *name* 文字列の最大の長さは 32 文字であり、大文字と小文字が区別されます。
ステップ 6	**revision** *version* 例： `Switch(config-mst)# revision 1`	設定リビジョン番号を指定します。 指定できる範囲は 0 ～ 65535 です。
ステップ 7	**show pending** 例： `Switch(config-mst)# show pending`	保留中の設定を表示し、設定を確認します。
ステップ 8	**exit** 例： `Switch(config-mst)# exit`	すべての変更を適用し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**spanning-tree mode mst** 例： `Switch(config)# spanning-tree mode mst`	MSTP をイネーブルにします。RSTP もイネーブルになります。 スパニングツリー モードを変更すると、すべてのスパニングツリーインスタンスは以前のモードであるため停止し、新しいモードで再起動するので、トラフィックを中断させる可能性があります。 MSTP と PVST+ または MSTP と Rapid PVST+ を同時に実行することはできません。
ステップ 10	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MSTP 設定時の注意事項, （38 ページ）
MST リージョン, （40 ページ）
MSTP の前提条件, （35 ページ）
MSTP の制約事項, （36 ページ）
スパニングツリーの相互運用性と下位互換性, （14 ページ）
オプションのスパニングツリー設定時の注意事項
BackboneFast, （87 ページ）
UplinkFast, （82 ページ）
MSTP のデフォルト設定, （55 ページ）
ルート Switchの設定, （59 ページ）
MSTP の制約事項, （36 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID, （5 ページ）
セカンダリ ルートの設定Switch, （60 ページ）
ポート プライオリティの設定, （62 ページ）
パス コストの設定, （64 ページ）
Switch プライオリティの設定, （65 ページ）
hello タイムの設定, （67 ページ）
転送遅延時間の設定, （68 ページ）
最大エージング タイムの設定, （70 ページ）
最大ホップ カウントの設定, （71 ページ）
高速移行を確実にするためのリンク タイプの指定, （72 ページ）

ネイバー タイプの設定, （73 ページ）
プロトコルの移行プロセスの再開, （75 ページ）

ルート Switchの設定

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、switchで指定されて有効になっている必要があります。 詳細については、関連項目を参照してください。

指定された MST インスタンス ID も把握する必要があります。 この例の手順 2 では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree mst** *instance-id* **root primary**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst** *instance-id* **root primary** 例： `Switch(config)# spanning-tree mst 0 root primary`	ルート switchとしてswitchを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 指定できる範囲は 0 ～ 4094 です

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

ルート スイッチ, （39 ページ）
MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）
MSTP の制約事項, （36 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID, （5 ページ）
セカンダリ ルートの設定Switch, （60 ページ）

セカンダリ ルートの設定Switch

拡張システム ID をサポートするswitchをセカンダリ ルートとして設定する場合、switch プライオリティはデフォルト値（32768）から 28672 に修正されます。 プライマリ ルート switchで障害が発生した場合は、このswitchが指定インスタンスのルート switchになる可能性があります。 ここでは、その他のネットワーク switchesが、デフォルトのswitch プライオリティの 32768 を使用しているためにルート switchになる可能性が低いことが前提となっています。

このコマンドを複数のswitchに対して実行すると、複数のバックアップ ルート switchesを設定できます。 **spanning-tree mst** *instance-id* **root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート switchを設定したときと同じネットワーク直径およびhello タイム値を使用してください。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、switchで指定されて有効になっている必要があります。 詳細については、関連項目を参照してください。

指定された MST インスタンス ID も把握する必要があります。 この例では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree mst** *instance-id* **root secondary**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst** *instance-id* **root secondary** 例： `Switch(config)# spanning-tree mst 0 root secondary`	セカンダリ ルート switchとしてswitchを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 指定できる範囲は 0 ～ 4094 です
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）
ルート Switchの設定, （59 ページ）

ポート プライオリティの設定

ループが発生した場合、MSTP はポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。 最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）を割り当てることができます。 すべてのインターフェイスに同じプライオリティ値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

（注） switchがswitch スタックのメンバーの場合、**spanning-tree mst** [*instance-id*] **port-priority** *priority* インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree mst** [*instance-id*] **cost** *cost* インターフェイス コンフィギュレーション コマンドを使用し、フォワーディング ステートにするインターフェイスを選択する必要があります。 最初に選択させたいポートには、より小さいコスト値を割り当て、最後に選択させたいポートには、より大きいコスト値を割り当てることができます。 詳細については、関連項目の下に表示されるパス コストのトピックを参照してください。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、switchで指定されて有効になっている必要があります。 詳細については、関連項目を参照してください。

指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。 この例では、インスタンス ID として 0 を使用し、インターフェイスとして GigabitEthernet1/0/1 を使用します。これは「関連項目」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **spanning-tree mst** *instance-id* **port-priority** *priority*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface GigabitEthernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**spanning-tree mst** *instance-id* **port-priority** *priority* 例： `Switch(config-if)# spanning-tree mst 0 port-priority 64`	ポート プライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 指定できる範囲は 0 ～ 4094 です • *priority* 値の範囲は 0 ～ 240 で、16 ずつ増加します。デフォルト値は 128 です。 値が小さいほど、プライオリティが高くなります。 使用可能な値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 だけです。 その他の値はすべて拒否されます。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

show spanning-tree mst interface *interface-id* 特権 EXEC コマンドによって表示されるのは、リンクアップ動作可能状態のポートの情報だけです。 ポートがリンクアップ動作状態になっていない場合は、**show running-config interface** 特権 EXEC コマンドを使用して設定を確認できます。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）
パス コストの設定, （64 ページ）

パス コストの設定

MSTP パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。 ループが発生した場合、MSTP はコストを使用して、フォワーディング ステートにするインターフェイスを選択します。 最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択されるインターフェイスには高いコスト値を割り当てることができます。 すべてのインターフェイスに同じコスト値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、switchで指定されて有効になっている必要があります。 詳細については、関連項目を参照してください。

指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。 この例では、インスタンス ID として 0 を使用し、インターフェイスとして GigabitEthernet1/0/1 を使用します。これは「関連項目」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **spanning-tree mst** *instance-id* **cost** *cost*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。 有効なインターフェイスには、物理ポートとポート チャネル論理インターフェイスがあります。 ポート チャネル範囲は 1 ～ 48 です。
ステップ 4	**spanning-tree mst** *instance-id* **cost** *cost* 例： `Switch(config-if)# spanning-tree mst 0 cost 17031970`	コストを設定します。 ループが発生した場合、MSTPはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。 低いパス コストは高速送信を表します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 指定できる範囲は 0 ～ 4094 です • *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

show spanning-tree mst interface *interface-id* 特権 EXEC コマンドによって表示されるのは、リンクアップ動作可能状態のポートの情報だけです。 そうでない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

関連トピック

ポート プライオリティの設定, （62 ページ）
MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）

Switch プライオリティの設定

switchのプライオリティを変更すると、スタンドアロン switchまたはスタック内のswitchであるかに関係なく、ルートswitchとして選択される可能性が高くなります。

（注） このコマンドの使用には注意してください。 通常のネットワーク設定では、**spanning-tree mst** *instance-id* **root primary** および **spanning-tree mst** *instance-id* **root secondary** グローバル コンフィギュレーション コマンドを使用して、switchをルートまたはセカンダリ ルート switchとして指定することをお勧めします。 これらのコマンドが動作しない場合にのみswitchプライオリティを変更する必要があります。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、switchで指定されて有効になっている必要があります。 詳細については、関連項目を参照してください。

使用する指定された MST インスタンス ID も把握する必要があります。 この例では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree mst** *instance-id* **priority** *priority*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst** *instance-id* **priority** *priority* 例： `Switch(config)# spanning-tree mst 0 priority 40960`	switchのプライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 指定できる範囲は 0 ～ 4094 です

	コマンドまたはアクション	目的
		• *priority* の範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。 この値が低いほど、switchがルート switch として選択される可能性が高くなります。 使用可能な値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。 これらは唯一の許容値です。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）

hello タイムの設定

hello タイムはルート switchによって設定メッセージが生成されて送信される時間の間隔です。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、switchで指定されて有効になっている必要があります。 詳細については、関連項目を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree mst hello-time** *seconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst hello-time** *seconds* 例： `Switch(config)# spanning-tree mst hello-time 4`	すべての MST インスタンスについて、hello タイムを設定します。 hello タイムはルート switchによって設定メッセージが生成されて送信される時間の間隔です。 このメッセージは、switchが活動中であることを表します。 *seconds* に指定できる範囲は 1 ～ 10 です。デフォルトは 3 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）

転送遅延時間の設定

はじめる前に

マルチ スパニングツリー（MST）が、switchで指定されて有効になっている必要があります。 詳細については、関連項目を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree mst forward-time** *seconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst forward-time** *seconds* 例： `Switch(config)# spanning-tree mst forward-time 25`	すべての MST インスタンスについて、転送時間を設定します。 転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、ポートが待機する秒数です。 *seconds* に指定できる範囲は 4 ～ 30 です。デフォルトは 20 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）

最大エージング タイムの設定

はじめる前に

マルチ スパニングツリー（MST）が、switchで指定されて有効になっている必要があります。 詳細については、関連項目を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree mst max-age** *seconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst max-age** *seconds* 例： `Switch(config)# spanning-tree mst max-age 40`	すべての MST インスタンスについて、最大エージング タイムを設定します。 最大エージング タイムは、switchが再設定を試す前にスパニングツリー設定メッセージを受信せずに待機する秒数です。 *seconds* に指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）

最大ホップ カウントの設定

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、switchで指定されて有効になっている必要があります。 詳細については、関連項目を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree mst max-hops** *hop-count*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree mst max-hops** *hop-count* 例： `Switch(config)# spanning-tree mst max-hops 25`	BPDU を廃棄してポート用に保持していた情報を期限切れにするまでの、リージョンでのホップ数を設定します。 *hop-count* に指定できる範囲は 1 ～ 255 です。デフォルト値は 20 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）

高速移行を確実にするためのリンク タイプの指定

ポイントツーポイント リンクでポート間を接続し、ローカル ポートが DP になると、RSTP は提案と合意のハンドシェークを使用して別のポートと高速移行をネゴシエーションし、ループがないトポロジーを保証します。

デフォルトの場合、リンク タイプはインターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続、半二重ポートは共有接続と見なされます。MSTP を実行しているリモート switchの単一ポートに、半二重リンクを物理的にポイントツーポイントで接続した場合は、リンク タイプのデフォルト設定を無効にして、フォワーディング ステートへの高速移行をイネーブルにすることができます。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、switchで指定されて有効になっている必要があります。 詳細については、関連項目を参照してください。

指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。 この例では、インスタンス ID として 0 を使用し、インターフェイスとして GigabitEthernet1/0/1 を使用します。これは「関連項目」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **spanning-tree link-type point-to-point**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface GigabitEthernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポート、VLAN、およびポート チャネル論理インターフェイスがあります。 VLAN ID の範囲は 1 ～ 4094 です。 ポート チャネル範囲は 1 ～ 48 です。
ステップ 4	**spanning-tree link-type point-to-point** 例： `Switch(config-if)# spanning-tree link-type point-to-point`	ポートのリンク タイプがポイントツーポイントであることを指定します。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）

ネイバー タイプの設定

トポロジには、先行標準に準拠したデバイスと IEEE 802.1s 標準準拠のデバイスの両方を加えることができます。 デフォルトの場合、ポートは準規格デバイスを自動的に検出できますが、規格 BPDU および準規格 BPDU の両方を受信できます。 デバイスとそのネイバーの間に不一致がある場合は、CIST だけがインターフェイスで動作します。

準規格 BPDU だけを送信するようにポートを設定できます。 ポートが STP 互換モードになっていても、すべての **show** コマンドで準規格フラグが表示されます。

この手順は任意です。

はじめる前に

マルチ スパニングツリー（MST）が、switchで指定されて有効になっている必要があります。 詳細については、関連項目を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **spanning-tree mst pre-standard**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface GigabitEthernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	**spanning-tree mst pre-standard** 例： `Switch(config-if)# spanning-tree mst pre-standard`	ポートが準規格 BPDU だけを送信できることを指定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）

プロトコルの移行プロセスの再開

この手順では、プロトコル移行プロセスを再開し、ネイバーswitchesとの再ネゴシエーションを強制します。 また、switchをMSTモードに戻します。 これは、IEEE 802.1D BPDUの受信後にswitchがそれらを受信しない場合に必要です。

switchでプロトコルの移行プロセスを再開する（隣接するswitchesで再ネゴシエーションを強制的に行う）手順については、これらの手順に従ってください。

はじめる前に

マルチ スパニングツリー（MST）が、switchで指定されて有効になっている必要があります。 詳細については、関連項目を参照してください。

コマンドのインターフェイス バージョンを使用する場合は、使用する MST インターフェイスが分かっている必要があります。 この例では、インターフェイスとして GigabitEthernet1/0/1 を使用します。それが「関連項目」で示されている手順によって設定されたインターフェイスであるからです。

手順の概要

1. **enable**
2. 次のいずれかのコマンドを入力します。
   - **clear spanning-tree detected-protocols**
   - **clear spanning-tree detected-protocols interface** *interface-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

ステップ 2	次のいずれかのコマンドを入力します。
	• **clear spanning-tree detected-protocols**
	• **clear spanning-tree detected-protocols interface** *interface-id*
	
	例：
	`Switch# clear spanning-tree detected-protocols`
	または
	`Switch# clear spanning-tree detected-protocols interface GigabitEthernet1/0/1`
		switchが MSTP モードに戻り、プロトコルの移行プロセスが再開されます。

次の作業

この手順は、switchでさらにレガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコル バージョンが 0 に設定された BPDU）を受信する場合に、繰り返しが必要なことがあります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化，（56 ページ）
プロトコル移行プロセス，（54 ページ）

MST の設定およびステータスのモニタリング

表 *10*：*MST* ステータスを表示するコマンド

show spanning-tree mst configuration	MST リージョンの設定を表示します。
show spanning-tree mst configuration digest	現在の MSTCI に含まれる MD5 ダイジェストを表示します。

このコマンドは、リンク アップ動作可能状態のポートの情報を表示します。	すべてのインスタンスの MST 情報を表示します。 （注） このコマンドは、リンク アップ動作可能状態のポートの情報を表示します。 このコマンドは、リンク アップ動作可能状態のポートの情報を表示します。
show spanning-tree mst *instance-id*	指定インスタンスの MST 情報を表示します。 （注） このコマンドは、ポートがリンク アップ動作可能状態の場合にのみ情報を表示します。
show spanning-tree mst interface *interface-id*	指定インターフェイスの MST 情報を表示します。

MSTP に関する追加情報

関連資料

関連項目	マニュアル タイトル
スパニング ツリー プロトコル コマンド	*LAN Switching Command Reference, Cisco IOS XE Release 3SE（Catalyst 3850 Switches）*

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

MSTP の機能情報

リリース	変更内容
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	この機能が導入されました。

第 3 章

オプションのスパニングツリー機能の設定

- 機能情報の確認，79 ページ
- オプションのスパニング ツリー機能の制約事項，79 ページ
- オプションのスパニングツリー機能について，80 ページ
- オプションのスパニングツリー機能の設定方法，91 ページ
- スパニングツリー ステータスのモニタリング，105 ページ
- オプションのスパニング ツリー機能に関する追加情報，106 ページ
- オプションのスパニングツリー機能の機能情報，107 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

オプションのスパニング ツリー機能の制約事項

- PortFast は、スパニング ツリーがコンバージェンスするまでにインターフェイスが待機する時間を最短にするため、これはエンドステーションに接続されているインターフェイスで使用される場合のみ有用です。 他のスイッチに接続するインターフェイスで PortFast をイネーブルにすると、スパニングツリーのループが生じることがあります。

- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

関連トピック

PortFast のイネーブル化, （91 ページ）
PortFast, （80 ページ）

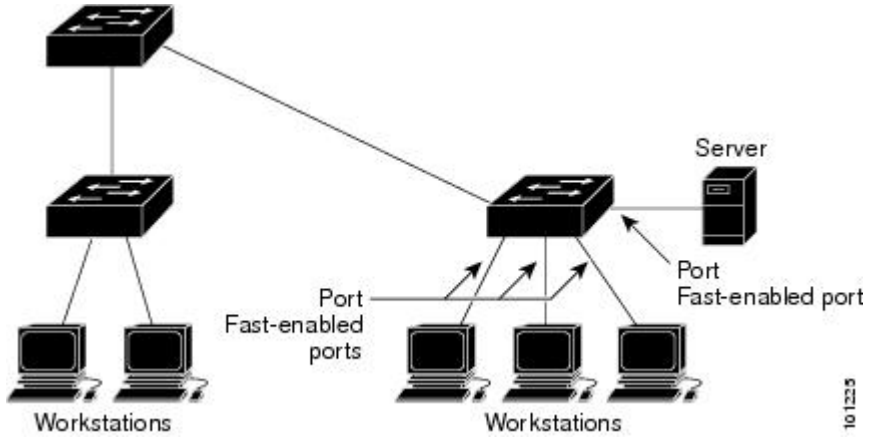
オプションのスパニングツリー機能について

PortFast

PortFast機能を使用すると、アクセス ポートまたはトランク ポートとして設定されているインターフェイスが、リスニング ステートおよびラーニング ステートを経由せずに、ブロッキング ステートから直接フォワーディング ステートに移行します。

1 台のワークステーションまたはサーバに接続されているインターフェイス上でPortFastを使用すると、スパニングツリーが収束するのを待たずにデバイスをすぐにネットワークに接続できます。

図 *10*：*PortFast* がイネーブルなインターフェイス



1 台のワークステーションまたはサーバに接続されたインターフェイスがブリッジ プロトコル データ ユニット（BPDU）を受信しないようにする必要があります。 スイッチを再起動すると、PortFast がイネーブルに設定されているインターフェイスは通常のスパニングツリー ステータスの遷移をたどります。

インターフェイスまたはすべての非トランク ポートでイネーブルにして、この機能をイネーブルにできます。

関連トピック

PortFast のイネーブル化, （91 ページ）

オプションのスパニング ツリー機能の制約事項, （79 ページ）

BPDU ガード

ブリッジプロトコルデータユニット（BPDU）ガード機能はスイッチ上でグローバルにイネーブルにすることも、ポート単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

PortFast 対応ポート上でグローバル レベルで BPDU ガードをイネーブルにすると、スパニングツリーは、BPDU が受信されると、PortFast 動作ステートのポートをシャット ダウンします。 設定が有効であれば、PortFast 対応ポートは BPDU を受信しません。 PortFast 対応ポートが BPDU を受信した場合は、認可されていないデバイスの接続などの無効な設定が存在することを示しており、BPDU ガード機能によってポートは errdisable ステートになります。 この状態になると、スイッチは違反が発生したポート全体をシャットダウンします。

PortFast 機能もイネーブルにせずにインターフェイス レベルでポート上の BPDU ガードをイネーブルにした場合、ポートが BPDU を受信すると、errdisable ステートになります。

インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。 サービスプロバイダー ネットワーク内でアクセス ポートがスパニングツリーに参加しないようにするには、BPDU ガード機能を使用します。

関連トピック

BPDU ガードのイネーブル化, （93 ページ）

BPDU フィルタリング

BPDU フィルタリング機能はスイッチ上でグローバルにイネーブルにすることも、インターフェイス単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

グローバル レベルで PortFast がイネーブルなインターフェイス上の BPDU フィルタリングをイネーブルにすると、PortFast 動作状態にあるインターフェイスでの BPDU の送信または受信が防止されます。 ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。 これらのインターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。 BPDU を受信した PortFast がイネーブルなインターフェイスでは PortFast 動作ステータスが解除され、BPDU フィルタリングがディセーブルになります。

PortFast 機能をイネーブルにせずに、インターフェイスで BPDU フィルタリングをイネーブルにすると、インターフェイスでの BPDU の送信または受信が防止されます。

注意 BPDUフィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリーループが発生することがあります。

スイッチ全体または 1 つのインターフェイスで BPDU フィルタリング機能をイネーブルにできます。

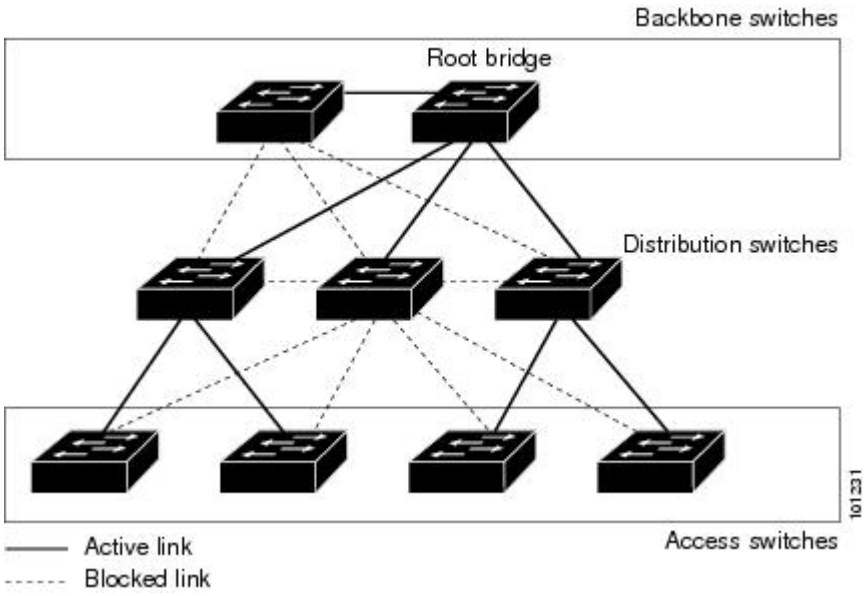
関連トピック

BPDU フィルタリングのイネーブル化, （95 ページ）

UplinkFast

階層型ネットワークに配置されたスイッチは、バックボーン スイッチ、ディストリビューション スイッチ、およびアクセス スイッチに分類できます。 この複雑なネットワークには、ディストリビューション スイッチとアクセス スイッチがあり、ループを防止するために、スパニング ツリーがブロックする冗長リンクが少なくとも 1 つあります。

図 *11*：階層型ネットワークのスイッチ



スイッチの接続が切断されると、スイッチはスパニングツリーが新しいルート ポートを選択すると同時に代替パスの使用を開始します。 リンクやスイッチに障害が発生した場合、またはスパニングツリーが UplinkFast のイネーブル化によって自動的に再設定された場合に、新しいルート ポートを短時間で選択できます。 ルート ポートは、通常のスパニングツリー手順とは異なり、リスニング ステートおよびラーニング ステートを経由せず、ただちにフォワーディング ステートに移行します。

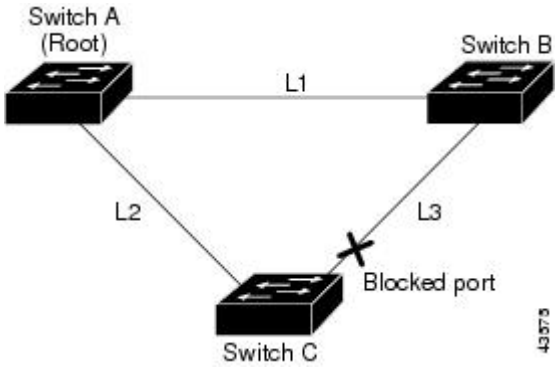
スパニングツリーが新規ルート ポートを再設定すると、他のインターフェイスはネットワークにマルチキャスト パケットをフラッディングし、インターフェイス上で学習した各アドレスにパケットを送信します。 max-update-rate パラメータの値を小さくすることで、これらのマルチキャスト トラフィックのバーストを制限できます（このパラメータはデフォルトで毎秒 150 パケットです）。 ただし、0 を入力すると、ステーション学習フレームが生成されないので、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。

（注） UplinkFastは、ネットワークのアクセスまたはエッジに位置する、ワイヤリング クローゼットのスイッチで非常に有効です。 バックボーン デバイスには適していません。 他のアプリケーションにこの機能を使用しても、有効とは限りません。

UplinkFast は、直接リンク障害発生後に高速コンバージェンスを行い、アップリンク グループを使用して、冗長レイヤ 2 リンク間でロード バランシングを実行します。 アップリンク グループは、（VLAN ごとの）レイヤ 2 インターフェイスの集合であり、いかなるときも、その中の 1 つのインターフェイスだけが転送を行います。 つまり、アップリンク グループは、（転送を行う）ルート ポートと、（セルフループを行うポートを除く）ブロックされたポートの集合で構成されます。アップリンク グループは、転送中のリンクで障害が起きた場合に代替パスを提供します。

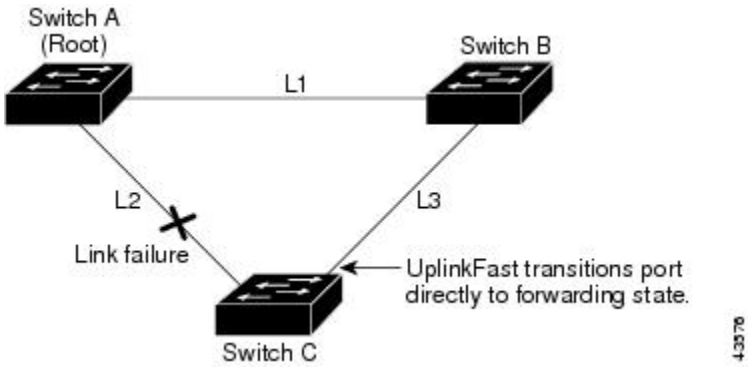
このトポロジにはリンク障害がありません。 ルート スイッチであるスイッチ A は、リンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。 スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

図 *12*：直接リンク障害が発生する前の *UplinkFast* の例



スイッチ C が、ルート ポートの現在のアクティブ リンクである L2 でリンク障害（直接リンク障害）を検出すると、UplinkFast がスイッチ C でブロックされていたインターフェイスのブロックを解除し、リスニング ステートおよびラーニング ステートを経由せずに、直接フォワーディング ステートに移行させます。 この切り替えに必要な時間は、約 1 ～ 5 秒です。

図 *13*：直接リンク障害が発生したあとの *UplinkFast* の例



関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）
MSTP 設定時の注意事項, （38 ページ）
MST リージョン, （40 ページ）
冗長リンクで使用するための UplinkFast のイネーブル化, （97 ページ）
高速コンバージェンスを発生させるイベント, （86 ページ）

クロススタック UplinkFast

クロススタック UplinkFast（CSUF）は、スイッチ スタック全体にスパニングツリー高速移行（通常のネットワーク状態の下では 1 秒未満の高速コンバージェンス）を提供します。 高速移行の間は、スタック上の代替冗長リンクがフォワーディング ステートになり、一時的なスパニングツリー ループもバックボーンへの接続の損失も発生させません。 一部の設定では、この機能により、冗長性と復元力を備えたネットワークが得られます。 CSUF は UplinkFast 機能をイネーブルにすると、自動的にイネーブルになります。

CSUF で高速移行が得られない場合もあります。この場合は、通常のスパニングツリー移行が発生し、30 ～ 40 秒以内に完了します。 詳細については、「関連項目」を参照してください。

関連トピック

冗長リンクで使用するための UplinkFast のイネーブル化, （97 ページ）
高速コンバージェンスを発生させるイベント, （86 ページ）

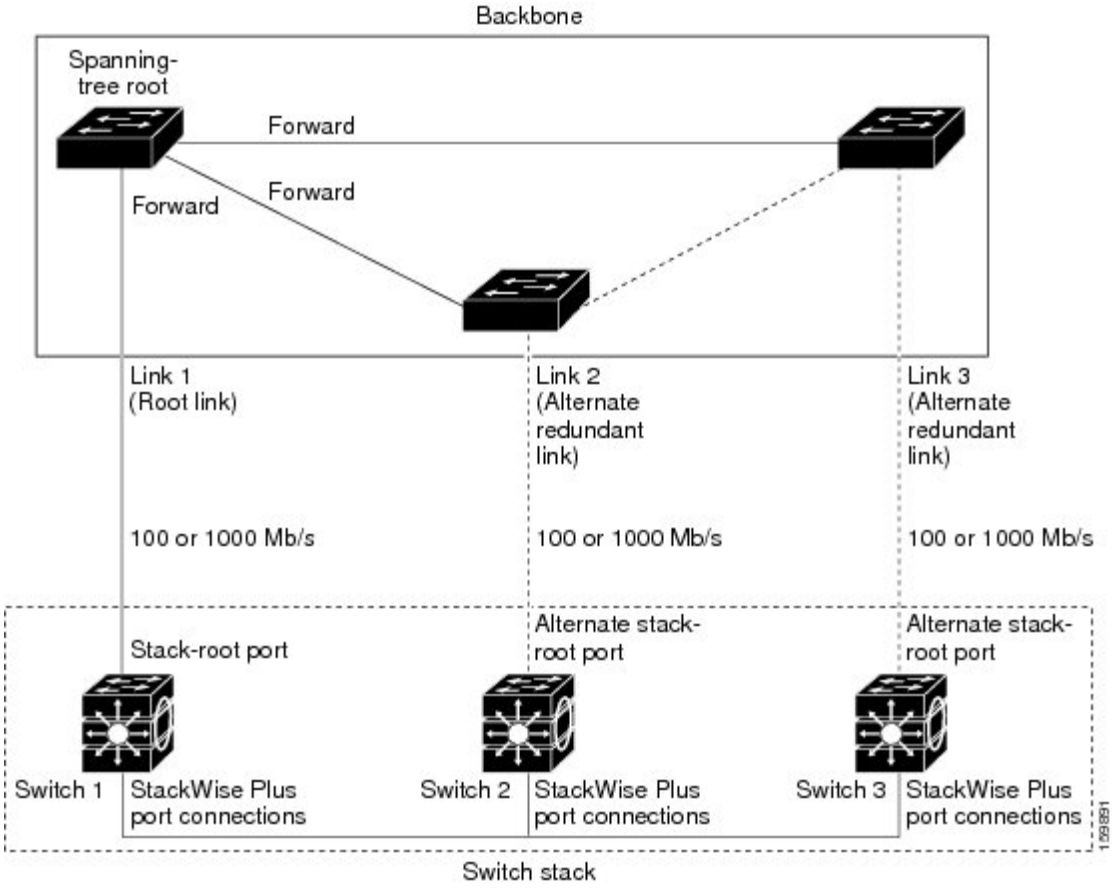
クロススタック UplinkFast の動作

クロススタック UplinkFast（CSUF）によって、ルートへのパスとしてスタック内で 1 つのリンクが確実に選択されます。

スイッチ 1 のスタック ルート ポートは、スパニングツリーのルートへパスを提供しています。 スイッチ 2 およびスイッチ 3 の代替スタック ルート ポートは、現在のスタック ルート スイッチに障害が発生したか、またはそのスパニングツリー ルートへのリンクに障害が発生した場合に、スパニングツリー ルートへの代替パスを提供できます。

ルート リンクである Link 1 は、スパニングツリー フォワーディング ステートになっています。 Link 2 と Link 3 は、スパニングツリー ブロッキング ステートになっている代替冗長リンクです。 スイッチ 1 に障害が発生したか、そのスタック ルート ポートに障害が発生したか、または Link 1 に障害が発生した場合には、CSUF が、1 秒未満でスイッチ 2 またはスイッチ 3 のいずれかにある代替スタック ルート ポートを選択して、それをフォワーディング ステートにします。

図 *14* : クロススタック *UplinkFast* トポロジ



特定のリンク損失またはスパニングツリーイベントが発生した場合（次のトピックを参照）、Fast Uplink Transition Protocol は、ネイバー リストを使用して、高速移行要求をスタック メンバーに送信します。

高速移行要求を送信するスイッチは、ルート ポートとして選択されたポートをフォワーディング ステートへ高速移行する必要があります。また、高速移行を実行するには、事前に各スタックから確認応答を取得しておく必要があります。

スタック内の各スイッチが、ルート、コスト、およびブリッジ ID を比較することにより、このスパニングツリーインスタンスのスタック ルートとなるよりも送信スイッチの方がよりよい選択肢であるかどうかを判断します。 スタック ルートとして送信スイッチが最も良い選択である場合は、スタック内の各スイッチが確認応答を返します。それ以外の場合は、高速移行要求を送信します。 この時点では、送信スイッチは、すべてのスタック スイッチから確認応答を受け取っていません。

すべてのスタック スイッチから確認応答を受け取ると、送信スイッチの Fast Uplink Transition Protocol は代替スタック ルート ポートをすぐにフォワーディング ステートに移行させます。 送信スイッチがすべてのスタック スイッチからの確認応答を取得しなかった場合、通常のスパニングツリー移行（ブロッキング、リスニング、ラーニング、およびフォワーディング）が行われ、ス

パニングツリー トポロジが通常のレート（2 × 転送遅延時間 + 最大エージング タイム）で収束します。

Fast Uplink Transition Protocol は、VLAN ごとに実装されており、一度に 1 つのスパニングツリー インスタンスにしか影響しません。

関連トピック

冗長リンクで使用するための UplinkFast のイネーブル化，（97 ページ）
高速コンバージェンスを発生させるイベント，（86 ページ）

高速コンバージェンスを発生させるイベント

CSUF 高速コンバージェンスは、ネットワーク イベントまたはネットワーク障害に応じて、発生する場合もあれば発生しない場合もあります。

高速コンバージェンス（通常のネットワーク状態で1秒未満）は、次のような状況で発生します。

- スタック ルート ポート リンクに障害が発生した。

  スタック内の 2 つのスイッチがルートへの代替パスを持つ場合、それらのスイッチの片方だけが高速移行を行います。

- スタック ルートをスパニングツリー ルートに接続するリンクに障害が発生し、回復した。
- ネットワークの再設定により、新しいスタックルート スイッチが選択された。
- ネットワークの再設定により、現在のスタックルート スイッチ上で新しいポートがスタック ルート ポートとして選択された。

（注） 複数のイベントが同時に発生すると、高速移行が行われなくなる場合もあります。 たとえば、スタック メンバの電源がオフになり、それと同時にスタック ルートをスパニングツリー ルートに接続しているリンクが回復した場合、通常のスパニングツリー コンバージェンスが発生します。

通常のスパニングツリー コンバージェンス（30 ～ 40 秒）は、次のような状況で発生します。

- スタック ルート スイッチの電源がオフになったか、またはソフトウェアに障害が発生した。
- 電源がオフになっていたか、または障害が発生していたスタック ルート スイッチの電源が入った。
- スタック ルートになる可能性のある新しいスイッチがスタックに追加された。

関連トピック

冗長リンクで使用するための UplinkFast のイネーブル化，（97 ページ）
UplinkFast，（82 ページ）
クロススタック UplinkFast，（84 ページ）

クロススタック UplinkFast の動作, （84 ページ）

BackboneFast

BackboneFastは、バックボーンのコアにおける間接障害を検出します。 BackboneFastは、UplinkFast機能を補完するテクノロジーです。UplinkFast は、アクセス スイッチに直接接続されたリンクの障害に対応します。 BackboneFastは、最大エージング タイマーを最適化します。最大エージングタイマーによって、スイッチがインターフェイスで受信したプロトコル情報を保存しておく時間の長さが制御されます。 スイッチが別のスイッチの指定ポートから下位BPDU を受信した場合、BPDUは他のスイッチでルートまでのパスが失われた可能性を示すシグナルとなり、BackboneFastはルートまでの別のパスを見つけようとします。

スイッチのルートポートまたはブロックされたインターフェイスが、指定スイッチから下位BPDUを受け取ると、BackboneFastが開始します。 下位BPDUは、ルートブリッジと指定スイッチの両方を宣言しているスイッチを識別します。 スイッチが下位BPDUを受信した場合、そのスイッチが直接接続されていないリンク（間接リンク）で障害が発生したことを意味します（指定スイッチとルートスイッチ間の接続が切断されています）。スパニングツリーのルールに従い、スイッチは最大エージング タイム（デフォルトは 20 秒）の間、下位 BPDU を無視します。

スイッチは、ルートスイッチへの代替パスの有無を判別します。 下位BPDUがブロックインターフェイスに到達した場合、スイッチ上のルート ポートおよび他のブロック インターフェイスがルート スイッチへの代替パスになります （セルフループ ポートは、ルート スイッチへの代替パスとは見なされません）。下位 BPDU がルート ポートに到達した場合、すべてのブロック インターフェイスがルートスイッチへの代替パスになります。 下位BPDUがルートポートに到達し、しかもブロックインターフェイスがない場合、スイッチはルートスイッチへの接続が切断されたものと見なし、ルートポートの最大エージングタイムが経過するまで待ち、通常のスパニングツリー ルールに従ってルート スイッチになります。

スイッチが代替パスでルート スイッチに到達できる場合、スイッチはその代替パスを使用して、Root Link Query（RLQ）要求を送信します。 スイッチは、スタック メンバーがルート スイッチへの代替ルートを持つかどうかを学習するために、すべての代替パスにRLQ要求を送信し、ネットワーク内およびスタック内の他のスイッチからの RLQ 応答を待機します。 スイッチは、すべての代替パスにRLQ要求を送信し、ネットワーク内の他のスイッチからのRLQ応答を待機します。

スタック メンバが、ブロック インターフェイス上の非スタック メンバから RLQ 応答を受信し、その応答が他の非スタックスイッチ宛てのものであった場合、そのスタックメンバは、スパニングツリー インターフェイス ステートに関係なく、その応答パケットを転送します。

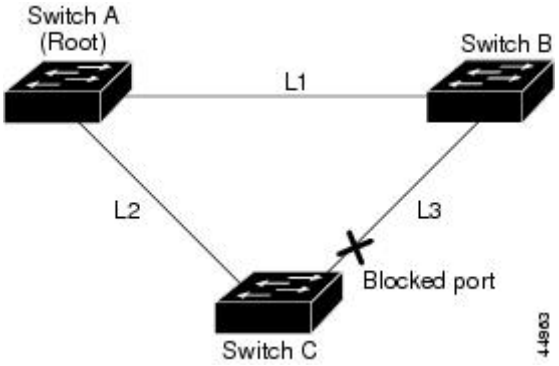
スタック メンバが非スタック メンバから RLQ 応答を受信し、その応答がスタック宛てのものであった場合、そのスタックメンバは、他のすべてのスタックメンバがその応答を受信するようにその応答を転送します。

ルートへの代替パスがまだ存在していると判断したスイッチは、下位 BPDU を受信したインターフェイスの最大エージング タイムが経過するまで待ちます。 ルート スイッチへのすべての代替パスが、スイッチとルート スイッチ間の接続が切断されていることを示している場合、スイッチは RLQ 応答を受信したインターフェイスの最大エージング タイムを満了させます。 1 つまたは複数の代替パスからルート スイッチへ引き続き接続できる場合、スイッチは下位BPDUを受信したすべてのインターフェイスを指定ポートにして、（ブロッキング ステートになっていた場合）

ブロッキング ステートを解除し、リスニング ステート、ラーニング ステートを経てフォワーディング ステートに移行させます。

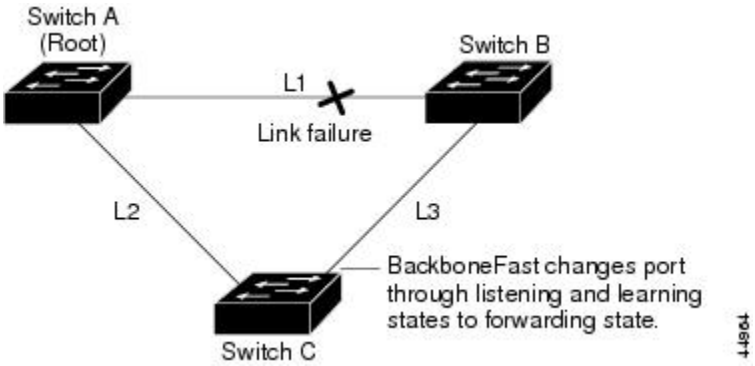
これは、リンク障害が発生していないトポロジー例です。 ルート スイッチであるスイッチ A はリンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。 スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

図 *15*：間接リンク障害が発生する前の *BackboneFast* の例



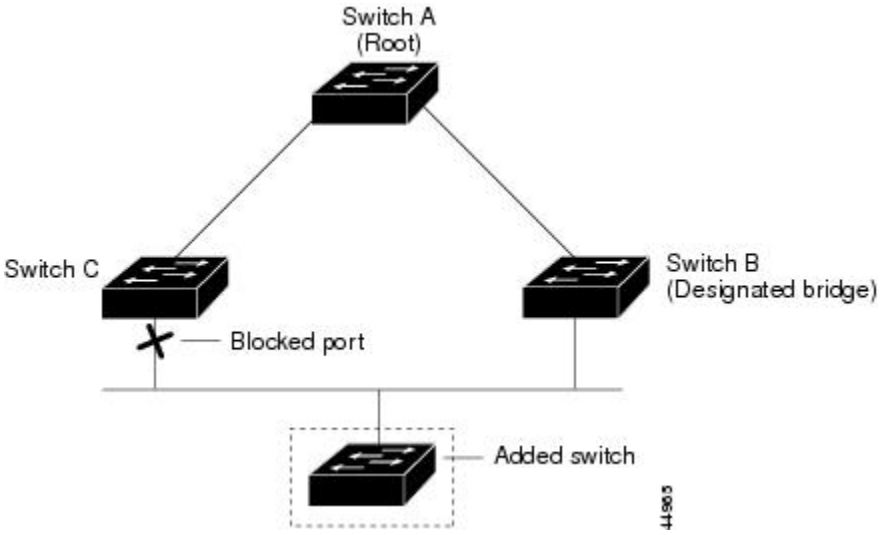
リンク L1 で障害が発生した場合、スイッチ C はリンク L1 に直接接続されていないので、この障害を検出できません。 一方スイッチ B は、L1 によってルート スイッチに直接接続されているため障害を検出し、スイッチ B 自身をルートとして選定して、自らをルートとして特定した状態で BPDU をスイッチ C へ送信し始めます。 スイッチ B から下位 BPDU を受信したスイッチ C は、間接障害が発生していると見なします。 この時点で、BackboneFast は、スイッチ C のブロック インターフェイスを、インターフェイスの最大エージング タイムが満了するまで待たずに、ただちにリスニング ステートに移行させます。 BackboneFast は、次に、スイッチ C のレイヤ 2 インターフェイスをフォワーディング ステートに移行させ、スイッチ B からスイッチ A へのパスを設定します。 ルートスイッチの選択には約 30 秒必要です。これは転送遅延時間がデフォルトの 15 秒に設定されていればその倍の時間です。 BackboneFast がリンク L1 で発生した障害に応じてトポロジーを再設定します。

図 *16*：間接リンク障害が発生したあとの *BackboneFast* の例



新しいスイッチがメディア共有型トポロジーに組み込まれた場合、認識された指定スイッチ（スイッチ B）から下位 BPDU が届いていないので、BackboneFast はアクティブになりません。 新しいスイッチは、自身がルート スイッチであることを伝える下位 BPDU の送信を開始します。 ただし、他のスイッチはこれらの下位 BPDU を無視し、新しいスイッチはスイッチ B がルート スイッチであるスイッチ A への指定スイッチであることを学習します。

図 *17*：メディア共有型トポロジにおけるスイッチの追加



関連トピック

MST リージョン設定の指定と MSTP のイネーブル化, （56 ページ）
MSTP 設定時の注意事項, （38 ページ）
MST リージョン, （40 ページ）
BackboneFast をイネーブル化, （99 ページ）

EtherChannel ガード

EtherChannel ガードを使用すると、スイッチと接続したデバイス間での EtherChannel の設定の矛盾を検出できます。 スイッチ インターフェイスは EtherChannel として設定されているものの、もう一方のデバイスのインターフェイスではその設定が行われていない場合、設定の矛盾が発生します。 また、EtherChannel の両端でチャネルのパラメータが異なる場合にも、設定の矛盾が発生します。

スイッチが、他のデバイス上で設定の矛盾を検出した場合、EtherChannel ガードは、スイッチのインターフェイスを errdisable ステートにし、エラー メッセージを表示します。

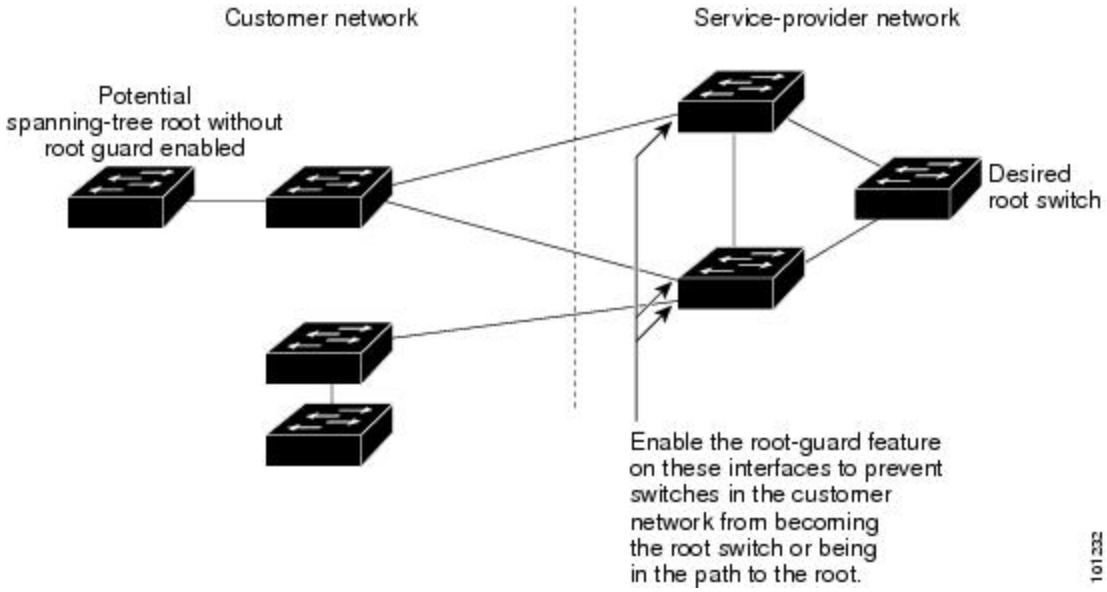
関連トピック

EtherChannel ガードのイネーブル化, （101 ページ）

ルート ガード

サービス プロバイダー（SP）のレイヤ 2 ネットワークには、SP 以外が所有するスイッチへの接続が多く含まれている場合があります。 このようなトポロジでは、スパニングツリーが再構成され、カスタマー スイッチをルート スイッチとして選択する可能性があります。 この状況を防ぐには、カスタマー ネットワーク内のスイッチに接続する SP スイッチ インターフェイス上でルート ガード機能をイネーブルに設定します。 スパニングツリーの計算によってカスタマー ネットワーク内のインターフェイスがルート ポートとして選択されると、ルート ガードがそのインターフェイスを root-inconsistent（ブロッキング）ステートにして、カスタマーのスイッチがルート スイッチにならないようにするか、ルートへのパスに組み込まれないようにします。

図 *18*：サービス プロバイダー ネットワークのルート ガード



SP ネットワーク外のスイッチがルート スイッチになると、インターフェイスがブロックされ（root-inconsistent ステートになり）、スパニングツリーが新しいルート スイッチを選択します。カスタマーのスイッチがルート スイッチになることはありません。ルートへのパスに組み込まれることもありません。

スイッチが MST モードで動作している場合、ルート ガードが強制的にそのインターフェイスを指定ポートにします。 また、境界ポートがルート ガードによって Internal Spanning-Tree（IST）インスタンスでブロックされている場合にも、このインターフェイスはすべての MST インスタンスでもブロックされます。 境界ポートは、指定スイッチが IEEE 802.1D スイッチまたは異なる MST リージョン設定を持つスイッチのいずれかである LAN に接続されるインターフェイスです。

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。 VLAN は、MST インスタンスに対してグループ化された後、マッピングされます。

注意 ルート ガード機能を誤って使用すると、接続が切断されることがあります。

関連トピック

ルート ガードのイネーブル化, （102 ページ）

ループ ガード

ループ ガードを使用すると、代替ポートまたはルートポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。 この機能は、スイッチド ネットワーク全体でイネーブルにした場合に最も効果があります。 ループ ガードによって、代替ポートおよびルートポートが指定ポートになることが防止され、スパニングツリーがルート ポートまたは代替ポートで BPDU を送信することはありません。

スイッチが PVST+ または Rapid PVST+ モードで動作している場合、ループ ガードによって、代替ポートおよびルート ポートが指定ポートになることが防止され、スパニングツリーがルートポートまたは代替ポートで BPDU を送信することはありません。

スイッチが MST モードで動作しているとき、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされている場合でのみ、非境界ポートで BPDU を送信しません。境界ポートでは、ループ ガードがすべての MST インスタンスでインターフェイスをブロックします。

関連トピック

ループ ガードのイネーブル化, （103 ページ）

オプションのスパニングツリー機能の設定方法

PortFast のイネーブル化

PortFast機能がイネーブルに設定されているインターフェイスは、標準の転送遅延時間の経過を待たずに、すぐにスパニングツリー フォワーディング ステートに移行されます。

音声 VLAN 機能をイネーブルにすると、PortFast 機能が自動的にイネーブルになります。 音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

注意 PortFast を使用するのは、1 つのエンド ステーションがアクセス ポートまたはトランク ポートに接続されている場合に限定されます。 スイッチまたはハブに接続するインターフェイス上でこの機能をイネーブルにすると、スパニングツリーがネットワーク ループを検出または阻止できなくなり、その結果、ブロードキャスト ストームおよびアドレス ラーニングの障害が起きる可能性があります。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **spanning-tree portfast** [**trunk**]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**spanning-tree portfast** [**trunk**] 例： `Switch(config-if)#`	単一ワーク ステーションまたはサーバに接続されたアクセス ポート上で PortFast をイネーブルにします。 **trunk** キーワードを指定すると、トランク ポート上で PortFast をイネーブルにできます。

	コマンドまたはアクション	目的
	spanning-tree portfast trunk	（注） トランク ポートで PortFast をイネーブルにするには、**spanning-tree portfast trunk** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**spanning-tree portfast** コマンドは、トランク ポート上では機能しないためです。 トランク ポート上で PortFast をイネーブルにする場合は、事前に、トランク ポートとワークステーションまたはサーバの間にループがないことを確認してください。 デフォルトでは、PortFast はすべてのインターフェイスでディセーブルです。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

次の作業

spanning-tree portfast default グローバル コンフィギュレーション コマンドを使用すると、すべての非トランク ポート上で PortFast 機能をグローバルにイネーブルにできます。

関連トピック

PortFast, （80 ページ）
オプションのスパニング ツリー機能の制約事項, （79 ページ）

BPDU ガードのイネーブル化

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU ガード機能をイネーブルにできます。

注意 PortFast は、エンド ステーションに接続するポートのみに設定します。それ以外に設定すると、予期しないトポロジ ループが原因でデータのパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree portfast bpduguard default**
4. **interface** *interface-id*
5. **spanning-tree portfast**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree portfast bpduguard default** 例： `Switch(config)# spanning-tree portfast bpduguard default`	BPDU ガードをグローバルにイネーブルにします。 BPDU ガードは、デフォルトではディセーブルに設定されています。
ステップ 4	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	エンド ステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**spanning-tree portfast** 例： `Switch(config-if)# spanning-tree portfast`	PortFast 機能をイネーブルにします。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

次の作業

ポートのシャットダウンを防ぐには、**errdisable detect cause bpduguard shutdown vlan** グローバル コンフィギュレーション コマンドを使用すると、違反の発生時にポートで問題になっている VLAN のみをシャットダウンできます。

PortFast 機能をイネーブルにしなくても、**spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のポートで BPDU ガードをイネーブルにすることもできます。 BPDU を受信したポートは、errdisable ステートになります。

関連トピック

BPDU ガード, （81 ページ）

BPDU フィルタリングのイネーブル化

PortFast 機能をイネーブルにしなくても、**spanning-tree bpdufilter enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のインターフェイスで BPDU フィルタリングをイネーブルにすることもできます。 このコマンドを実行すると、インターフェイスは BPDU を送受信できなくなります。

注意 BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリー ループが発生することがあります。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU フィルタリング機能をイネーブルにできます。

注意 PortFast は、エンド ステーションに接続するインターフェイスのみに設定します。それ以外に設定すると、予期しないトポロジ ループが原因でデータのパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree portfast bpdufilter default**
4. **interface** *interface-id*
5. **spanning-tree portfast**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree portfast bpdufilter default** 例： `Switch(config)# spanning-tree portfast bpdufilter default`	BPDU フィルタリングをグローバルにイネーブルにします。 BPDU フィルタリングは、デフォルトではディセーブルに設定されています。
ステップ 4	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	エンド ステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**spanning-tree portfast** 例： `Switch(config-if)# spanning-tree portfast`	指定したインターフェイスで PortFast 機能をイネーブルにします。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

BPDU フィルタリング, （81 ページ）

冗長リンクで使用するための UplinkFast のイネーブル化

（注） UplinkFast をイネーブルにすると、スイッチまたはスイッチ スタックのすべての VLAN に影響します。 個々の VLAN について UplinkFast を設定することはできません。

Rapid PVST+ または MSTP に対して UplinkFast または Cross-Stack UplinkFast（CSUF）機能を設定できますが、この機能は、スパニングツリーのモードを PVST+ に変更するまではディセーブル（非アクティブ）になったままです。

この手順は任意です。 UplinkFast および CSUF をイネーブルにするには、次の手順に従います。

はじめる前に

スイッチ プライオリティが設定されている VLAN 上で UplinkFast をイネーブルにすることはできません。 スイッチ プライオリティが設定されている VLAN 上で UplinkFast をイネーブルにする場合は、最初に **no spanning-tree vlan** *vlan-id* **priority** グローバル コンフィギュレーション コマンドを使用することによって、VLAN のスイッチ プライオリティをデフォルト値に戻す必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree uplinkfast** [**max-update-rate** *pkts-per-second*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree uplinkfast** [**max-update-rate** *pkts-per-second*]	UplinkFast をイネーブルにします。 （任意）*pkts-per-second* に指定できる範囲は毎秒 0 ～ 32000 パケットです。デフォルト値は 150 です。

	コマンドまたはアクション	目的
	例： `Switch(config)# spanning-tree uplinkfast max-update-rate 200`	0 を入力すると、ステーション学習フレームが生成されないので、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。 このコマンドを入力すると、すべての非スタック ポート インターフェイス上で CSUF もイネーブルになります。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチ プライオリティは 49152 に設定されます。 UplinkFast をイネーブルにする場合、または UplinkFast がすでにイネーブルに設定されている場合に、パス コストを 3000 未満の値に変更すると、すべてのインターフェイスおよび VLAN トランクのパス コストが 3000 だけ増加します（パス コストを 3000 以上の値に変更した場合、パス コストは変更されません）。 スイッチ プライオリティおよびパス コストを変更すると、スイッチがルート スイッチになる可能性が低くなります。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

次の手順に従って UplinkFast 機能をイネーブルにすると、CSUF は非スタック ポート インターフェイスで自動的にグローバルにイネーブルになります。

関連トピック

UplinkFast, （82 ページ）
クロススタック UplinkFast, （84 ページ）
クロススタック UplinkFast の動作, （84 ページ）
高速コンバージェンスを発生させるイベント, （86 ページ）

UplinkFast のディセーブル化

この手順は任意です。

UplinkFast および Cross-Stack UplinkFast（SUF）をディセーブルにするには、次の手順に従います。

はじめる前に

UplinkFast を有効にする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **no spanning-tree uplinkfast**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no spanning-tree uplinkfast** 例： `Switch(config)# no spanning-tree uplinkfast`	スイッチおよびそのスイッチのすべての VLAN で UplinkFast および CSUF をディセーブルにします。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

次の手順に従って UplinkFast 機能をディセーブルにすると、CSUF は非スタック ポート インターフェイスで自動的にグローバルにディセーブルになります。

BackboneFast をイネーブル化

BackboneFast をイネーブルにすると、間接リンク障害を検出し、スパニングツリーの再構成をより早く開始できます。

Rapid PVST+ または MSTP に対して BackboneFast 機能を設定できます。ただし、スパニングツリーモードを PVST+ に変更するまで、この機能はディセーブル（非アクティブ）のままです。

この手順は任意です。 スイッチ上で BackboneFast をイネーブルにするには、次の手順に従います。

はじめる前に

BackboneFast を使用する場合は、ネットワーク上のすべてのスイッチでイネーブルする必要があります。 BackboneFast は、トークンリング VLAN ではサポートされません。 この機能は他社製スイッチでの使用にサポートされています。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree backbonefast**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree backbonefast** 例： `Switch(config)# spanning-tree backbonefast`	BackboneFast をイネーブルにします。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

BackboneFast, （87 ページ）

EtherChannel ガードのイネーブル化

switchで PVST+、Rapid PVST+、または MSTP が稼働している場合、EtherChannel の設定の矛盾を検出する EtherChannel ガード機能をイネーブルにできます。

この手順は任意です。

switchで EtherChannel ガードをイネーブルにするには、次の手順に従います。

手順の概要

1. **enable**
2. **configure terminal**
3. **spanning-tree etherchannel guard misconfig**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree etherchannel guard misconfig** 例： `Switch(config)# spanning-tree etherchannel guard misconfig`	EtherChannel ガードをイネーブルにします。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

次の作業

show interfaces status err-disabled 特権 EXEC コマンドを使用することで、EtherChannel の設定矛盾が原因でディセーブルになっているswitch ポートを表示できます。 リモート デバイス上では、**show etherchannel summary** 特権 EXEC コマンドを使用して、EtherChannel の設定を確認できます。

設定を修正した後、誤って設定していたポート チャネル インターフェイス上で、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してください。

関連トピック

EtherChannel ガード, （89 ページ）

ルート ガードのイネーブル化

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。 UplinkFast 機能が使用するインターフェイスで、ルート ガードをイネーブルにしないでください。 UplinkFast を使用すると、障害発生時に（ブロック ステートの）バックアップ インターフェイスがルート ポートになります。 ただし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップ インターフェイスが root-inconsistent（ブロック）ステートになり、フォワーディング ステートに移行できなくなります。

（注） ルート ガードとループ ガードの両方を同時にイネーブルにすることはできません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

この手順は任意です。

スイッチ上でルート ガードをイネーブルにするには、次の手順に従います。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **spanning-tree guard root**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**spanning-tree guard root** 例： `Switch(config-if)# spanning-tree guard root`	インターフェイス上でルート ガードをイネーブルにします。 デフォルトでは、ルート ガードはすべてのインターフェイスでディセーブルです。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

ルート ガード, （90 ページ）

ループ ガードのイネーブル化

ループ ガードを使用すると、代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。 この機能は、スイッチド ネットワーク全体に設定した場合に最も効果があります。 ループ ガードは、スパニングツリーがポイントツーポイントと見なすインターフェイス上でのみ動作します。

（注） ループ ガードとルート ガードの両方を同時にイネーブルにすることはできません。

switchでPVST+、Rapid PVST+、またはMSTPが稼働している場合、この機能をイネーブルにできます。

この手順は任意です。 switchでループ ガードをイネーブルにするには、次の手順に従います。

手順の概要

1. 次のいずれかのコマンドを入力します。
   - **show spanning-tree active**
   - **show spanning-tree mst**
2. **configure terminal**
3. **spanning-tree loopguard default**
4. **end**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	次のいずれかのコマンドを入力します。
	• **show spanning-tree active**
	• **show spanning-tree mst**
	
	例：
	`Switch# show spanning-tree active`
	または
	`Switch# show spanning-tree mst`
		どのインターフェイスが代替ポートまたはルート ポートであるかを確認します。

ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree loopguard default** 例： `Switch(config)# spanning-tree loopguard default`	ループ ガードをイネーブルにします。 ループ ガードは、デフォルトではディセーブルに設定されています。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

ループ ガード, （91 ページ）

スパニングツリー ステータスのモニタリング

表 *11*：スパニングツリー ステータスをモニタリングするコマンド

コマンド	目的
show spanning-tree active	アクティブインターフェイスに関するスパニングツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree mst interface *interface-id*	指定インターフェイスの MST 情報を表示します。
show spanning-tree summary [**totals**]	インターフェイス ステートのサマリーを表示します。またはスパニングツリー ステート セクションのすべての行を表示します。

オプションのスパニング ツリー機能に関する追加情報

関連資料

関連項目	マニュアル タイトル
スパニング ツリー プロトコル コマンド	*LAN Switching Command Reference, Cisco IOS XE Release 3SE（Catalyst 3850 Switches）*

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

オプションのスパニングツリー機能の機能情報

リリース	変更内容
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	この機能が導入されました。

第 4 章

EtherChannel の設定

- 機能情報の確認，109 ページ
- EtherChannel の制約事項，109 ページ
- EtherChannel について，110 ページ
- EtherChannel の設定方法，131 ページ
- EtherChannel、PAgP、および LACP ステータスのモニタ，146 ページ
- EtherChannel の設定例，147 ページ
- EtherChannels の追加リファレンス，149 ページ
- EtherChannels の機能情報，150 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

EtherChannel の制約事項

次に、EtherChannels の制約事項を示します。

- EtherChannel のすべてのポートは同じ VLAN に割り当てるか、またはトランク ポートとして設定する必要があります。

- LAN Base ライセンス フィーチャ セットを実行している場合は、レイヤ 3 EtherChannels はサポートされません。
- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

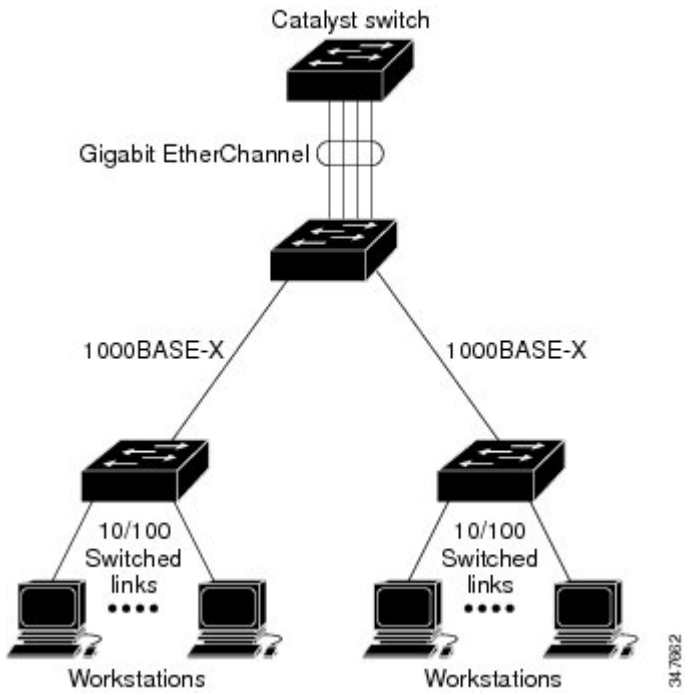
EtherChannel について

EtherChannel の概要

EtherChannel は、スイッチ、ルータ、およびサーバ間にフォールトトレラントな高速リンクを提供します。 EtherChannel を使用して、ワイヤリング クローゼットとデータセンター間の帯域幅を増やすことができます。さらに、ボトルネックが発生しやすいネットワーク上のあらゆる場所に EtherChannel を配置できます。 EtherChannel は、他のリンクに負荷を再分散させることによって、リンク切断から自動的に回復します。 リンク障害が発生した場合、EtherChannel は自動的に障害リンクからチャネル内の他のリンクにトラフィックをリダイレクトします。

EtherChannel は、単一の論理リンクにバンドルする個別のイーサネット リンクで構成されます。

図 *19*：一般的な *EtherChannel* 構成



EtherChannel は、スイッチ間またはスイッチとホスト間に、最大 8 Gb/s（ギガビット EtherChannel）または 80 Gb/s（10 ギガビット EtherChannel）の全二重帯域幅を提供します。

各 EtherChannel は、互換性のある設定のイーサネット ポートを 8 つまで使用して構成できます。

EtherChannel の数は 128 に制限されています。

各 EtherChannel 内のすべてのポートは、レイヤ 2 またはレイヤ 3 ポートのいずれかとして設定する必要があります。 EtherChannel レイヤ 3 ポートは、ルーテッド ポートで構成されます。 ルーテッド ポートは、**no switchport** インターフェイス コンフィギュレーション コマンドを使用してレイヤ 3 モードに設定された物理ポートです。 詳細については、「Configuring Interface Characteristics」を参照してください。

関連トピック

レイヤ 2 EtherChannel の設定, （131 ページ）
EtherChannel 設定時の注意事項, （128 ページ）
EtherChannel のデフォルト設定, （126 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （129 ページ）

EtherChannel のモード

EtherChannel は、ポート集約プロトコル（PAgP）、Link Aggregation Control Protocol（LACP）、または On のいずれかのモードに設定できます。 EtherChannel の両端は同じモードで設定します。

- EtherChannel の一方の端を PAgP または LACP モードに設定すると、システムはもう一方の端とネゴシエーションし、アクティブにするポートを決定します。 リモート ポートが EtherChannel とネゴシエーションができない場合、ローカル ポートは独立ステートになり、他の単一リンクと同様にデータ トラフィックを引き続き伝送します。 ポート設定は変更されませんが、ポートは EtherChannel に参加しません。
- EtherChannel を **on** モードに設定すると、ネゴシエーションは実行されません。 スイッチは EtherChannel 内で互換性のあるすべてのポートを強制的にアクティブにします。 EtherChannel のもう一方の端（他のスイッチ上）も、同じように **on** モードに設定する必要があります。 それ以外を設定した場合、パケットの損失が発生します。

関連トピック

レイヤ 2 EtherChannel の設定, （131 ページ）
EtherChannel 設定時の注意事項, （128 ページ）
EtherChannel のデフォルト設定, （126 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （129 ページ）

Switches上の EtherChannel

switch上、スタックの単一switch上、またはスタックの複数switches上（クロススタック EtherChannel とも呼ぶ）で EtherChannel を作成できます。

図 *20*：単一スイッチ *EtherChannel*

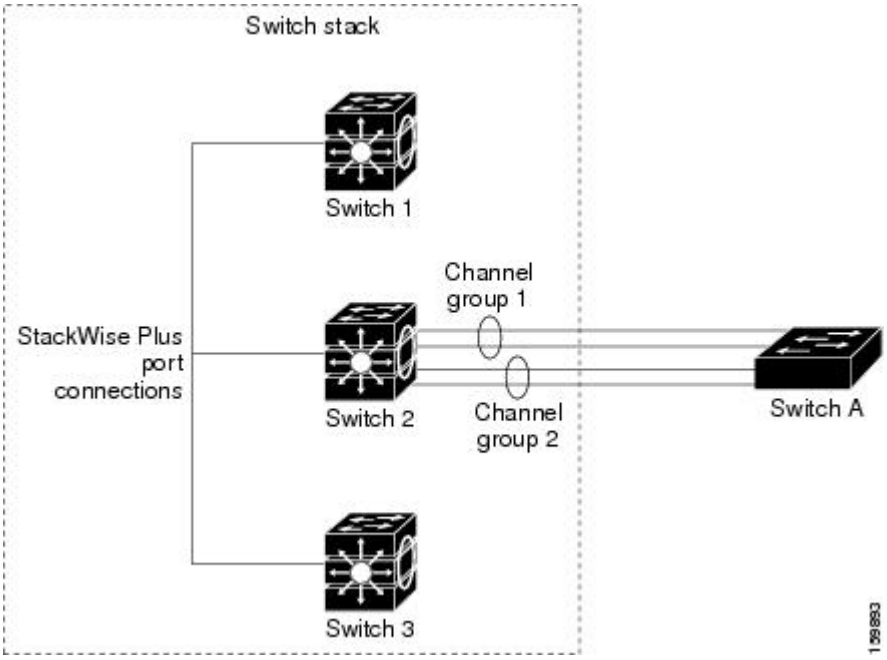


図 *21*：クロススタック *EtherChannel*

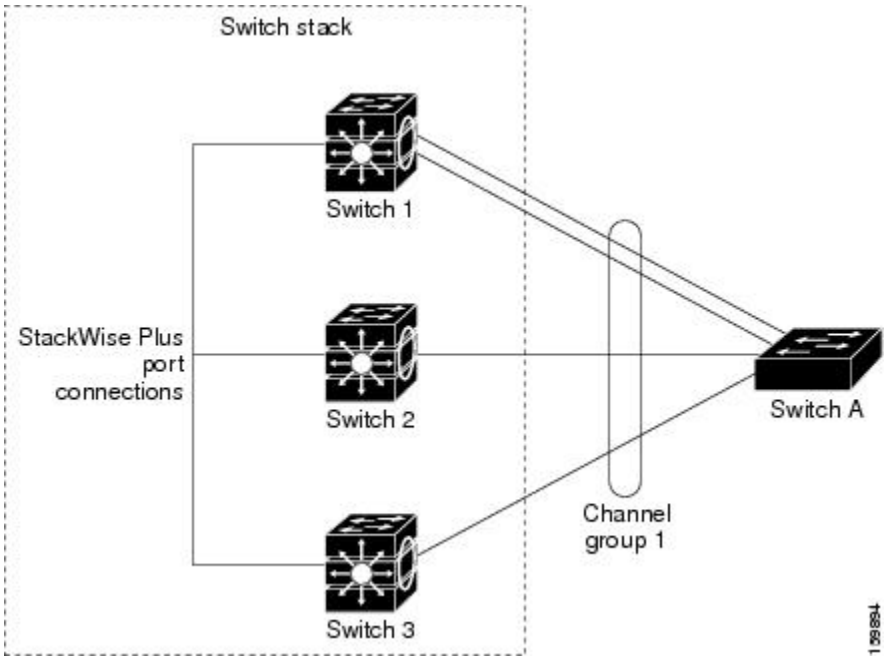
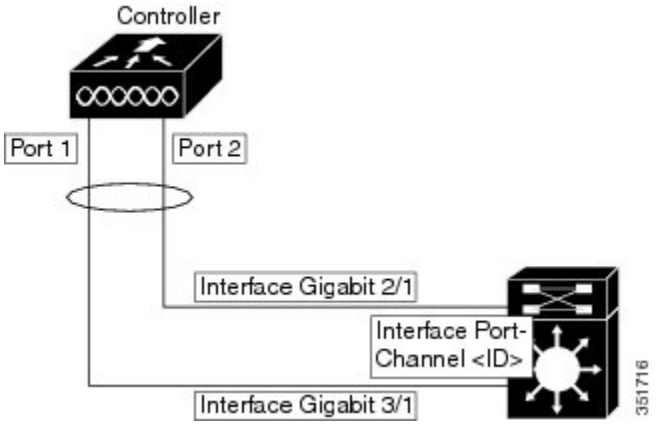
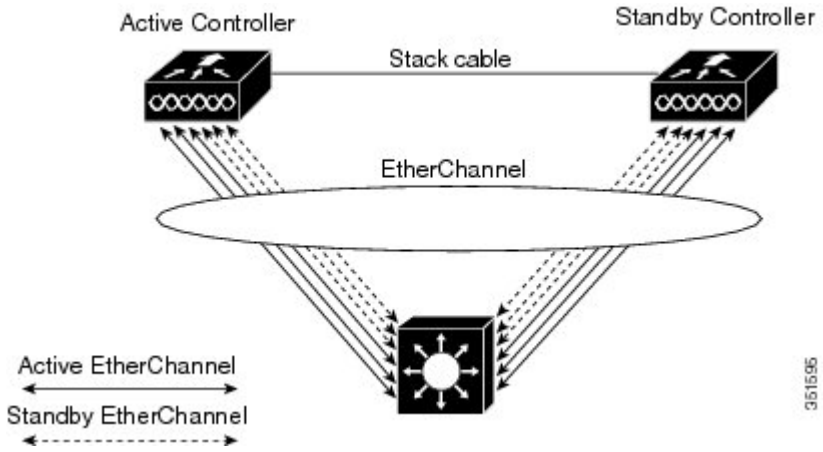


図 *22* : シングル コントローラ *EtherChannel*



この図は、3 個のアクティブ リンクと 3 個のスタンバイ リンクがあるクロススタック EtherChannel 推奨設定を示します。

図 *23*：クロススタック *EtherChannel*



関連トピック

レイヤ 2 EtherChannel の設定，（131 ページ）
EtherChannel 設定時の注意事項，（128 ページ）
EtherChannel のデフォルト設定，（126 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（129 ページ）

EtherChannel リンクのフェールオーバー

EtherChannel 内のリンクで障害が発生すると、それまでその障害リンクで伝送されていたトラフィックが EtherChannel 内の残りのリンクに切り替えられます。 スイッチでトラップがイネーブルになっている場合、スイッチ、EtherChannel、および失敗したリンクを区別したトラップが送信されます。 EtherChannel の 1 つのリンク上の着信ブロードキャストおよびマルチキャスト パケットは、EtherChannel の他のリンクに戻らないようにブロックされます。

関連トピック

レイヤ 2 EtherChannel の設定，（131 ページ）
EtherChannel 設定時の注意事項，（128 ページ）
EtherChannel のデフォルト設定，（126 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（129 ページ）

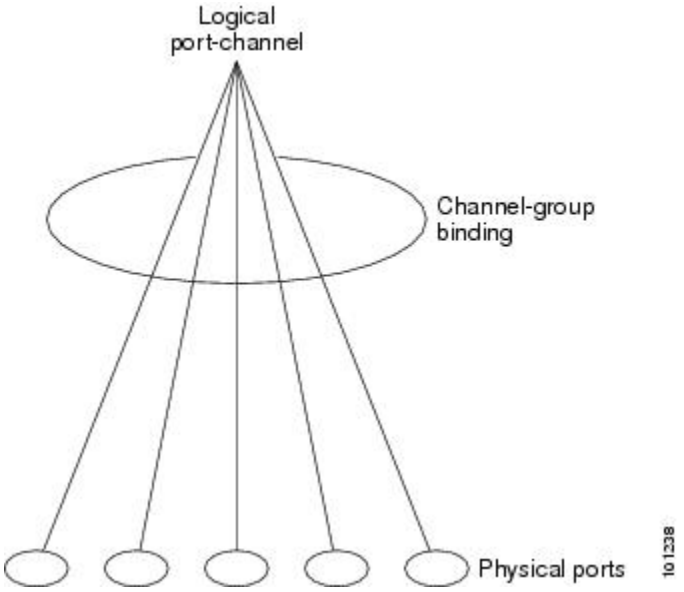
チャネル グループおよびポートチャネル インターフェイス

EtherChannel は、チャネル グループとポートチャネル インターフェイスから構成されます。 チャネル グループはポートチャネル インターフェイスに物理ポートをバインドします。 ポートチャ

ネルインターフェイスに適用した設定変更は、チャネルグループにまとめてバインドされるすべての物理ポートに適用されます。

channel-group コマンドは、物理ポートおよびポートチャネル インターフェイスをまとめてバインドします。 各 EtherChannel には 1 ～ 128 までの番号が付いたポートチャネル論理インターフェイスがあります。 このポートチャネル インターフェイス番号は、**channel-group** インターフェイス コンフィギュレーション コマンドで指定した番号に対応しています。

図 *24*：物理ポート、チャネル グループおよびポートチャネル インターフェイスの関係



- レイヤ 2 ポートの場合は、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ポートチャネル インターフェイスを動的に作成します。

  また、**interface port-channel** *port-channel-number* グローバル コンフィギュレーション コマンドを使用して、ポートチャネル論理インターフェイスを手動で作成することもできます。ただし、その場合、論理インターフェイスを物理ポートにバインドするには、**channel-group** *channel-group-number* コマンドを使用する必要があります。 *channel-group-number* は *port-channel-number* と同じ値に設定することも、違う値を使用することもできます。 新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポートチャネルを作成します。

- レイヤ 3 ポートの場合は、**interface port-channel** グローバル コンフィギュレーション コマンド、およびそのあとに **no switchport** インターフェイス コンフィギュレーション コマンドを使用して、論理インターフェイスを手動で作成する必要があります。 その後、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、手動で EtherChannel にインターフェイスを割り当てます。

- レイヤ 3 ポートでレイヤ 3 インターフェイスとしてインターフェイスを設定するには、**no switchport** インターフェイス コマンドを使用した上で **channel-group** インターフェイス コンフィギュレーション コマンドを使用して動的にポートチャネル インターフェイスを作成します。

関連トピック

ポートチャネル論理インターフェイスの作成
EtherChannel 設定時の注意事項, （128 ページ）
EtherChannel のデフォルト設定, （126 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （129 ページ）

物理インターフェイスの設定
EtherChannel 設定時の注意事項, （128 ページ）
EtherChannel のデフォルト設定, （126 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （129 ページ）

ポート集約プロトコル

ポート集約プロトコル（PAgP）はシスコ独自のプロトコルで、Cisco switchesおよびPAgPをサポートするベンダーによってライセンス供与されたswitchesでのみ稼働します。 PAgP を使用すると、イーサネット ポート間で PAgP パケットを交換することにより、EtherChannel を自動的に作成できます。 PAgP はクロススタック EtherChannel でイネーブルにできます。

switchまたはswitch スタックはPAgP を使用することによって、PAgP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。 次に、設定が類似している（スタック内の単一switch上の）ポートを、単一の論理リンク（チャネルまたは集約ポート）に動的にグループ化します。 設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。 たとえば、PAgP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同じポートをグループとしてまとめます。 リンクを EtherChannel にグループ化した後で、PAgP は単一switch ポートとして、スパニングツリーにそのグループを追加します。

PAgP モード

PAgP モードは、PAgP ネゴシエーションを開始する PAgP パケットをポートが送信できるか、または受信した PAgP パケットに応答できるかを指定します。

表 *12* : *EtherChannel PAgP* モード

モード	説明
auto	ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。 これにより、PAgP パケットの送信は最小限に抑えられます。

モード	説明
desirable	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 EtherChannel メンバが、スイッチ スタックにある異なるスイッチから（クロススタック EtherChannel）の場合、このモードはサポートされません。

スイッチ ポートは、**auto** モードまたは **desirable** モードに設定された相手ポートとだけ PAgP パケットを交換します。 **on** モードに設定されたポートは、PAgP パケットを交換しません。

auto モードおよび **desirable** モードはともに、相手ポートとネゴシエーションして、ポート速度などの条件に基づいて、ポートで EtherChannel を形成できるようにします。 レイヤ 2 EtherChannel の場合は、トランク ステートおよび VLAN 番号に基づきます。

PAgP モードが異なっていても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。 次に例を示します。

- **desirable** モードのポートは、**desirable** モードまたは **auto** モードの別のポートとともに EtherChannel を形成できます。
- **auto** モードのポートは、**desirable** モードの別のポートとともに EtherChannel を形成できます。

どのポートも PAgP ネゴシエーションを開始しないため、**auto** モードのポートは、**auto** モードの別のポートとは EtherChannel を形成できません。

関連トピック

レイヤ 2 EtherChannel の設定, （131 ページ）
EtherChannel 設定時の注意事項, （128 ページ）
EtherChannel のデフォルト設定, （126 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （129 ページ）
ポートチャネル論理インターフェイスの作成
EtherChannel 設定時の注意事項, （128 ページ）
EtherChannel のデフォルト設定, （126 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （129 ページ）
物理インターフェイスの設定
EtherChannel 設定時の注意事項, （128 ページ）
EtherChannel のデフォルト設定, （126 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （129 ページ）

サイレント モード

PAgP 対応のデバイスにスイッチを接続する場合、**non-silent** キーワードを使用すると、非サイレント動作としてスイッチ ポートを設定できます。 **auto** モードまたは **desirable** モードとともに **non-silent** を指定しなかった場合は、サイレント モードが指定されていると見なされます。

サイレント モードを使用するのは、PAgP 非対応で、かつほとんどパケットを送信しないデバイスにスイッチを接続する場合です。 サイレント パートナーの例は、トラフィックを生成しないファイル サーバ、またはパケット アナライザなどです。 この場合、サイレント パートナーに接続された物理ポート上で PAgP を稼働させると、このスイッチ ポートが動作しなくなります。 ただし、サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。

関連トピック

レイヤ 2 EtherChannel の設定, （131 ページ）
EtherChannel 設定時の注意事項, （128 ページ）
EtherChannel のデフォルト設定, （126 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （129 ページ）
ポートチャネル論理インターフェイスの作成
EtherChannel 設定時の注意事項, （128 ページ）
EtherChannel のデフォルト設定, （126 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （129 ページ）
物理インターフェイスの設定
EtherChannel 設定時の注意事項, （128 ページ）
EtherChannel のデフォルト設定, （126 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （129 ページ）

PAgP 学習方式およびプライオリティ

ネットワーク デバイスは、PAgP 物理ラーナーまたは集約ポート ラーナーに分類されます。 物理ポートによってアドレスを学習し、その知識に基づいて送信を指示するデバイスは物理ラーナーです。 集約（論理）ポートによってアドレスを学習するデバイスは、集約ポート ラーナーです。 学習方式は、リンクの両端で同一の設定にする必要があります。

デバイスとそのパートナーが両方とも集約ポート ラーナーの場合、論理ポートチャネル上のアドレスを学習します。 デバイスは EtherChannel のいずれかのポートを使用することによって、送信元にパケットを送信します。 集約ポート ラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。

PAgP は、パートナー デバイスが物理ラーナーの場合およびローカル デバイスが集約ポート ラーナーの場合には自動検出できません。 したがって、物理ポートでアドレスを学習するには、ローカルデバイスに手動で学習方式を設定する必要があります。 また、負荷の分散方式を送信元ベース分散に設定して、指定された送信元 MAC アドレスが常に同じ物理ポートに送信されるようにする必要もあります。

グループ内の 1 つのポートですべての伝送を行うように設定して、他のポートをホット スタンバイに使用することもできます。 選択された 1 つのポートでハードウェア信号が検出されなくなった場合は、数秒以内に、グループ内の未使用のポートに切り替えて動作させることができます。パケット伝送用に常に選択されるようにポートを設定するには、**pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用してプライオリティを変更します。プライオリティが高いほど、そのポートが選択される可能性が高まります。

（注） CLI（コマンドライン インターフェイス）で **physical-port** キーワードを指定した場合でも、switchがサポートするのは、集約ポート上でのアドレス ラーニングのみです。 **pagp learn-method** コマンドおよび **pagp port-priority** コマンドは、switchのハードウェアには作用しませんが、Catalyst 1900 スイッチなどの物理ポートによるアドレス ラーニングだけをサポートするデバイスと PAgP の相互運用性を確保するために必要です。

switchのリンク パートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用して物理ポート ラーナーとしてswitchを設定することを推奨します。 送信元MACアドレスに基づいて負荷の分散方式を設定するには、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用します。 すると、switchは送信元アドレスを学習した EtherChannel 内の同じポートを使用して、物理ラーナーにパケットを送信します。 **pagp learn-method** コマンドは、このような場合のみ使用してください。

関連トピック

PAgP 学習方式およびプライオリティの設定，（139 ページ）
EtherChannel 設定時の注意事項，（128 ページ）
EtherChannel のデフォルト設定，（126 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ，（146 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（129 ページ）

PAgP と他の機能との相互作用

ダイナミック トランキング プロトコル（DTP）および Cisco Discovery Protocol（CDP）は、EtherChannel の物理ポートを使用してパケットを送受信します。 トランク ポートは、番号が最も小さい VLAN 上で PAgP プロトコル データ ユニット（PDU）を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを渡します。 このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。 レイヤ 3 EtherChannel の場合は、（**interface port-channel** グローバル コンフィギュレーション コマンドを使用して）ポートが作成された直後に、アクティブなswitchによって MAC アドレスが割り当てられます。

PAgP が PAgP PDU を送受信するのは、PAgP が auto モードまたは desirable モードでイネーブルになっている、稼働状態のポート上だけです。

Link Aggregation Control Protocol

LACP は IEEE 802.3ad で定義されており、Cisco switchesが IEEE 802.3ad プロトコルに適合したswitches間のイーサネット チャネルを管理できるようにします。 LACP を使用すると、イーサネット ポート間で LACP パケットを交換することにより、EtherChannel を自動的に作成できます。

switchまたはswitch スタックは LACP を使用することによって、LACP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。 次に、設定が類似しているポートを単一の倫理リンク（チャネルまたは集約ポート）に動的にグループ化します。 設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。 たとえば、LACP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同じポートをグループとしてまとめます。 リンクをまとめて EtherChannel を形成した後で、LACP は単一switch ポートとして、スパニングツリーにそのグループを追加します。

LACP モード

LACPモードでは、ポートがLACPパケットを送信できるか、LACPパケットの受信のみができるかどうかを指定します。

表 *13*：*EtherChannel LACP* モード

モード	説明
active	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートはLACPパケットを送信することによって、相手ポートとのネゴシエーションを開始します。
passive	ポートはパッシブ ネゴシエーション ステートになります。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。 これにより、LACPパケットの送信を最小限に抑えます。

active モードおよび **passive LACP** モードはともに、相手ポートとネゴシエーションして、ポート速度などの条件に基づいて（レイヤ 2 EtherChannel の場合は、トランク ステートおよび VLAN 番号などの基準に基づいて）、ポートで EtherChannel を形成できるようにします。

LACP モードが異なっていても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。 次に例を示します。

- **active**モードのポートは、**active**モードまたは**passive**モードの別のポートとともにEtherChannelを形成できます。
- 両ポートともLACPネゴシエーションを開始しないため、**passive**モードのポートは、**passive**モードの別のポートと EtherChannel を形成することはできません。

関連トピック

レイヤ 2 EtherChannel の設定，（131 ページ）
EtherChannel 設定時の注意事項，（128 ページ）
EtherChannel のデフォルト設定，（126 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（129 ページ）

LACP とリンクの冗長性

LACP ポートチャネルの最小リンクおよびLACP の最大バンドルの機能を使用して、LACP ポートチャネル動作、帯域幅の可用性およびリンク冗長性をさらに高めることができます。

LACP ポートチャネルの最小リンク機能：

- LACP ポート チャネルでリンクし、バンドルする必要があるポートの最小数を設定します。
- 低帯域幅の LACP ポート チャネルがアクティブにならないようにします。
- 必要な最低帯域幅を提供する十分なアクティブ メンバ ポートがない場合、LACP ポート チャネルが非アクティブになるようにします。

LACP の最大バンドル機能：

- LACP ポート チャネルのバンドル ポートの上限数を定義します。
- バンドル ポートがより少ない場合のホット スタンバイ ポートを可能にします。 たとえば、5 個のポートがある LACP ポート チャネルで、3 個の最大バンドルを指定し、残りの 2 個のポートをホット スタンバイ ポートとして指定できます。

関連トピック

LACP 最大バンドル機能の設定，（141 ページ）
LACP ホット スタンバイ ポートの設定：例，（149 ページ）
ポート チャネル最小リンク機能の設定，（142 ページ）
LACP ホット スタンバイ ポートの設定：例，（149 ページ）

LACP と他の機能との相互作用

DTP および CDP は、EtherChannel の物理ポートを介してパケットを送受信します。 トランク ポートは、番号が最も小さい VLAN 上で LACP PDU を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを渡します。 このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。 レイヤ 3 EtherChannel の場合、**interface port-channel** グローバル コンフィギュレーション コマンドを経由してインターフェイスが作成された直後に、アクティブなswitchにより MAC アドレスが割り当てられます。

LACP が LACP PDU を送受信するのは、LACP が active モードまたは passive モードでイネーブルになっている稼働状態のポートとの間だけです。

EtherChannel の On モード

EtherChannel の **on** モードは、EtherChannel の手動設定に使用します。 **on** モードを使用すると、ポートはネゴシエーションせずに強制的に EtherChannel に参加します。 リモート デバイスが PAgP や LACP をサポートしていない場合にこの **on** モードが役立ちます。 **on** モードでは、リンクの両端のswitchesが **on** モードに設定されている場合のみ EtherChannel を使用できます。

同じチャネル グループの **on** モードで設定されたポートは、速度やデュプレックスのようなポート特性に互換性を持たせる必要があります。 **on** モードで設定されていたとしても、互換性のないポートは suspended ステートになります。

注意 **on** モードの使用には注意が必要です。 これは手動の設定であり、EtherChannel の両端のポートには、同一の設定が必要です。 グループの設定を誤ると、パケット損失またはスパニング ツリー ループが発生することがあります。

ロードバランシングおよび転送方式

EtherChannel は、フレーム内のアドレスに基づいて形成されたバイナリ パターンの一部を、チャネル内の 1 つのリンクを選択する数値に縮小することによって、チャネル内のリンク間でトラフィックのロード バランシングを行います。 MAC アドレス、IP アドレス、送信元アドレス、宛先アドレス、または送信元と宛先両方のアドレスに基づいた負荷分散など、複数の異なるロード バランシング モードから 1 つを指定できます。 選択したモードは、switch上で設定されているすべての EtherChannel に適用されます。

port-channel load-balance および **port-channel load-balance extended** グローバル コンフィギュレーション コマンドを使用して、ロードバランシングおよび転送方式を設定します。

関連トピック

EtherChannel ロードバランシングの設定, （136 ページ）
EtherChannel 設定時の注意事項, （128 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （129 ページ）
EtherChannel のデフォルト設定, （126 ページ）
レイヤ 3 EtherChannel 設定時の注意事項, （130 ページ）

MAC アドレス転送

送信元 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 MAC アドレスに基づいてチャネル ポート間で分配されます。 したがって、ロード バランシングを行うために、送信元ホストが異なるパケットはそれぞれ異なるチャネル ポートを使用しますが、送信元ホストが同じパケットは同じチャネル ポートを使用します。

宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットの宛先ホストの MAC アドレスに基づいてチャネル ポート間で分配されます。 したがって、宛先が同じパケットは同じポートに転送され、宛先の異なるパケットはそれぞれ異なるチャネル ポートに転送されます。

送信元および宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、送信元および宛先の両方の MAC アドレスに基づいてチャネル ポート間で分配されます。 この転送方式は、負荷分散の送信元 MAC アドレス転送方式と宛先 MAC アドレス転送方式を組み合わせたものです。特定のswitchに対して送信元 MAC アドレス転送と宛先 MAC アドレス転送のどちらが適切であるかが不明な場合に使用できます。 送信元および宛先 MAC アドレス転送の場合、ホスト A からホスト B、ホスト A からホスト C、およびホスト C からホスト B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

関連トピック

EtherChannel ロードバランシングの設定, （136 ページ）
EtherChannel 設定時の注意事項, （128 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （129 ページ）
EtherChannel のデフォルト設定, （126 ページ）
レイヤ 3 EtherChannel 設定時の注意事項, （130 ページ）

IP アドレス転送

送信元 IP アドレスベース転送の場合、パケットは、着信パケットの送信元 IP アドレスに基づいて EtherChannel ポート間で分配されます。 ロードバランシングを行うために、IP アドレスが異なるパケットはチャネルでそれぞれ異なるポートを使用しますが、IP アドレスが同じパケットはチャネルで同じポートを使用します。

宛先 IP アドレスベース転送の場合、パケットは着信パケットの宛先 IP アドレスに基づいて EtherChannel ポート間で分配されます。 ロードバランシングを行うために、同じ送信元 IP アドレスから異なる宛先 IP アドレスに送信されるパケットは、チャネルの異なるチャネル ポートに送信できます。 異なる送信元 IP アドレスから同じ宛先 IP アドレスに送信されるパケットは、常にチャネルの同じポートに送信されます。

送信元と宛先 IP アドレスベース転送の場合、パケットは着信パケットの送信元および宛先の両方の IP アドレスに基づいて EtherChannel ポート間で分配されます。 この転送方式は、送信元 IP アドレスベース転送方式と宛先 IP アドレスベース転送方式を組み合わせたもので、特定のswitchに対して送信元 IP アドレスベース転送と宛先 IP アドレスベース転送のどちらが適切であるか不明な場合に使用できます。 この方式では、IP アドレス A から IP アドレス B に、IP アドレス A から IP アドレス C に、および IP アドレス C から IP アドレス B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

関連トピック

EtherChannel ロードバランシングの設定, （136 ページ）
EtherChannel 設定時の注意事項, （128 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （129 ページ）

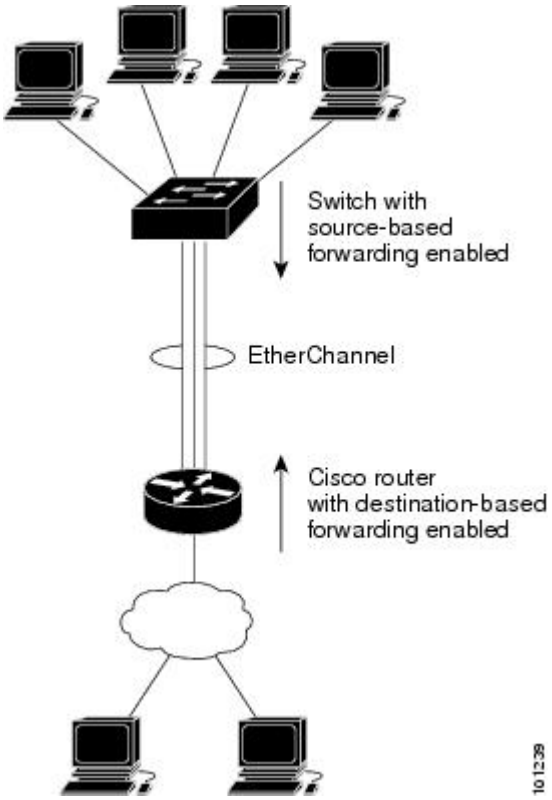
EtherChannel のデフォルト設定, （126 ページ）
レイヤ 3 EtherChannel 設定時の注意事項, （130 ページ）

ロードバランシングの利点

ロードバランシング方式には異なる利点があるため、ネットワーク内のswitchの位置、および負荷分散が必要なトラフィックの種類に基づいて特定のロードバランシング方式を選択する必要があります。

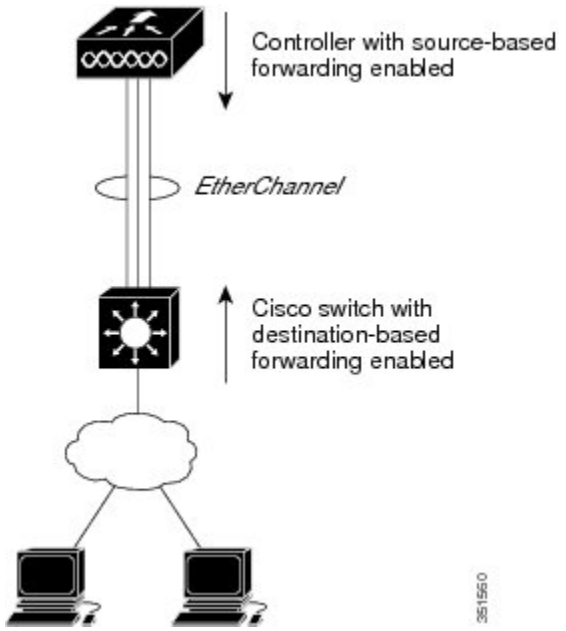
次の図では、4 台のワーク ステーションの EtherChannel がルータと通信します。 ルータは単一 MAC アドレス デバイスであるため、switch EtherChannel で送信元ベース転送を行うことにより、switchが、ルータで使用可能なすべての帯域幅を使用することが保証されます。 ルータは、宛先アドレスベース転送を行うように設定されます。これは、多数のワークステーションで、トラフィックがルータ EtherChannel から均等に分配されることになっているためです。

図 *25*：負荷の分散および転送方式



下の図では、コントローラが EtherChannel リンク上で送信元 MAC ベースの転送を行い、EtherChannel の複数のリンク上でトラフィックを均等に分散します。

図 *26*：負荷分散と転送



設定で一番種類が多くなるオプションを使用してください。 たとえば、チャネル上のトラフィックが単一MACアドレスを宛先とする場合、宛先MACアドレスを使用すると、チャネル内の同じリンクが常に選択されます。 ただし、送信元アドレスまたはIPアドレスを使用した方が、ロードバランシングの効率がよくなる場合があります。

関連トピック

EtherChannel ロードバランシングの設定，（136 ページ）
EtherChannel 設定時の注意事項，（128 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（129 ページ）
EtherChannel のデフォルト設定，（126 ページ）
レイヤ 3 EtherChannel 設定時の注意事項，（130 ページ）

EtherChannel およびSwitch スタック

EtherChannel に加入しているポートが含まれているスタック メンバに障害が発生したり、スタックを離れると、アクティブなswitchにより、障害が発生したスタック switch メンバ ポートが削除されます。 EtherChannel に残っているポートがある場合、接続は引き続き確保されます。

switchが既存のスタックに追加されると、新しいswitchがアクティブなswitchから実行コンフィギュレーションを受信し、EtherChannel 関連のスタック コンフィギュレーションで更新されます。 スタック メンバでは、動作情報（動作中で、チャネルのメンバであるポートのリスト）も受信します。

2 つのスタック間で設定されている EtherChannel がマージされた場合、セルフループ ポートになります。 スパニングツリーにより、この状況が検出され、必要な動作が発生します。 権利を獲得したswitch スタックにある PAgP 設定または LACP 設定は影響を受けませんが、権利を失った switch スタックの PAgP 設定または LACP 設定は、スタックのリブート後に失われます。

Switch スタックおよび PAgP

PAgP では、アクティブ switchに障害が発生するか、スタックを離れた場合、スタンバイ switchが新しいアクティブ switchになります。 EtherChannel 帯域幅に変更がない場合、スパニングツリーの再コンバージェンスはトリガーされません。 新しいアクティブ switchはアクティブ switchの該当項目にスタック メンバの設定を同期します。 PAgP 設定は、EtherChannel に古いアクティブ switch上にあるポートがない限り、アクティブ switchの変更後も影響を受けません。

Switch スタックおよび LACP

LACP の場合、システム ID は、アクティブ switchから取得したスタック MAC アドレスが使用されます。 アクティブ switchに障害が発生したり、スタックを離れ、スタンバイ switchが新しいアクティブ switchが変更になっても、LACP システム ID は変更されません。 デフォルトでは、LACP 設定はアクティブ switchの変更後も影響を受けません。

EtherChannel のデフォルト設定

EtherChannel のデフォルト設定を、次の表に示します。

表 *14*：*EtherChannel* のデフォルト設定

機能	デフォルト設定
チャネル グループ	割り当てなし
ポートチャネル論理インターフェイス	未定義
PAgP モード	デフォルトなし
PAgP 学習方式	すべてのポートで集約ポート ラーニング
PAgP プライオリティ	すべてのポートで 128
LACP モード	デフォルトなし
LACP 学習方式	すべてのポートで集約ポート ラーニング
LACP ポート プライオリティ	すべてのポートで 32768
LACP システム プライオリティ	32768

機能	デフォルト設定
LACP システム ID	LACP システムのプライオリティ、switchまたはスタックの MAC アドレス。
ロード バランシング	switch上での負荷分散は着信パケットの送信元 MAC アドレスに基づきます。

関連トピック

レイヤ 2 EtherChannel の設定, （131 ページ）
EtherChannel の概要, （110 ページ）
EtherChannel のモード, （111 ページ）
Switches上の EtherChannel, （112 ページ）
EtherChannel リンクのフェールオーバー, （114 ページ）
LACP モード, （120 ページ）
PAgP モード , （116 ページ）
サイレント モード, （118 ページ）
ポートチャネル論理インターフェイスの作成
チャネル グループおよびポートチャネル インターフェイス, （114 ページ）
PAgP モード , （116 ページ）
サイレント モード, （118 ページ）
物理インターフェイスの設定
チャネル グループおよびポートチャネル インターフェイス, （114 ページ）
PAgP モード , （116 ページ）
サイレント モード, （118 ページ）
EtherChannel ロードバランシングの設定, （136 ページ）
ロードバランシングおよび転送方式, （122 ページ）
MAC アドレス転送, （122 ページ）
IP アドレス転送, （123 ページ）
ロードバランシングの利点, （124 ページ）
PAgP 学習方式およびプライオリティの設定 , （139 ページ）
PAgP 学習方式およびプライオリティ, （118 ページ）
LACP システム プライオリティの設定, （143 ページ）
LACP ポート プライオリティの設定, （145 ページ）

EtherChannel 設定時の注意事項

EtherChannel ポートを正しく設定していない場合は、ネットワーク ループおよびその他の問題を回避するために、一部の EtherChannel インターフェイスが自動的にディセーブルになります。 設定上の問題を回避するために、次の注意事項に従ってください。

- switchまたはswitch スタック上では、128 を超える EtherChannel を設定しないでください。
- PAgP EtherChannel は、同じタイプのイーサネット ポートを 8 つまで使用して設定します。
- 同じタイプのイーサネット ポートを最大で 16 個備えた LACP EtherChannel を設定してください。 最大 8 個をアクティブに、最大 8 個をスタンバイ モードにできます。
- EtherChannel 内のすべてのポートを同じ速度および同じデュプレックス モードで動作するように設定します。
- EtherChannel 内のすべてのポートをイネーブルにします。 **shutdown** インターフェイス コンフィギュレーション コマンドによってディセーブルにされた EtherChannel 内のポートは、リンク障害として扱われます。そのポートのトラフィックは、EtherChannel 内の他のポートの 1 つに転送されます。
- グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。 次のパラメータのいずれかで設定を変更した場合は、グループ内のすべてのポートでも変更する必要があります。
  - 許可 VLAN リスト
  - 各 VLAN のスパニングツリー パス コスト
  - 各 VLAN のスパニングツリー ポート プライオリティ
  - スパニングツリー PortFast の設定
- 1 つのポートが複数の EtherChannel グループのメンバになるように設定しないでください。
- EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。 PAgP および LACP を実行している EtherChannel グループはスタックの同一switch、または異なるswitches で共存できます。 個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用することはできません。
- EtherChannel の一部としてセキュア ポートを設定したり、セキュア ポートの一部として EtherChannel を設定したりしないでください。
- アクティブまたはアクティブでない EtherChannel メンバであるポートを IEEE 802.1x ポートとして設定しないでください。 EtherChannel ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。
- EtherChannel がswitch インターフェイス上に設定されている場合、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを使用して、IEEE 802.1x をswitch上でグローバルにイネーブルにする前に、EtherChannel の設定をインターフェイスから削除します。

- クロススタック EtherChannel が設定されていると、switch スタック パーティション、ループおよび転送の問題が発生する可能性があります。

関連トピック

レイヤ 2 EtherChannel の設定, （131 ページ）
EtherChannel の概要, （110 ページ）
EtherChannel のモード, （111 ページ）
Switches上の EtherChannel, （112 ページ）
EtherChannel リンクのフェールオーバー, （114 ページ）
LACP モード, （120 ページ）
PAgP モード , （116 ページ）
サイレント モード, （118 ページ）
ポートチャネル論理インターフェイスの作成
チャネル グループおよびポートチャネル インターフェイス, （114 ページ）
PAgP モード , （116 ページ）
サイレント モード, （118 ページ）
物理インターフェイスの設定
チャネル グループおよびポートチャネル インターフェイス, （114 ページ）
PAgP モード , （116 ページ）
サイレント モード, （118 ページ）
EtherChannel ロードバランシングの設定, （136 ページ）
ロードバランシングおよび転送方式, （122 ページ）
MAC アドレス転送, （122 ページ）
IP アドレス転送, （123 ページ）
ロードバランシングの利点, （124 ページ）
PAgP 学習方式およびプライオリティの設定 , （139 ページ）
PAgP 学習方式およびプライオリティ, （118 ページ）
LACP システム プライオリティの設定, （143 ページ）
LACP ポート プライオリティの設定, （145 ページ）

レイヤ 2 EtherChannel 設定時の注意事項

レイヤ 2 EtherChannels を設定する場合は、次の注意事項に従ってください。

- EtherChannel 内のすべてのポートを同じ VLAN に割り当てるか、またはトランクとして設定してください。 複数のネイティブ VLAN に接続されるポートは、EtherChannel を形成できません。

- EtherChannel は、トランキング レイヤ 2 EtherChannel 内のすべてのポート上で同じ VLAN 許容範囲をサポートしています。 VLAN 許容範囲が一致していないと、PAgP が **auto** モードまたは **desirable** モードに設定されていても、ポートは EtherChannel を形成しません。
- スパニングツリー パス コストが異なるポートは、設定上の矛盾がない限り、EtherChannel を形成できます。 異なるスパニングツリー パス コストを設定すること自体は、EtherChannel を形成するポートの矛盾にはなりません。

関連トピック

レイヤ 2 EtherChannel の設定, （131 ページ）
EtherChannel の概要, （110 ページ）
EtherChannel のモード, （111 ページ）
Switches上の EtherChannel, （112 ページ）
EtherChannel リンクのフェールオーバー, （114 ページ）
LACP モード, （120 ページ）
PAgP モード , （116 ページ）
サイレント モード, （118 ページ）
ポートチャネル論理インターフェイスの作成
チャネル グループおよびポートチャネル インターフェイス, （114 ページ）
PAgP モード , （116 ページ）
サイレント モード, （118 ページ）
物理インターフェイスの設定
チャネル グループおよびポートチャネル インターフェイス, （114 ページ）
PAgP モード , （116 ページ）
サイレント モード, （118 ページ）
EtherChannel ロードバランシングの設定, （136 ページ）
ロードバランシングおよび転送方式, （122 ページ）
MAC アドレス転送, （122 ページ）
IP アドレス転送, （123 ページ）
ロードバランシングの利点, （124 ページ）
PAgP 学習方式およびプライオリティの設定 , （139 ページ）
PAgP 学習方式およびプライオリティ, （118 ページ）
LACP システム プライオリティの設定, （143 ページ）
LACP ポート プライオリティの設定, （145 ページ）

レイヤ 3 EtherChannel 設定時の注意事項

- レイヤ 3 EtherChannel の場合は、レイヤ 3 アドレスをチャネル内の物理ポートでなく、ポートチャネル論理インターフェイスに割り当ててください。

関連トピック

EtherChannel ロードバランシングの設定, （136 ページ）
ロードバランシングおよび転送方式, （122 ページ）
MAC アドレス転送, （122 ページ）
IP アドレス転送, （123 ページ）
ロードバランシングの利点, （124 ページ）

EtherChannel の設定方法

EtherChannelの設定後、ポートチャネルインターフェイスに適用した設定変更は、そのポートチャネル インターフェイスに割り当てられたすべての物理ポートに適用されます。また、物理ポートに適用した設定変更は、設定を適用したポートだけに作用します。

レイヤ 2 EtherChannel の設定

2 EtherChannel を設定するには、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、チャネル グループにポートを割り当てます。 このコマンドにより、ポートチャネル論理インターフェイスが自動的に作成されます。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport mode** {**access** | **trunk**}
4. **switchport access vlan** *vlan-id*
5. **channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on** } | { **active** | **passive**}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスは、物理ポートです。 PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 まで設定できます。 最大 8 個をアクティブに、最大 8 個をスタンバイ モードにできます。
ステップ 3	**switchport mode** {**access** | **trunk**} 例： `Switch(config-if)# switchport mode access`	すべてのポートをスタティックアクセスポートとして同じVLANに割り当てるか、またはトランクとして設定します。 ポートをスタティックアクセス ポートとして設定する場合は、ポートを 1 つの VLAN にのみ割り当ててください。 指定できる範囲は 1 ～ 4094 です。
ステップ 4	**switchport access vlan** *vlan-id* 例： `Switch(config-if)# switchport access vlan 22`	ポートをスタティックアクセス ポートとして設定する場合は、ポートを 1 つの VLAN にのみ割り当ててください。 指定できる範囲は 1 ～ 4094 です。
ステップ 5	**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on** } | { **active** | **passive**} 例： `Switch(config-if)# channel-group 5 mode auto`	チャネル グループにポートを割り当て、PAgP モードまたは LACP モードを指定します。 *channel-group-number* の範囲は 1 ～ 128 です。 **mode** には、次のキーワードのいずれか 1 つを選択します。 • **auto**：PAgP デバイスが検出された場合のみ、PAgP をイネーブルにします。 ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。 このキーワードは、EtherChannel メンバがswitches スタックの異なるswitchのものである場合にはサポートされません。 • **desirable**：PAgP を無条件でイネーブルにします。 ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 このキーワードは、EtherChannel メンバがswitches スタックの異なるswitchのものである場合にはサポートされません。 • **on** ：PAgP または LACP を使用せずにポートが強制的にチャネル化されます。 **on** モードでは、使用可能な EtherChannel が存在するのは、**on** モー

	コマンドまたはアクション	目的
		ドのポート グループが、**on** モードの別のポート グループに接続する場合だけです。 • **non-silent** ： （任意）switch が PAgP 対応のパートナーに接続されている場合、ポートが **auto** または **desirable** モードになると非サイレント動作を行うようにswitch ポートを設定します。 **non-silent** を指定しないと、サイレントが想定されます。 サイレント設定は、ファイル サーバまたはパケット アナライザとの接続に適しています。 サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。 • **active**：LACP デバイスが検出された場合に限り、LACP をイネーブルにします。 ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • **passive**：ポート上で LACP をイネーブルにして、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

EtherChannel の概要, （110 ページ）
EtherChannel のモード, （111 ページ）
Switches上の EtherChannel, （112 ページ）
EtherChannel リンクのフェールオーバー, （114 ページ）
LACP モード, （120 ページ）
PAgP モード , （116 ページ）
サイレント モード, （118 ページ）
EtherChannel 設定時の注意事項, （128 ページ）
EtherChannel のデフォルト設定, （126 ページ）
レイヤ 2 EtherChannel 設定時の注意事項, （129 ページ）

レイヤ 3 EtherChannel の設定

レイヤ 3 EtherChannel にイーサネット ポートを割り当てるには、この手順を実行します。 この手順は必須です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **no ip address**
5. **no switchport**
6. **channel-group** *channel-group-number* **mode** { **auto** [**non-silent**] | **desirable** [**non-silent**] | **on** } | { **active** | **passive** }
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/2`	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。 PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 まで設定できます。 最大 8 個をアクティブに、最大 8 個をスタンバイ モードにできます。

	コマンドまたはアクション	目的
ステップ 4	**no ip address** 例： `Switch(config-if)# no ip address`	物理ポートに割り当てられている IP アドレスがないことを確認します。
ステップ 5	**no switchport** 例： `Switch(config-if)# no switchport`	ポートをレイヤ 3 モードにします。
ステップ 6	**channel-group** *channel-group-number* **mode** { **auto** [**non-silent**] | **desirable** [**non-silent**] | **on** } | { **active** | **passive** } 例： `Switch(config-if)# channel-group 5 mode auto`	チャネル グループにポートを割り当て、PAgP モードまたは LACP モードを指定します。 **mode** には、次のキーワードのいずれか 1 つを選択します。 • **auto**：PAgP デバイスが検出された場合に限り、PAgP をイネーブルにします。 ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。 このキーワードは、EtherChannel メンバがswitch スタックの異なるswitchesのものである場合にはサポートされません。 • **desirable**：PAgP を無条件でイネーブルにします。 ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 このキーワードは、EtherChannel メンバがswitch スタックの異なるswitchesのものである場合にはサポートされません。 • **on**：PAgP や LACP を使用しないで、ポートを強制的にチャネル化します。 **on** モードでは、使用可能な EtherChannel が存在するのは、**on** モードのポート グループが、**on** モードの別のポート グループに接続する場合だけです。 • **non-silent**：（任意）switchが PAgP 対応の相手先に接続されている場合、ポートが **auto** または **desirable** モードになると、非サイレント動作を行うようにswitch ポートを設定します。 **non-silent** を指定しないと、サイレントが想定されます。 サイレント設定は、ファイル サーバまたはパケット アナライザとの接続に適しています。 サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。 • **active**：LACP デバイスが検出された場合に限り、LACP をイネーブルにします。 ポートをアクティブ ネゴシエーション ステートにします。

	コマンドまたはアクション	目的
		この場合、ポートはLACPパケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • **passive**：ポート上でLACPをイネーブルにして、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信するLACPパケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。
ステップ 7	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

EtherChannel ロードバランシングの設定

複数の異なる転送方式の1つを使用するようにEtherChannelロードバランシングを設定できます。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **port-channel load-balance** { **dst-ip** | **dst-mac** | **dst-mixed-ip-port** | **dst-port** | **extended** [**dst-ip** | **dst-mac** | **dst-port** | **ipv6-label** | **l3-proto** | **src-ip** | **src-mac** | **src-port**] | **src-dst-ip** | **src-dst-mac** **src-dst-mixed-ip-port src-dst-portsrc-ip** | **src-mac** | **src-mixed-ip-port** | **src-port**}
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**port-channel load-balance** { **dst-ip**	**dst-mac**	**dst-mixed-ip-port**	**dst-port**	**extended** [**dst-ip**	**dst-mac**	**dst-port**	**ipv6-label**	**l3-proto**	**src-ip**		EtherChannel のロードバランシング方式を設定します。 デフォルトは **src-mac** です。 次のいずれかの負荷分散方式を選択します。

	コマンドまたはアクション	目的
	src-mac | **src-port**] | **src-dst-ip** | **src-dst-mac** **src-dst-mixed-ip-port** **src-dst-portsrc-ip** | **src-mac** | **src-mixed-ip-port** | **src-port**} 例： `Switch(config)# port-channel load-balance src-mac`	• **dst-ip**：宛先ホストの IP アドレスを指定します。 • **dst-mac**：着信パケットの宛先ホストの MAC アドレスを指定します。 • **dst-mixed-ip-port**：ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • **dst-port**：宛先 TCP/UDP ポートを指定します。 • **extended**：標準コマンドで使用可能なもの以外に、送信元および宛先の方式を組み合わせた、拡張ロードバランシング方式を指定します。 • **ipv6-label**：IPv6 フロー ラベルを指定します。 • **l3-proto**：レイヤ 3 プロトコルを指定します。 • **src-dst-ip**：送信元および宛先ホストの IP アドレスを指定します。 • **src-dst-mac**：送信元および宛先ホストの MAC アドレスを指定します。 • **src-dst-mixed-ip-port**：送信元および宛先ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • **src-dst-port**：送信元および宛先 TCP/UDP ポートを指定します。 • **src-ip**：送信元ホストの IP アドレスを指定します。 • **src-mac**：着信パケットの送信元 MAC アドレスを指定します。 • **src-mixed-ip-port**：送信元ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • **src-port**：送信元 TCP/UDP ポートを指定します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

ロードバランシングおよび転送方式，（122 ページ）
MAC アドレス転送，（122 ページ）

IP アドレス転送，（123 ページ）
ロードバランシングの利点，（124 ページ）
EtherChannel 設定時の注意事項，（128 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（129 ページ）
EtherChannel のデフォルト設定，（126 ページ）
レイヤ 3 EtherChannel 設定時の注意事項，（130 ページ）

EtherChannel 拡張ロードバランシングの設定

ロードバランシング方式を組み合わせて使用する場合には、拡張ロードバランシングを設定します。

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **port-channel load-balance extended** [**dst-ip** | **dst-mac dst-port** | **ipv6-label** | **l3-proto** | **src-ip** | **src-mac** | **src-port**]
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**port-channel load-balance extended** [**dst-ip** | **dst-mac dst-port** | **ipv6-label** | **l3-proto** | **src-ip** | **src-mac** | **src-port**] 例： `Switch(config)# port-channel load-balance extended dst-ip dst-mac src-ip`	EtherChannel 拡張ロードバランシング方式を設定します。 デフォルトは **src-mac** です。 次のいずれかの負荷分散方式を選択します。 • **dst-ip**：宛先ホストの IP アドレスを指定します。 • **dst-mac**：着信パケットの宛先ホストの MAC アドレスを指定します。 • **dst-port**：宛先 TCP/UDP ポートを指定します。 • **ipv6-label**：IPv6 フロー ラベルを指定します。 • **l3-proto**：レイヤ 3 プロトコルを指定します。 • **src-ip**：送信元ホストの IP アドレスを指定します。

	コマンドまたはアクション	目的
		• **src-mac**：着信パケットの送信元MACアドレスを指定します。 • **src-port**：送信元 TCP/UDP ポートを指定します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

PAgP 学習方式およびプライオリティの設定

このタスクはオプションです。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **pagp learn-method physical-port**
4. **pagp port-priority** *priority*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/2`	伝送ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**pagp learn-method physical-port** 例： `Switch(config-if)# pagp learn-method physical port`	PAgP 学習方式を選択します。 デフォルトでは、**aggregation-port learning** が選択されています。つまり、EtherChannel 内のポートのいずれかを使用して、switchがパケットを送信元に送信します。集約ポート ラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。 物理ポート ラーナーである別のswitchに接続する**物理ポート**を選択します。 **port-channel load-balance** グローバル コンフィギュレーション コマンドを **src-mac** に設定してください。 学習方式はリンクの両端で同じ方式に設定する必要があります。
ステップ 4	**pagp port-priority** *priority* 例： `Switch(config-if)# pagp port-priority 200`	選択したポートがパケット伝送用として選択されるように、プライオリティを割り当てます。 *priority* に指定できる範囲は 0 ～ 255 です。 デフォルト値は 128 です。 プライオリティが高いほど、ポートが PAgP 伝送に使用される可能性が高くなります。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

PAgP 学習方式およびプライオリティ，（118 ページ）
EtherChannel 設定時の注意事項，（128 ページ）
EtherChannel のデフォルト設定，（126 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ，（146 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（129 ページ）

LACP ホット スタンバイ ポートの設定

LACP がイネーブルの場合、ソフトウェアはデフォルトで、チャネルにおける LACP 互換ポートの最大数（最大 16 個のポート）の設定を試みます。 一度にアクティブにできる LACP リンクは 8 つだけです。残りの 8 個のリンクがホット スタンバイ モードになります。 アクティブ リンクの 1 つが非アクティブになると、ホット スタンバイ モードのリンクが代わりにアクティブになります。

チャネルでアクティブ ポートの最大数を指定することでデフォルト動作を上書きできます。この場合、残りのポートがホット スタンバイ ポートになります。 たとえばチャネルで最大 5 個のポートを指定した場合、11 個までのポートがホット スタンバイ ポートになります。

9 つ以上のリンクが EtherChannel グループとして設定された場合、ソフトウェアは LACP プライオリティに基づいてアクティブにするホット スタンバイ ポートを決定します。 ソフトウェアは、LACP を操作するシステム間のすべてのリンクに、次の要素（プライオリティ順）で構成された一意のプライオリティを割り当てます。

- LACP システム プライオリティ
- システム ID（switch MAC アドレス）
- LACP ポート プライオリティ
- ポート番号

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。 プライオリティは、ハードウェア上の制約がある場合に、すべての互換ポートが集約されないように、スタンバイ モードにするポートを決定します。

アクティブ ポートかホット スタンバイ ポートかを判別するには、次の（2 つの）手順を使用します。 まず、数値的に低いシステム プライオリティとシステム ID を持つシステムの方を選びます。次に、ポート プライオリティおよびポート番号の値に基づいて、そのシステムのアクティブ ポートとホット スタンバイ ポートを決定します。 他のシステムのポート プライオリティとポート番号の値は使用されません。

ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響を与えるように、LACP システム プライオリティおよび LACP ポート プライオリティのデフォルト値を変更できます。

LACP 最大バンドル機能の設定

ポート チャネルで許可されるバンドル化された LACP ポートの最大数を指定すると、ポート チャネル内の残りのポートがホット スタンバイ ポートとして指定されます。

ポート チャネルの LACP ポートの最大数を設定するには、特権 EXEC モードで開始して、次の手順に従います。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **lacp max-bundle** *max-bundle-number*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface port-channel** *channel-number* 例： `Switch(config)# interface port-channel 2`	ポート チャネルのインターフェイス コンフィギュレーション モードを開始します。 指定できる範囲は 1 ～ 128 です。
ステップ 3	**lacp max-bundle** *max-bundle-number* 例： `Switch(config-if)# lacp max-bundle 3`	ポートチャネル バンドルで LACP ポートの最大数を指定します。 指定できる範囲は 1 ～ 8 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

LACP とリンクの冗長性，（121 ページ）
LACP ホット スタンバイ ポートの設定：例，（149 ページ）

ポート チャネル最小リンク機能の設定

リンク アップ状態で、リンク アップ ステートに移行するポート チャネル インターフェイスの EtherChannel でバンドルする必要のあるアクティブ ポートの最小数を指定できます。

ポート チャネルに必要なリンクの最小数を設定するには、特権 EXEC モードで開始して、次の手順に従います。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **port-channel min-links** *min-links-number*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface port-channel** *channel-number* 例： `Switch(config)# interface port-channel 2`	ポートチャネルのインターフェイス コンフィギュレーション モードを開始します。 *channel-number* の範囲は 1 ～ 128 です。
ステップ 3	**port-channel min-links** *min-links-number* 例： `Switch(config-if)# port-channel min-links 3`	リンク アップ状態で、リンク アップ ステートに移行するポート チャネル インターフェイスの EtherChannel でバンドルする必要のあるメンバ ポートの最小数を指定できます。 *min-links-number* の範囲は 2 ～ 8 です。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

LACP とリンクの冗長性 , （121 ページ）
LACP ホット スタンバイ ポートの設定：例, （149 ページ）

LACP システム プライオリティの設定

lacp system-priority グローバル コンフィギュレーション コマンドを使用して、LACP をイネーブルにしているすべての EtherChannel に対してシステム プライオリティを設定できます。 LACP を

設定済みの各チャネルに対しては、システムプライオリティを設定できません。デフォルト値を変更すると、ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響します。

show etherchannel summary 特権 EXEC コマンドを使用して、ホット スタンバイ モードのポートを確認できます（ポートステート フラグが H になっています）。

LACP システム プライオリティを設定するには、次の手順に従います。 この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **lacp system-priority** *priority*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**lacp system-priority** *priority* 例： `Switch(config)# lacp system-priority 32000`	LACP システム プライオリティを設定します。 指定できる範囲は 1 ～ 65535 です。 デフォルト値は 32768 です。 値が小さいほど、システムプライオリティは高くなります。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

EtherChannel 設定時の注意事項, （128 ページ）

EtherChannel のデフォルト設定，（126 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（129 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ，（146 ページ）

LACP ポート プライオリティの設定

デフォルトでは、すべてのポートは同じポート プライオリティです。 ローカル システムのシステム プライオリティおよびシステム ID の値がリモート システムよりも小さい場合は、LACP EtherChannel ポートのポート プライオリティをデフォルトよりも小さい値に変更して、最初にアクティブになるホットスタンバイ リンクを変更できます。 ホット スタンバイ ポートは、番号が小さい方が先にチャネルでアクティブになります。 **show etherchannel summary** 特権 EXEC コマンドを使用して、ホット スタンバイ モードのポートを確認できます（ポートステート フラグが H になっています）。

（注） LACP がすべての互換ポートを集約できない場合（たとえば、ハードウェアの制約が大きいリモート システム）、EtherChannel 中でアクティブにならないポートはすべてホット スタンバイ ステートになり、チャネル化されたポートのいずれかが機能しない場合に限り使用されます。

LACP ポート プライオリティを設定するには、次の手順に従います。 この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **lacp port-priority** *priority*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/2`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**lacp port-priority** *priority* 例： `Switch(config-if)# lacp port-priority 32000`	LACP ポート プライオリティを設定します。 指定できる範囲は 1 ～ 65535 です。 デフォルト値は 32768 です。 値が小さいほど、ポートが LACP 伝送に使用される可能性が高くなります。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

EtherChannel 設定時の注意事項，（128 ページ）
EtherChannel のデフォルト設定，（126 ページ）
レイヤ 2 EtherChannel 設定時の注意事項，（129 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ，（146 ページ）

EtherChannel、PAgP、および LACP ステータスのモニタ

この表に記載されているコマンドを使用して EtherChannel、PAgP、および LACP ステータスを表示できます。

表 *15*：*EtherChannel*、*PAgP*、および *LACP* ステータスのモニタ用コマンド

コマンド	説明
clear lacp ｛*channel-group-number* **counters**｜**counters**｝	LACP チャネル グループ情報およびトラフィック カウンタをクリアします。
clear pagp ｛*channel-group-number* **counters**｜**counters**｝	PAgP チャネル グループ情報およびトラフィック カウンタをクリアします。

コマンド	説明
show etherchannel [*channel-group-number* { **detail** | **port** | **port-channel** | **protocol** | **summary** }] [**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**]	EtherChannel 情報が簡潔、詳細に、1 行のサマリー形式で表示されます。 ロード バランシング方式またはフレーム配布方式、ポート、ポートチャネル、プロトコルの情報も表示されます。
show pagp [*channel-group-number*] { **counters** | **internal** | **neighbor** }	トラフィック情報、内部 PAgP 設定、ネイバー情報などの PAgP 情報が表示されます。
show pagp [*channel-group-number*] **dual-active**	デュアルアクティブ検出ステータスが表示されます。
show lacp [*channel-group-number*] { **counters** | **internal** | **neighbor** | **sys-id**}	トラフィック情報、内部 LACP 設定、ネイバー情報などの LACP 情報が表示されます。
show running-config	設定エントリを確認します。
show etherchannel load-balance	ポート チャネル内のポート間のロード バランシング、またはフレーム配布方式を表示します。

関連トピック

PAgP 学習方式およびプライオリティの設定 , （139 ページ）
PAgP 学習方式およびプライオリティ, （118 ページ）
LACP システム プライオリティの設定, （143 ページ）
LACP ポート プライオリティの設定, （145 ページ）

EtherChannel の設定例

レイヤ 2 EtherChannel の設定：例

この例では、スタック内の 1 つのswitchに EtherChannel を設定する例を示します。 2 つのポートを VLAN 10 のスタティック アクセス ポートとして、PAgP モードが **desirable** であるチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable non-silent
Switch(config-if-range)# end
```

この例では、スタック内の 1 つのswitchに EtherChannel を設定する例を示します。 2 つのポートは VLAN 10 のスタティックアクセス ポートとして、LACP モードが **active** であるチャネル 5 に割り当てられます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

次の例では、クロススタック EtherChannel を設定する方法を示します。 LACP passive モードを使用して、VLAN 10 内のスタティックアクセス ポートとしてスタック メンバ 1 のポートを 2 つ、スタック メンバ 2 のポートを 1 つチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/4 -5
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode passive
Switch(config-if-range)# exit
Switch(config)# interface gigabitethernet3/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# channel-group 5 mode passive
Switch(config-if)# exit
```

レイヤ 3 EtherChannel の設定：例

この例では、レイヤ 3 インターフェイスの設定方法を示します。 2 つのポートは、LACP モードが **active** であるチャネル 5 に割り当てられます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

この例では、クロススタック レイヤ 3 EtherChannel の設定方法を示します。 スタック メンバー 2 の 2 つのポートとスタック メンバー 3 の 1 つのポートは、LACP active モードでチャネル 7 に割り当てられます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/4 -5
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 7 mode active
Switch(config-if-range)# exit
Switch(config)# interface gigabitethernet3/0/3
Switch(config-if)# no ip address
Switch(config-if)# no switchport
Switch(config-if)# channel-group 7 mode active
```

```
Switch(config-if)# exit
```

LACP ホット スタンバイ ポートの設定：例

この例では、少なくとも 3 個のアクティブ ポートがある場合にアクティブ化される EtherChannel を設定する例を示します（ポート チャネル 2）。これは、7 個のアクティブ ポートとホット スタンバイ ポートとしての最大 9 個の残りのポートから構成されます。

```
Switch# configure terminal
Switch(config)# interface port-channel 2
Switch(config-if)# port-channel min-links 3
Switch(config-if)# lacp max-bundle 7
```

関連トピック

LACP 最大バンドル機能の設定, （141 ページ）
LACP とリンクの冗長性 , （121 ページ）
ポート チャネル最小リンク機能の設定, （142 ページ）
LACP とリンクの冗長性 , （121 ページ）

EtherChannels の追加リファレンス

関連資料

関連項目	マニュアル タイトル
レイヤ 2 コマンド リファレンス	*Layer 2/3 Command Reference (Catalyst 3850 Switches)Layer 2 Command Reference (Cisco WLC 5700 Series)*

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

EtherChannels の機能情報

リリース	変更内容
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	この機能が導入されました。

リリース	変更内容
Cisco IOS XE 3.3SE	LACP最大バンドル機能、ポート チャネルの最小リンク機能のサポートが追加されました。

第 5 章

Flex Link および MAC アドレス テーブル移動更新機能の設定

- 機能情報の確認，153 ページ
- Flex Link および MAC アドレス テーブル移動更新設定の制約事項，154 ページ
- Flex Link および MAC アドレス テーブル移動更新に関する情報，155 ページ
- Flex Link および MAC アドレス テーブル移動更新機能の設定方法，163 ページ
- Flex Link、マルチキャスト高速コンバージェンス、および MAC アドレス テーブル移動更新のモニタ，170 ページ
- Flex Link の設定例，171 ページ
- Flex Link および MAC アドレス テーブル移動更新の追加リファレンス，176 ページ
- Flex Link および MAC アドレス テーブル移動更新の機能情報，177 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

Flex Link および MAC アドレス テーブル移動更新設定の制約事項

- Flex Link はレイヤ 2 ポートおよびポート チャネルだけでサポートされます。
- 最大 16 のバックアップ リンクを設定できます。
- アクティブ リンクには、Flex Link バックアップ リンクを 1 つだけ設定できます。バックアップ リンクは、アクティブ インターフェイスとは異なるインターフェイスにする必要があります。
- インターフェイスは 1 つの Flex Link ペアだけに属します。 インターフェイスは、1 つだけのアクティブ リンクのバックアップ リンクにすることができます。 アクティブ リンクは、別の Flex Link ペアに属することができません。
- どちらのリンクも、EtherChannel に属するポートには設定できません。 ただし、2 つのポート チャネル（EtherChannel 論理インターフェイス）を Flex Link として設定でき、ポート チャネルおよび物理インターフェイスを Flex Link として設定して、ポート チャネルか物理インターフェイスのどちらかをアクティブ リンクにすることができます。
- バックアップ リンクはアクティブ リンクと同じタイプ（ギガビット イーサネットまたはポート チャネル）にする必要はありません。 ただし、スタンバイ リンクがトラフィック転送を開始した場合にループが発生したり動作が変更したりしないように、両方の Flex Link を同様の特性で設定する必要があります。
- Flex Link ポートでは STP がディセーブルになります。 ポート上にある VLAN が STP 用に設定されている場合でも、Flex Link ポートは STP に参加しません。 STP がイネーブルでない場合は、設定されているトポロジでループが発生しないようにしてください。
- Catalyst 3850 および Catalyst 3650 スイッチの組み合わせを含むスイッチ スタックを含めることはできません。

関連トピック

Flex Link ペアのプリエンプション方式の設定 , （164 ページ）
Flex Link の設定, （163 ページ）
Flex Link の設定：例, （171 ページ）
Flex Link の VLAN ロード バランシングの設定 , （166 ページ）
Flex Link における VLAN ロード バランシングの設定：例, （171 ページ）
MAC アドレス テーブル移動更新メッセージの取得および処理用のSwitch設定, （169 ページ）
MAC アドレス テーブル移動更新の設定, （167 ページ）
MAC アドレス テーブル移動更新の設定：例, （173 ページ）

Flex Link および MAC アドレス テーブル移動更新に関する情報

Flex Link

Flex Link は、レイヤ 2 インターフェイス（switch ポートまたはポート チャネル）のペアで、一方のインターフェイスが他方のインターフェイスのバックアップとして機能するように設定されます。 この機能は、スパニングツリー プロトコル（STP）の代替ソリューションです。 ユーザは、STP をディセーブルにしても、基本的リンク冗長性を保つことができます。 Flex Link は、通常、ユーザがswitchで STP を実行したくない場合に、サービス プロバイダーまたは企業ネットワークで設定されます。 switchが STP を実行中の場合は、STP がすでにリンク レベルの冗長性またはバックアップを提供しているため、Flex Link は不要です。

別のレイヤ 2 インターフェイスを Flex Link またはバックアップ リンクとして割り当てることで、1 つのレイヤ 2 インターフェイス（アクティブ リンク）に Flex Link を設定します。 switchesでは、Flex Link を、同じswitchまたはスタックの別のswitch上で使用できます。 リンクの 1 つがアップでトラフィックを転送しているときは、もう一方のリンクがスタンバイ モードで、このリンクがシャットダウンした場合にトラフィックの転送を開始できるように準備しています。 どの時点でも、1 つのインターフェイスのみがリンクアップ ステートでトラフィックを転送しています。 プライマリ リンクがシャットダウンされると、スタンバイ リンクがトラフィックの転送を開始します。 アクティブ リンクがアップに戻った場合はスタンバイ モードになり、トラフィックが転送されません。 STP は Flex Link インターフェイス上ではディセーブル化されています。

関連トピック

Flex Link ペアのプリエンプション方式の設定 , （164 ページ）
Flex Link の設定, （163 ページ）
Flex Link の設定：例, （171 ページ）

Flex Link の設定

次の図では、switch A のポート 1 および 2 がアップリンク スイッチ B および C に接続されています。 これらのスイッチは Flex Link として設定されているので、どちらかのインターフェイスがトラフィックを転送し、もう一方のインターフェイスはスタンバイ モードになります。 ポート 1 がアクティブ リンクになる場合、ポート 1 とスイッチ B との間でトラフィックの転送を開始し、ポート 2（バックアップ リンク）とスイッチ C との間のリンクでは、トラフィックは転送されません。 ポート 1 がダウンした場合はポート 2 がアップし、トラフィックをスイッチ C に転送し始めます。 ポート 1 は、再び動作を開始するとスタンバイ モードになり、トラフィックを転送しません。ポート 2 がトラフィック転送を続けます。

また、トラフィックを転送する優先ポートを指定して、プリエンプション機能を設定できます。 たとえば、プリエンプション モードと Flex Link ペアを設定できます。 図のシナリオでは、ポート 1 がバックアップとなって、ポート 2 より帯域幅が大きい場合、ポート 1 は 60 秒後にパケット

の転送を開始します。 ポート 2 がスタンバイとなります。 これを行うには、**switchport backup interface preemption mode bandwidth** および **switchport backup interface preemption delay** インターフェイス コンフィギュレーション コマンドを入力します。

図 *27*：*Flex Link* の設定例

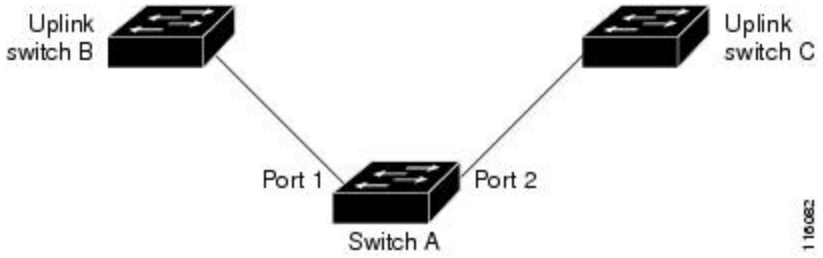
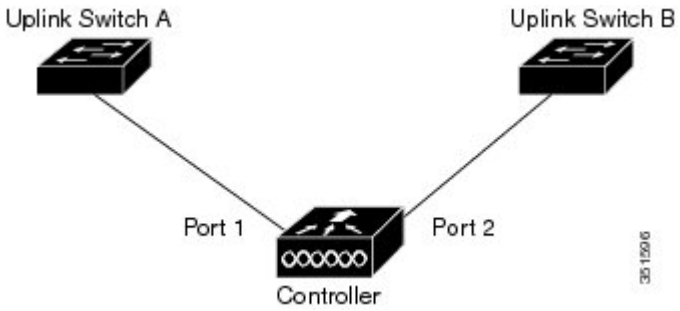


図 *28*：*Flex Link* の設定例



プライマリ（転送）リンクがダウンすると、トラップによってネットワーク管理ステーションが通知を受けます。 スタンバイ リンクがダウンすると、トラップによってユーザが通知を受けます。

Flex Link はレイヤ 2 ポートおよびポート チャネルだけでサポートされ、VLAN またはレイヤ 3 ポートではサポートされません。

関連トピック

Flex Link ペアのプリエンプション方式の設定，（164 ページ）
Flex Link の設定，（163 ページ）

VLAN Flex Link ロード バランシングおよびサポート

VLAN Flex Link ロード バランシングにより、ユーザは相互排他的な VLAN のトラフィックを両方のポートで同時に転送するように Flex Link ペアを設定できます。 たとえば、Flex Link ポートが 1 ～ 100 の VLAN に対して設定されている場合、最初の 50 の VLAN のトラフィックを 1 つのポートで転送し、残りの VLAN のトラフィックをもう一方のポートで転送できます。 どちらかのポートで障害が発生した場合には、もう一方のアクティブ ポートがすべてのトラフィックを転送します。 障害が発生したポートが元に戻ると、優先 VLAN のトラフィックの転送を再開します。

冗長性を提供する以外に、このFlex Linkのペアはロードバランシングに使用できます。 Flex Link VLAN ロード バランシングによってアップリンク switchesが制約を受けることはありません。

次の図に、Flex Link の VLAN ロードバランシング設定を示します。

図 *29*：*VLAN Flex Link* ロード バランシングの設定例

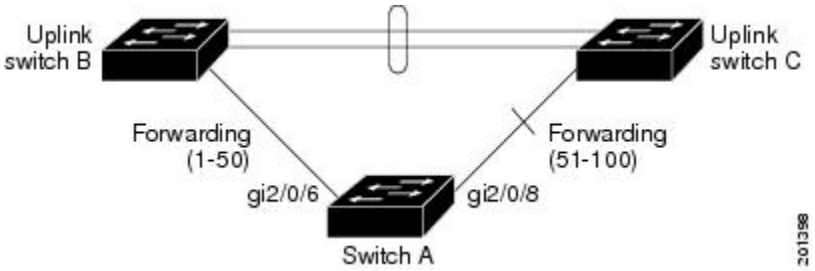
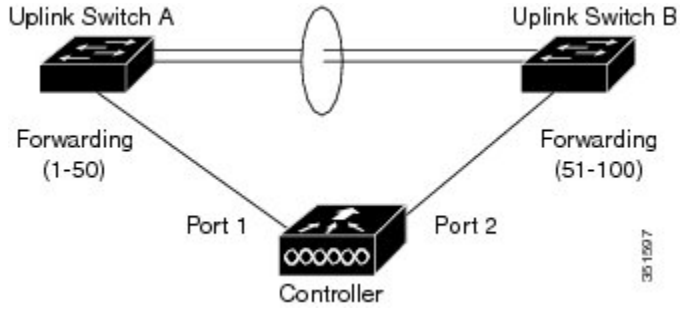


図 *30*：*VLAN Flex Link* ロード バランシングの設定例



Flex Link フェールオーバーによるマルチキャスト高速コンバージェンス

Flex Linkマルチキャスト高速コンバージェンスにより、Flex Link障害発生後のマルチキャスト トラフィック コンバージェンス時間が短縮されます。 マルチキャスト高速コンバージェンスは mrouter ポートとしてのバックアップ リンクの学習、IGMP レポートの生成、およびIGMP レポートのリークを組み合わせて実行されます。

関連トピック

Flex Link フェールオーバーによるマルチキャスト高速コンバージェンスの設定: 例, （173 ページ）

その他の Flex Link ポートを mrouter ポートとして学習

通常のマルチキャスト ネットワークでは、個々の VLAN について 1 つのクエリアが選定されます。 ネットワーク エッジに展開されたswitchには、クエリーを受信するいずれかのFlex Link ポートが存在します。 Flex Link ポートは常に、転送状態になります。

クエリーを受信するポートが、switchの mrouter ポートとして追加されます。 mrouter ポートは、switchが学習したすべてのマルチキャスト グループの 1 つとして認識されます。 切り替えの後、クエリーは別の Flex Link ポートによって受信されます。 この別の Flex Link ポートは mrouter ポートとして認識されるようになります。 切り替えの後、マルチキャスト トラフィックは別の Flex Link ポートを介して流れます。 トラフィック コンバージェンスを高速化するために、いずれかの Flex Link ポートが mrouter ポートとして学習されると、両方の Flex Link ポートが mrouter ポートとして認識されます。 いずれの Flex Link ポートも常に、マルチキャスト グループの一部として扱われます。

通常の動作モードではいずれの Flex Link ポートもグループの一部として認識されますが、バックアップ ポートを通過するトラフィックはすべてブロックされます。 mrouter ポートとしてバックアップ ポートを追加しても、通常のマルチキャスト データ フローが影響を受けることはありません。切り替えが生じると、バックアップポートのブロックが解除され、トラフィックが流れるようになります。この場合、バックアップポートのブロックが解除されるとただちに、アップストリーム データが流れ始めます。

IGMP レポートの生成

切り替えの後、バックアップ リンクがアップ状態になると、アップストリームでの新しいディストリビューション switchでのマルチキャスト データの転送は開始されません。これは、ブロックされた Flex Link ポートに接続されているアップストリーム ルータのポートが、マルチキャスト グループの一部として認識されないからです。 マルチキャスト グループのレポートは、バックアップ リンクがブロックされているため、ダウンストリーム switchで転送されませんでした。 このポートのデータは、マルチキャストグループが学習されるまで流れません。マルチキャストグループの学習は、レポートを受信した後にだけ行われます。

レポートは、一般クエリーが受信されると、ホストより送信されます。一般クエリーは、通常のシナリオであれば 60 秒以内に送信されます。 バックアップ リンクが転送を開始し、マルチキャスト データの高速コンバージェンスを達成できるようになると、ダウンストリーム switchが一般クエリーを待つことなく、ただちにこのポート上のすべての学習済みグループに対し、プロキシレポートを送信します。

IGMP レポートのリーク

マルチキャスト トラフィック コンバージェンスを最小限の損失で達成できるように、Flex Link のアクティブ リンクがダウンする前に冗長データ パスを設定しておく必要があります。 これは、Flex Link バックアップ リンクで IGMP レポート パケットだけをリークさせることで行えます。こうしてリークさせた IGMP レポート メッセージがアップストリームのディストリビューション ルータで処理されるため、マルチキャストデータのトラフィックはバックアップインターフェイスに転送されます。 バックアップ インターフェイスの着信トラフィックはすべてアクセス switch の入り口部分でドロップされるため、ホストが重複したマルチキャスト トラフィックを受信することはありません。 Flex Link のアクティブ リンクに障害が発生した場合、ただちにアクセス switchがバックアップ リンクからのトラフィックを受け入れ始めます。 このスキームの唯一の欠点は、ディストリビューション switches間のリンク、およびディストリビューションとアクセス switchesの間のバックアップ リンクで帯域幅が大幅に消費される点です。 この機能はデフォルト

でディセーブルになっています。**switchport backup interface** *interface-id* **multicast fast-convergence** コマンドを使用して、設定を変更できます。

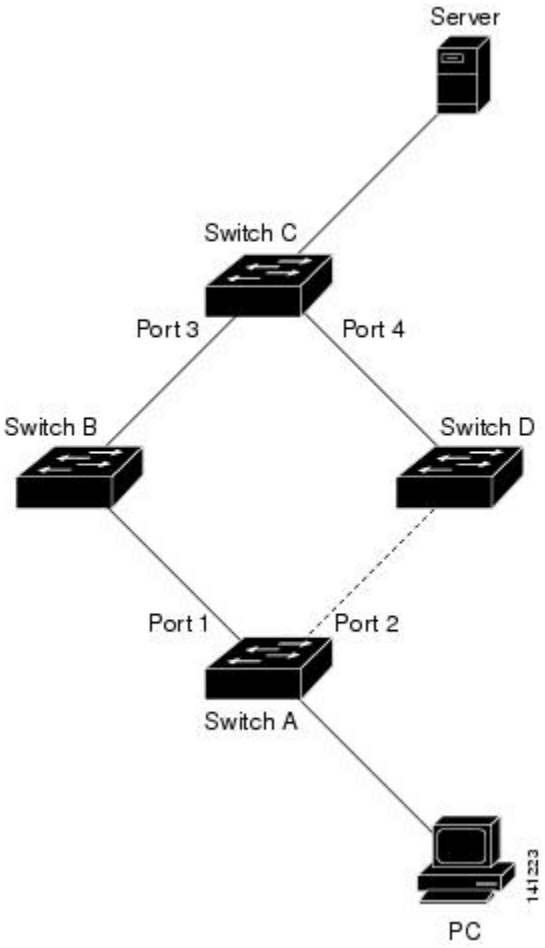
切り替え時にこの機能がイネーブルになっている場合、switchで転送ポートに設定されたバックアップ ポート上でプロキシ レポートは生成されません。

MAC アドレス テーブル移動更新

MAC アドレス テーブル移動更新機能により、プライマリ（転送）リンクがダウンしてスタンバイ リンクがトラフィックの転送を開始したときに、switchで高速双方向コンバージェンスが提供されます。

次の図では、スイッチ A がアクセス スイッチで、スイッチ A のポート 1 および 2 が Flex Link ペア経由でアップリンク switches B および D に接続されます。 ポート 1 はトラフィックの転送中で、ポート 2 はバックアップ ステートです。 PC からサーバへのトラフィックはポート 1 からポート 3 に転送されます。 PC の MAC アドレスが、switch C のポート 3 で学習されています。 サーバから PC へのトラフィックはポート 3 からポート 1 に転送されます。

図 *31*：*MAC* アドレス テーブル移動更新の例



MAC アドレス テーブル移動更新機能が設定されておらず、ポート 1 がダウンした場合は、ポート 2 がトラフィックの転送を開始します。 しかし、少しの間、switch C がポート 3 経由でサーバから PC にトラフィックを転送し続けるため、ポート 1 がダウンしていることにより、PC へのトラフィックが途切れます。 switch C がポート 3 で PC の MAC アドレスを削除し、ポート 4 で再度学習した場合は、トラフィックはポート 2 経由でサーバから PC へ転送される可能性があります。

switches で MAC アドレス テーブル移動更新機能が設定されイネーブル化されていると、ポート 1 がダウンした場合、ポート 2 が PC からサーバへのトラフィックの転送を開始します。 switchは、ポート 2 から MAC アドレス テーブル移動更新パケットを送信します。 Switch C はこのパケットをポート 4 で受信し、ただちにポート 4 で PC の MAC アドレスを学習します。これにより、再コンバージェンス時間が短縮されます。

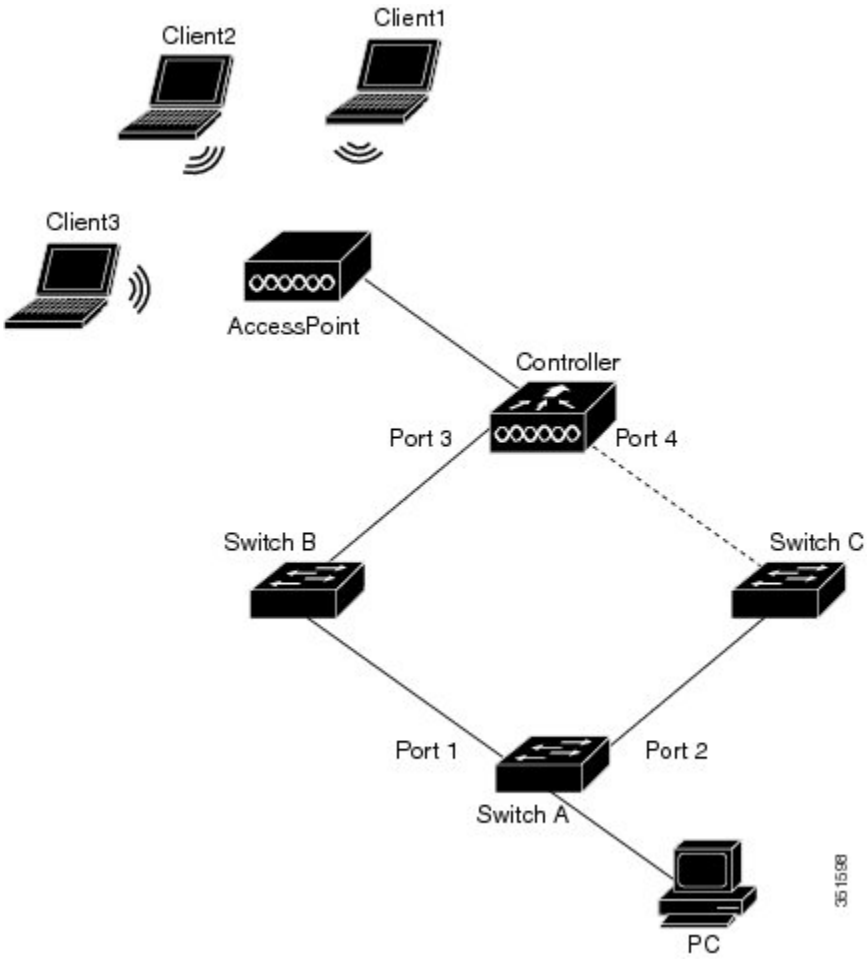
switch、switch A のアクセスを設定して、MAC アドレス テーブル移行更新メッセージを送信できます。 また、アップリンク switches B、C、および D を設定して、MAC アドレス テーブル移動更新メッセージの取得および処理を行うこともできます。 switch C が switch A から MAC アドレス テーブル移動更新メッセージを取得すると、switch C はポート 4 で PC の MAC アドレスを学習します。 Switch C は、PC の転送テーブル エントリ転送を含め、MAC アドレス テーブルをアップデートします。

Switch A が、MAC アドレス テーブル移動更新を待機する必要はありません。 switch はポート 1 上の障害を検出して、ただちに新しい転送ポートであるポート 2 からのサーバ トラフィックの転送を開始します。 この変更は 100 ミリ秒 (ms) 未満で発生します。 PC はswitch A に直接接続され、その接続状態に変更はありません。 Switch A による、MAC アドレス テーブルで PC エントリの更新は必要ありません。

次の図では、コントローラとスイッチ B および C は Flex Link ペア経由で Flexlink を形成します。ポート 3 はトラフィックの転送中で、ポート 2 はバックアップ ステートです。 スイッチ A はア

クセス スイッチで、スイッチ A のポート 1 および 2 がアップリンク スイッチ B および C に接続されます。 無線クライアントの MAC アドレスは、スイッチ A のポート 1 で学習済みです。

図 *32* : ***MAC*** アドレス テーブル移動更新の例



上の図では、3 個の無線クライアントがアクセスポイントに接続し、コントローラと通信します。スイッチ A に接続された PC は、ポート 3 からポート 1 へのデータ パスを介して無線クライアントと通信します。 MAC アドレステーブル移動更新機能がコントローラで設定されておらず、ポート 3 がダウンした場合は、ポート 4 がトラフィックの転送を開始します。 ただし、少しの間は、ポート 3 がダウンしているため、無線クライアントがトラフィックを PC に渡すことはできません。

MAC アドレス テーブル移動更新機能がコントローラで設定されイネーブル化されており、ポート 3 がダウンした場合は、コントローラがポート 4 から MAC アドレス テーブル移動更新パケット（MMU）を送信します。 この MMU のパケットは無線クライアントのすべての MAC アドレスを伝送します。 スイッチ C はポート 4 でこのパケットを取得し、ただちに無線クライアントの MAC アドレスを学習します。これにより、再コンバージェンス時間が短縮されます。 PC はポート 2 からポート 4 へのパスを使用して、無線クライアントにデータを送信します。 スイッチ C はまた、VLAN で同じ MMU パケットをブリッジングします。これにより、ネットワークのすべて

のスイッチで MAC アドレス テーブルが更新され、無線クライアントへの次のパケットがコントローラに対して適切なパスに向かうようになります。 コントローラは無線クライアントの MAC アドレスだけを学習します。

関連トピック

MACアドレステーブル移動更新メッセージの取得および処理用のSwitch設定，（169ページ）
MAC アドレス テーブル移動更新の設定，（167 ページ）
MAC アドレス テーブル移動更新の設定：例，（173 ページ）

Flex Link の VLAN ロード バランシング設定時の注意事項

- Flex Link VLAN ロード バランシングでは、バックアップ インターフェイス上で優先される VLAN を選択する必要があります。
- 同じ Flex Link ペアに対して、プリエンプション メカニズムと VLAN ロード バランシングを設定することはできません。

関連トピック

Flex Link の VLAN ロード バランシングの設定，（166 ページ）
Flex Link における VLAN ロード バランシングの設定：例，（171 ページ）

MAC アドレス テーブル移動更新設定時の注意事項

- アクセス switchでこの機能のイネーブル化と設定を行うと、MAC アドレス テーブル移動更新を送信（*send*）できます。
- MAC アドレス テーブル移動更新メッセージを取得（*get*）する場合、この機能をアップリンク switchesでイネーブルにして設定します。

デフォルトの Flex Link および MAC アドレス テーブル移動更新の設定

- Flex Link は設定されておらず、バックアップ インターフェイスは定義されていません。
- プリエンプション モードはオフです。
- プリエンプション遅延は 35 秒です。
- MAC アドレス テーブル移動更新機能は、 switch上で設定されません。

関連トピック

Flex Link ペアのプリエンプション方式の設定，（164 ページ）
Flex Link の設定，（163 ページ）

Flex Link の設定：例, （171 ページ）

Flex Link および MAC アドレス テーブル移動更新機能の設定方法

Flex Link の設定

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport backup interface** *interface-id*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(conf)# interface gigabitethernet1/0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。 ポートチャネル範囲は 1 ～ 128 です。
ステップ 3	**switchport backup interface** *interface-id* 例： `Switch(conf-if)# switchport backup interface gigabitethernet1/0/2`	物理レイヤ 2 インターフェイス（ポート チャネル）をインターフェイスがある Flex Link ペアの一部として設定します。 1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 4	**end** 例： `Switch(conf-if)# end`	特権 EXEC モードに戻ります。

関連トピック

Flex Link, （155 ページ）
デフォルトの Flex Link および MAC アドレス テーブル移動更新の設定, （162 ページ）
Flex Link および MAC アドレス テーブル移動更新設定の制約事項, （154 ページ）
Flex Link の設定：例, （171 ページ）
Flex Link の設定, （155 ページ）
Flex Link、マルチキャスト高速コンバージェンス、および MAC アドレス テーブル移動更新のモニタ, （170 ページ）
Flex Link の設定：例, （171 ページ）

Flex Link ペアのプリエンプション方式の設定

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport backup interface** *interface-id*
4. **switchport backup interface** *interface-id* **preemption mode** [**forced** | **bandwidth** | **off**]
5. **switchport backup interface** *interface-id* **preemption delay** *delay-time*
6. **end**
7. **show interface** [*interface-id*] **switchport backup**
8. **copy running-config startup config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(conf)# interface gigabitethernet1/0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。 ポートチャネル範囲は 1 ～ 128 です。

	コマンドまたはアクション	目的
ステップ 3	**switchport backup interface** *interface-id* 例： `Switch(conf-if)# switchport backup interface gigabitethernet1/0/2`	物理レイヤ2インターフェイス（ポート チャネル）をインターフェイスがある Flex Link ペアの一部として設定します。 1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 4	**switchport backup interface** *interface-id* **preemption mode** [**forced** | **bandwidth** | **off**] 例： `Switch(conf-if)# switchport backup interface gigabitethernet1/0/2 preemption mode forced`	Flex Link インターフェイス ペアのプリエンプション メカニズムおよび遅延を設定します。 次のプリエンプション モードを設定することができます。 • **forced**：（任意）アクティブ インターフェイスはバックアップをプリエンプトします。 • **bandwidth**：（任意）より大きい帯域幅のインターフェイスが常にアクティブインターフェイスとして動作します。 • **off**：アクティブからバックアップへのプリエンプトは発生しません。
ステップ 5	**switchport backup interface** *interface-id* **preemption delay** *delay-time* 例： `Switch(conf-if)# switchport backup interface gigabitethernet1/0/2 preemption delay 50`	ポートが他のポートより先に使用されるまでの遅延時間を設定します。 （注） 遅延時間の設定は、forced モードおよび bandwidth モードでのみ有効です。
ステップ 6	**end** 例： `Switch(conf-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show interface** [*interface-id*] **switchport backup** 例： `Switch# show interface gigabitethernet1/0/2 switchport backup`	設定を確認します。
ステップ 8	**copy running-config startup config** 例： `Switch# copy running-config startup`	（任意）switch スタートアップ コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`config`	

関連トピック

Flex Link, （155 ページ）
デフォルトの Flex Link および MAC アドレス テーブル移動更新の設定, （162 ページ）
Flex Link および MAC アドレス テーブル移動更新設定の制約事項, （154 ページ）
Flex Link の設定：例, （171 ページ）
Flex Link の設定, （155 ページ）
Flex Link、マルチキャスト高速コンバージェンス、および MAC アドレス テーブル移動更新のモニタ, （170 ページ）
Flex Link の設定：例, （171 ページ）

Flex Link の VLAN ロード バランシングの設定

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport backup interface** *interface-id* **prefer vlan** *vlan-range*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch (config)# interface gigabitethernet2/0/6`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。ポートチャネル範囲は 1 ～ 128 です。

	コマンドまたはアクション	目的
ステップ 3	**switchport backup interface** *interface-id* **prefer vlan** *vlan-range* 例： `Switch (config-if)# switchport backup interface gigabitethernet2/0/8 prefer vlan 2`	物理レイヤ 2 インターフェイス（またはポート チャネル）を、インターフェイスを装備した Flex Link ペアの一部として設定し、インターフェイス上の VLAN を指定します。VLAN ID の範囲は 1 ～ 4094 です。
ステップ 4	**end** 例： `Switch (config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

Flex Link の VLAN ロード バランシング設定時の注意事項，（162 ページ）
Flex Link および MAC アドレス テーブル移動更新設定の制約事項，（154 ページ）
Flex Link における VLAN ロード バランシングの設定：例，（171 ページ）
Flex Link における VLAN ロード バランシングの設定：例，（171 ページ）
Flex Link、マルチキャスト高速コンバージェンス、および MAC アドレス テーブル移動更新のモニタ，（170 ページ）

MAC アドレス テーブル移動更新の設定

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. 次のいずれかを使用します。
   - **switchport backup interface** *interface-id*
   - **switchport backup interface** *interface-id* **mmu primary vlan** *vlan-id*
4. **end**
5. **mac address-table move update transmit**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch#interface gigabitethernet1/0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスは物理レイヤ2インターフェイスまたはポートチャネル（論理インターフェイス）に設定できます。 ポートチャネル範囲は 1 ～ 128 です。
ステップ 3	次のいずれかを使用します。 • **switchport backup interface** *interface-id* • **switchport backup interface** *interface-id* **mmu primary vlan** *vlan-id* 例： `Switch(config-if)# switchport backup interface gigabitethernet0/2 mmu primary vlan 2`	物理レイヤ2インターフェイス（またはポートチャネル）を、インターフェイスを装備した Flex Link ペアの一部として設定します。 MAC アドレス テーブル移動更新 VLAN はインターフェイスで最も低い VLAN ID です。 物理レイヤ2インターフェイス（ポートチャネル）を設定し、MAC アドレス テーブル移動更新の送信に使用される VLAN ID をインターフェイスで指定します。 1つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 4	**end** 例： `Switch(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**mac address-table move update transmit** 例： `Switch(config)# mac address-table move update transmit`	プライマリ リンクがダウンし、スタンバイ リンクを介してswitchがトラフィックの転送を開始すると、アクセスswitchで、ネットワークの他のswitchesに MAC アドレス テーブル移動更新を送信できます。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MAC アドレス テーブル移動更新の設定：例，（173 ページ）
Flex Link、マルチキャスト高速コンバージェンス、およびMAC アドレス テーブル移動更新のモニタ，（170 ページ）
MAC アドレス テーブル移動更新，（159 ページ）
Flex Link および MAC アドレス テーブル移動更新設定の制約事項，（154 ページ）
MAC アドレス テーブル移動更新の設定：例，（173 ページ）

MAC アドレス テーブル移動更新メッセージの取得および処理用のSwitch設定

手順の概要

1. **configure terminal**
2. **mac address-table move update receive**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac address-table move update receive** 例： `Switch (config)# mac address-table move update receive`	switchで MAC アドレス テーブル移動更新の取得と処理を可能にします。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Switch (config)# end`	特権 EXEC モードに戻ります。

関連トピック

Flex Link、マルチキャスト高速コンバージェンス、および MAC アドレス テーブル移動更新のモニタ, （170 ページ）
MAC アドレス テーブル移動更新の設定：例, （173 ページ）
MAC アドレス テーブル移動更新, （159 ページ）
Flex Link および MAC アドレス テーブル移動更新設定の制約事項, （154 ページ）
MAC アドレス テーブル移動更新の設定：例, （173 ページ）

Flex Link、マルチキャスト高速コンバージェンス、および MAC アドレス テーブル移動更新のモニタ

コマンド	目的
show interface [*interface-id*] **switchport backup**	インターフェイス用に設定された Flex Link バックアップ インターフェイス、または設定されたすべての Flex Link と、各アクティブ インターフェイスおよびバックアップ インターフェイスの状態（アップまたはスタンバイ モード）を表示します。
show ip igmp profile address-table move update *profile-id*	特定の IGMP プロファイルまたはswitch上で定義されているすべての IGMP プロファイルを表示します。
show mac address-table move update	switch上に MAC アドレス テーブル移動移動を表示します。

関連トピック

Flex Link ペアのプリエンプション方式の設定 , （164 ページ）
Flex Link の設定, （163 ページ）

Flex Link の設定例

Flex Link の設定：例

この例では、バックアップ インターフェイスでインターフェイスを設定した後に、設定を確認する方法を示します。

```
Switch# show interface switchport backup

Switch Backup Interface Pairs:
Active Interface Backup Interface State
------------------------------------------------------------------------
GigabitEthernet1/0/1 GigabitEthernet1/0/2 Active Up/Backup Standby
```

この例では、バックアップ インターフェイス ペアにプリエンプション モードを強制として設定した後に、設定を確認する方法を示します。

```
Switch# show interface switchport backup detail

Switch Backup Interface Pairs:

Active Interface Backup Interface State
------------------------------------------------------------------------
GigabitEthernet1/0/211 GigabitEthernet1/0/2 Active Up/Backup Standby
Interface Pair : Gi1/0/1, Gi1/0/2
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : 100000 Kbit (Gi1/0/1), 100000 Kbit (Gi1/0/2)
Mac Address Move Update Vlan : auto
```

関連トピック

Flex Link ペアのプリエンプション方式の設定 , （164 ページ）
Flex Link の設定, （163 ページ）
Flex Link, （155 ページ）
デフォルトの Flex Link および MAC アドレス テーブル移動更新の設定, （162 ページ）
Flex Link および MAC アドレス テーブル移動更新設定の制約事項, （154 ページ）
Flex Link ペアのプリエンプション方式の設定 , （164 ページ）
Flex Link の設定, （163 ページ）

Flex Link における VLAN ロード バランシングの設定：例

次の例では、switchに VLAN 1 ～ 50、60、および 100 ～ 120 を設定する例を示します。

```
Switch(config)# interface gigabitethernet 2/0/6
Switch(config-if)# switchport backup interface gigabitethernet 2/0/8 prefer vlan 60,100-120
```

両方のインターフェイスが起動しているとき、Gi2/0/8 は VLAN 60 および 100 ～ 120 のトラフィックを転送し、Gi2/0/6 は VLAN 1 ～ 50 のトラフィックを転送します。

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Up/Backup Standby

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがダウンすると（LINK_DOWN）、このインターフェイスで優先される VLAN は、Flex Link ペアのピア インターフェイスに移動します。 この例では、インターフェイス Gi2/0/6 がダウンして、Gi2/0/8 が Flex Link ペアのすべての VLAN を引き継ぎます。

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

FlexLink インターフェイスがアップになると、このインターフェイスで優先される VLAN はピア インターフェイスでブロックされ、アップしたインターフェイスでフォワーディング ステートに移動します。 この例では、インターフェイス Gi2/0/6 がアップになると、このインターフェイスの優先 VLAN は、相手側のインターフェイス Gi2/0/8 でブロックされ、Gi2/0/6 で転送されます。

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Up/Backup Standby

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120

Switch# show interfaces switchport backup detail

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
FastEthernet1/0/3       FastEthernet1/0/4       Active Down/Backup Up

Vlans Preferred on Active Interface: 1-2,5-4094
Vlans Preferred on Backup Interface: 3-4
Preemption Mode  : off
Bandwidth : 10000 Kbit (Fa1/0/3), 100000 Kbit (Fa1/0/4)
Mac Address Move Update Vlan : auto
```

関連トピック

Flex Link の VLAN ロード バランシングの設定 , （166 ページ）
Flex Link の VLAN ロード バランシング設定時の注意事項, （162 ページ）

Flex Link および MAC アドレス テーブル移動更新設定の制約事項, （154 ページ）
Flex Link の VLAN ロード バランシングの設定 , （166 ページ）

MAC アドレス テーブル移動更新の設定：例

この例では、MACアドレステーブル移動更新を送信するためアクセスswitchを設定した後に設定を確認する方法を示します。

```
Switch# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 5
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 000b.462d.c502
Rcv last switch-ID : 0403.fd6a.8700
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

関連トピック

MAC アドレス テーブル移動更新の設定, （167 ページ）
MACアドレステーブル移動更新メッセージの取得および処理用のSwitch設定, （169ページ）
MACアドレステーブル移動更新メッセージの取得および処理用のSwitch設定, （169ページ）
MAC アドレス テーブル移動更新の設定, （167 ページ）
MAC アドレス テーブル移動更新, （159 ページ）
Flex Link および MAC アドレス テーブル移動更新設定の制約事項, （154 ページ）

Flex Link フェールオーバーによるマルチキャスト高速コンバージェンスの設定: 例

次に、Flex Link を GigabitEthernet1/0/11 および GigabitEthernet1/0/12 に設定したときに他の Flex Link ポートを mrouter ポートとして学習する例と、**show interfaces switchport backup** コマンドの出力を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet1/0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport backup interface GigabitEthernet1/0/12
```

```
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet1/0/12
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface Backup Interface State
GigabitEthernet1/0/11 GigabitEthernet1/0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : Off
Bandwidth : 100000 Kbit (Gi1/0/11), 100000 Kbit (Gi1/0/12)
Mac Address Move Update Vlan : auto
```

この出力は、GigabitEthernet1/0/11 を介してswitchに到達するクエリーのある、VLAN 1 および 401 のクエリアを示します。

```
Switch# show ip igmp snooping querier

Vlan   IP Address     IGMP Version      Port
-----------------------------------------------------------------
1      1.1.1.1        v2      Gi1/0/11
401    41.41.41.1     v2      Gi1/0/11
```

この例では、VLAN 1 および VLAN 401 用の **show ip igmp snooping mrouter** コマンドの出力を示します。

```
Switch# show ip igmp snooping mrouter

Vlan   ports
----   -----
1     Gi1/0/11(dynamic), Gi1/0/12(dynamic)
401   Gi1/0/11(dynamic), Gi1/0/12(dynamic)
```

同様に、両方の Flex Link ポートが学習されたグループに属しています。 次の例では、GigabitEthernet2/0/11 は VLAN 1 のレシーバ/ホストであり、2 つのマルチキャスト グループに関連しています。

```
Switch# show ip igmp snooping groups

Vlan   Group    Type   Version    Port List
------------------------------------------------------------------------
1   228.1.5.1    igmp   v2    Gi1/0/11, Gi1/0/12, Gi2/0/11
1   228.1.5.2    igmp   v2    Gi1/0/11, Gi1/0/12, Gi2/0/11
```

ホストが一般クエリーに応答するときに、switchはすべてのマルチキャスト ルータ ポートに関するこのレポートを転送します。 次の例では、ホストがグループ 228.1.5.1 のレポートを送信するとき、バックアップ ポート GigabitEthernet1/0/12 はブロックされているので、レポートは GigabitEthernet1/0/11 でだけ送信されます。 アクティブ リンク GigabitEthernet1/0/11 がダウンすると、バックアップ ポート GigabitEthernet1/0/12 が転送を開始します。

このポートが転送を開始すると、ただちにswitchがホストに代わり、228.1.5.1 と 228.1.5.2 のグループにプロキシ レポートを送信します。 アップストリーム ルータはグループを学習し、マルチキャストデータの転送を開始します。 これは、Flex Link のデフォルトの動作です。 ユーザが **switchport backup interface gigabitEthernet 1/0/12 multicast fast-convergence** コマンドを使用して高速コンバージェンスを設定すると、この動作は変更になります。 次に、この機能をオンにする例を示します。

```
Switch# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitEthernet 1/0/11
Switch(config-if)# switchport backup interface gigabitEthernet 1/0/12 multicast
fast-convergence
Switch(config-if)# exit
Switch# show interfaces switchport backup detail

Switch Backup Interface Pairs:
Active       Interface       Backup Interface State
------------------------------------------------------------------------
GigabitEthernet1/0/11  GigabitEthernet1/0/12  Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : On
Bandwidth : 100000 Kbit (Gi1/0/11), 100000 Kbit (Gi1/0/12)
Mac Address Move Update Vlan : auto
```

この出力は、GigabitEthernet1/0/11 を介してswitchに到達するクエリーのある、VLAN 1 および 401 のクエリアを示します。

```
Switch# show ip igmp snooping querier

Vlan    IP Address      IGMP Version     Port
-----------------------------------------------------------
1       1.1.1.1         v2      Gi1/0/11
401     41.41.41.1      v2      Gi1/0/11
```

次に VLAN 1 と 401 に対する **show ip igmp snooping mrouter** コマンドの出力を示します。

```
Switch# show ip igmp snooping mrouter

Vlan    ports
----    -----
1    Gi1/0/11(dynamic), Gi1/0/12(dynamic)
401    Gi1/0/11(dynamic), Gi1/0/12(dynamic)
```

同様に、両方の Flex Link ポートが学習されたグループに属しています。 次の例では、GigabitEthernet2/0/11 は VLAN 1 のレシーバ/ホストであり、2 つのマルチキャスト グループに関連しています。

```
Switch# show ip igmp snooping groups

Vlan   Group    Type   Version    Port List
------------------------------------------------------------------------
1   228.1.5.1    igmp   v2    Gi1/0/11, Gi1/0/12, Gi2/0/11
1   228.1.5.2    igmp   v2    Gi1/0/11, Gi1/0/12, Gi2/0/11
```

一般クエリーに対してあるホストが応答すると必ず、switchがすべての mrouter ポートに関するこのレポートを転送します。 コマンドラインポートを使用してこの機能をオンにすると、レポートは、GigabitEthernet1/0/11 上のswitchによって転送されるときにバックアップ ポート GigabitEthernet1/0/12 にも送信されます。 アップストリーム ルータはグループを学習して、マルチキャスト データの転送を開始しますが、GigabitEthernet1/0/12 がブロックされているため、このマルチキャスト データは入力側で廃棄されます。 アクティブ リンク GigabitEthernet1/0/11 がダウンすると、バックアップ ポート GigabitEthernet1/0/12 が転送を開始します。 マルチキャスト データはすでにアップストリーム ルータによって転送されているので、任意のプロキシ レポートを送信する必要はありません。 レポートをバックアップ ポートにリークすると冗長マルチキャスト パスが設定され、マルチキャスト トラフィック コンバージェンス用の時間が最小限になります。

関連トピック

Flex Link フェールオーバーによるマルチキャスト高速コンバージェンス, （157 ページ）

Flex Link および MAC アドレス テーブル移動更新の追加リファレンス

関連資料

関連項目	マニュアル タイトル
レイヤ 2 コマンド リファレンス	*Layer 2/3 Command Reference (Catalyst 3850 Switches)Layer 2 Command Reference (Cisco WLC 5700 Series)*
switchport backup interface コマンド	*Interface and Hardware Component Command Reference (Catalyst 3850 Switches)Interface Command Reference (Cisco WLC 5700 Series)*

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Flex Link および MAC アドレス テーブル移動更新の機能情報

リリース	変更内容
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	この機能が導入されました。
Cisco IOS XE 3.3SE	Flex Link フェールオーバーにマルチキャスト高速コンバージェンスのサポートが追加されました。

第 6 章

単方向リンク検出の設定

- 機能情報の確認，179 ページ
- UDLD 設定の制約事項，179 ページ
- UDLD について，180 ページ
- UDLD の設定方法，184 ページ
- UDLD のモニタおよびメンテナンス，187 ページ
- UDLD の追加リファレンス，187 ページ
- UDLD の機能情報，188 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

UDLD 設定の制約事項

次に、単方向リンク検出（UDLD）設定の制約事項を示します。

- UDLD 対応ポートが別のswitchの UDLD 非対応ポートに接続されている場合、このポートは単一方向リンクを検出できません。

- モード（通常またはアグレッシブ）を設定する場合、リンクの両側に同じモードを設定します。

注意 ループ ガードは、ポイントツーポイント リンクでのみサポートされます。 リンクの各終端には、STP を実行するデバイスを直接接続することを推奨します。

UDLD について

UniDirectional Link Detection（UDLD）は、光ファイバまたはツイストペア イーサネット ケーブルを通して接続されたデバイスからケーブルの物理設定をモニタリングしたり、単一方向リンクの存在を検出できるようにするためのレイヤ 2 プロトコルです。 このプロトコルが単一方向リンクを正常に識別してディセーブルにするには、接続されたすべてのデバイスで UDLD プロトコルがサポートされている必要があります。 UDLD は単一方向リンクを検出すると、影響を受けるポートをディセーブルにして警報を発信します。 単一方向リンクは、スパニングツリートポロジループをはじめ、さまざまな問題を引き起こす可能性があります。

動作モード

UDLD は、通常（デフォルト）とアグレッシブの 2 つの動作モードをサポートしています。 通常モードの UDLD は、光ファイバ接続におけるポートの誤った接続による単一方向リンクを検出できます。 アグレッシブ モードの UDLD は、光ファイバ リンクおよびツイストペア リンク上の片方向トラフィックと、光ファイバ リンク上のポートの誤った接続による単一方向リンクも検出できます。

通常およびアグレッシブの両モードの UDLD は、レイヤ 1 のメカニズムを使用して、リンクの物理ステータスを学習します。 レイヤ 1 では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。 UDLD は、ネイバー ID の検出、誤って接続されたポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。 自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 と 2 の検出機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

ローカル デバイスが送信したトラフィックをネイバーが受信するにもかかわらず、ネイバーから送信されたトラフィックをローカル デバイスが受信しない場合に、単一方向リンクが発生します。

通常モード

通常モードの UDLD は、光ファイバ ポートの光ファイバが誤って接続されている場合に単一方向リンクを検出しますが、レイヤ 1 メカニズムは、この誤った接続を検出しません。 ポートが正しく接続されていてもトラフィックが片方向である場合、単一方向リンクを検出するはずのレイヤ 1 メカニズムがこの状況を検出できないため、UDLD は単一方向リンクを検出できません。 この場合、論理リンクは不確定と見なされ、UDLD はポートをディセーブルにしません。

UDLD が通常モードのときに、ペアの一方の光ファイバが切断されており、自動ネゴシエーションがアクティブであると、レイヤ 1 メカニズムがリンクの物理的な問題を検出するため、リンクは稼働状態でなくなります。 この場合は、UDLD は何のアクションも行わず、論理リンクは不確定と見なされます。

関連トピック

UDLD のグローバルなイネーブル化, （184 ページ）
インターフェイスでの UDLD のイネーブル化, （185 ページ）

アグレッシブ モード

アグレッシブ モードでは、UDLD はこれまでの検出方法で単一方向リンクを検出します。 アグレッシブ モードの UDLD は、2 つのデバイス間の障害発生が許されないポイントツーポイント リンクの単一方向リンクも検出できます。 また、次のいずれかの問題が発生している場合に、単一方向リンクも検出できます。

- 光ファイバ リンクまたはツイストペア リンクで、ポートの 1 つがトラフィックを送受信できない。
- 光ファイバ リンクまたはツイストペア リンクで、ポートの1つがダウンし、残りのインターフェイスが稼働している。
- ケーブルのうち 1 本の光ファイバが切断されている。

これらの場合、UDLD は影響を受けたポートをディセーブルにします。

ポイントツーポイント リンクでは、UDLD hello パケットをハートビートと見なすことができ、ハートビートがあればリンクは正常です。 逆に、ハートビートがないということは、双方向リンクを再確立できない限り、リンクをシャットダウンする必要があることを意味しています。

レイヤ 1 の観点からケーブルの両方の光ファイバが正常な状態であれば、アグレッシブ モードの UDLD はそれらの光ファイバが正しく接続されているかどうか、およびトラフィックが正しいネイバー間で双方向に流れているかどうかを検出します。 自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは自動ネゴシエーションでは実行できません。

関連トピック

UDLD のグローバルなイネーブル化, （184 ページ）
インターフェイスでの UDLD のイネーブル化, （185 ページ）

単一方向の検出方法

UDLD は、2 つの方法で動作します。

- ネイバー データベース メンテナンス
- イベントドリブン検出およびエコー

関連トピック

UDLD のグローバルなイネーブル化, （184 ページ）
インターフェイスでの UDLD のイネーブル化, （185 ページ）

ネイバー データベース メンテナンス

UDLD は、アクティブな各ポート上で hello パケット（別名アドバタイズまたはプローブ）を定期的に送信して、他の UDLD 対応ネイバーに関して学習し、各デバイスがネイバーに関する情報を常に維持できるようにします。

switchが hello メッセージを受信すると、エージング タイム（ホールド タイムまたは存続可能時間）が経過するまで、情報をキャッシュします。 古いキャッシュ エントリの期限が切れる前に、switchが新しい hello メッセージを受信すると、switchが古いエントリを新しいエントリで置き換えます。

UDLD の実行中にポートがディセーブルになったり、ポート上で UDLD がディセーブルになったり、またはswitchをリセットした場合、UDLD は設定変更の影響を受けるポートの既存のキャッシュ エントリをすべてクリアします。 UDLD は、ステータス変更の影響を受けるキャッシュの一部をフラッシュするようにネイバーに通知するメッセージを 1 つまたは複数送信します。 このメッセージは、キャッシュを継続的に同期するためのものです。

イベントドリブン検出およびエコー

UDLD は検出動作としてエコーを利用します。 UDLD デバイスが新しいネイバーを学習するか、または同期していないネイバーから再同期要求を受信すると、接続の UDLD デバイス側の検出ウィンドウを再起動して、エコー メッセージを返送します。 この動作はすべての UDLD ネイバーに対して同様に行われるため、エコー送信側では返信エコーを受信するように待機します。

検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLD モードに応じてシャットダウンされることがあります。 UDLD が通常モードにある場合、リンクは不確定と見なされ、シャットダウンされない場合があります。 UDLD がアグレッシブ モードにある場合は、リンクは単一方向と見なされ、ポートはディセーブルになります。

関連トピック

UDLD のグローバルなイネーブル化, （184 ページ）
インターフェイスでの UDLD のイネーブル化, （185 ページ）

UDLD リセット オプション

インターフェイスが UDLD でディセーブル化された場合、次のオプションの 1 つを使用して UDLD をリセットできます。

- **udld reset** インターフェイス コンフィギュレーション コマンド。

- **shutdown** インターフェイス コンフィギュレーション コマンドに続いて **no shutdown** インターフェイス コンフィギュレーション コマンドを入力すると、ディセーブル化されたポートを再起動できます。
- **no udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドの後に **udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドを実行すると、ディセーブル化されたポートが再びイネーブルになります。
- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port** [**aggressive**] インターフェイス コンフィギュレーション コマンドを実行すると、ディセーブル化された光ファイバ ポートが再びイネーブルになります。
- **errdisable recovery cause udld** グローバル コンフィギュレーション コマンドを入力すると、UDLD の errdisable ステートから自動回復するタイマーをイネーブルにできます。さらに、**errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンドを入力すると、UDLD の errdisable ステートから回復する時間を指定できます。

関連トピック

UDLD のグローバルなイネーブル化, （184 ページ）
インターフェイスでの UDLD のイネーブル化, （185 ページ）

UDLD のデフォルト設定

表 *16* : *UDLD* のデフォルト設定

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

関連トピック

UDLD のグローバルなイネーブル化, （184 ページ）
インターフェイスでの UDLD のイネーブル化, （185 ページ）

UDLD の設定方法

UDLD のグローバルなイネーブル化

アグレッシブ モードまたは通常モードで UDLD をイネーブルにし、switch上のすべての光ファイバ ポートに設定可能なメッセージ タイマーを設定するには、次の手順に従います。

手順の概要

1. **configure terminal**
2. **udld** {**aggressive** | **enable** | **message time** *message-timer-interval*}
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**udld** {**aggressive** | **enable** | **message time** *message-timer-interval*} 例： `Switch(config)# udld enable message time 10`	UDLD モードの動作を指定します。 • **aggressive**：すべての光ファイバ ポート上で、UDLD をアグレッシブ モードでイネーブルにします。 • **enable**：switch上のすべての光ファイバ ポート上で、UDLD を通常モードでイネーブルにします。 UDLD はデフォルトでディセーブルです。 個々のインターフェイスの設定は、**udld enable** グローバル コンフィギュレーション コマンドの設定を上書きします。 • **message time** *message-timer-interval*：アドバタイズ フェーズに存在し、双方向と検出されたポートにおける UDLD プローブ メッセージ間の時間間隔を設定します。 有効な範囲は 1 ～ 90 秒です。デフォルト値は 15 です。 （注） このコマンドが作用するのは、光ファイバ ポートだけです。 他のポート タイプで UDLD をイネーブルにする場合は、**udld** インターフェイス コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
		UDLD をディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

UDLD のモニタおよびメンテナンス
アグレッシブ モード, （181 ページ）
通常モード, （180 ページ）
単一方向の検出方法, （181 ページ）
イベントドリブン検出およびエコー, （182 ページ）
UDLD リセット オプション, （182 ページ）
UDLD のデフォルト設定, （183 ページ）

インターフェイスでの UDLD のイネーブル化

アグレッシブ モードまたは通常モードをイネーブルにする、またはポート上で UDLD をディセーブルにするには、次の手順に従います。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **udld port** [**aggressive**]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	UDLD 用にイネーブルにするポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**udld port** [**aggressive**] 例： `Switch(config-if)# udld port aggressive`	UDLD はデフォルトでディセーブルです。 • **udld port**：指定されたポート上で、UDLD を通常モードでイネーブルにします。 • **udld port aggressive**：（任意）指定されたポート上でアグレッシブ モードで UDLD をイネーブルにします。 （注） 特定の光ファイバ ポート上で UDLD をディセーブルにする場合は、**no udld port** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

UDLD のモニタおよびメンテナンス
アグレッシブ モード, （181 ページ）
通常モード, （180 ページ）
単一方向の検出方法, （181 ページ）
イベントドリブン検出およびエコー, （182 ページ）
UDLD リセット オプション, （182 ページ）
UDLD のデフォルト設定, （183 ページ）

UDLD のモニタおよびメンテナンス

コマンド	目的
show udld [*interface-id* | **neighbors**]	指定されたポートまたはすべてのポートの UDLD ステータスを表示します。

UDLD の追加リファレンス

関連資料

関連項目	マニュアル タイトル
レイヤ 2 コマンド リファレンス	*Layer 2/3 Command Reference (Catalyst 3850 Switches)Layer 2 Command Reference (Cisco WLC 5700 Series)*

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

UDLD の機能情報

リリース	変更内容
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	この機能が導入されました。

索 引

記号

IEEE 802.3ad 120
　「EtherChannel」を参照 120
ポート集約プロトコル 116
　「EtherChannel」を参照 116

B

BackboneFast 87, 99
　イネーブル化 99
　説明 87
BPDU 3, 52, 81
　RSTP 形式 52
　内容 3
　フィルタリング 81

C

CIST リージョナル ルート 41, 43
　「MSTP」を参照 41, 43
CIST ルート 42
　「MSTP」を参照 42

E

EtherChannel 110, 114, 116, 118, 119, 120, 121, 122, 125, 126, 128, 131, 134, 136, 138, 139, 140, 141, 142, 143, 145
　IEEE:802.3ad、説明 120
　LACP 120, 121, 140, 141, 142, 143, 145
　　最小リンク 142
　　最大バンドル 141
　　システム プライオリティ 143
　　ポート プライオリティ 145
　　他の機能との相互作用 121
　　ホット スタンバイ ポート 140
EtherChannel *(続き)*
　LACP *(続き)*
　　モード 120
　PAgP 116, 118, 119, 139
　　学習方式およびプライオリティについて 118
　　学習方式とプライオリティの設定 139
　　集約ポート ラーナー 139
　　集約ポート ラーナーについて 118
　　説明 116
　　他の機能との相互作用 119
　　モード 116
　拡張ロードバランシング 138
　自動作成の 116, 120
　スタック変更、の影響 125
　設定 131, 134
　　レイヤ 2 インターフェイス 131
　　レイヤ 3 134
　設定時の注意事項 128
　相互作用 128
　　STP を使用 128
　チャネル グループ 114
　　の番号 114
　　物理および論理インターフェイスのバインド 114
　デフォルト設定 126
　転送方式 122, 136, 138
　ポートチャネル インターフェイス 114
　　の番号 114
　ロード バランシング 122, 136
　論理インターフェイス、説明 114
EtherChannel ガード 89, 101
　イネーブル化 101
　説明 89
EtherChannel コマンドの設定例 147
EtherChannel | 相互作用 128
　VLAN を使用 128
EtherChannel フェールオーバー 114
「EtherChannel」を参照 116, 120

F

Fast Uplink Transition Protocol 85
Flex Link の VLAN ロード バランシング 156, 162
　設定時の注意事項 162
　説明 156
Flex Link フェールオーバー 157
Flex Link 155, 156, 162, 163, 164, 166, 170, 171, 172
　VLAN ロード バランシングの設定 166
　VLAN ロード バランシングの例 171
　スイッチポート バックアップの例 171
　　強制プリエンプション モードの例 171
　設定 163, 164
　説明 155
　デフォルト設定 162
　プリエンプション方式 164
　モニタリング 170
　優先 VLAN の例 172
　リンクのロード バランシング 156

H

hello タイム 28, 67
　MSTP 67
　STP 28

I

IEEE:802.3ad、説明 120
IEEE 802.1s 37
　「MSTP」を参照 37
IGMP レポートの生成 158
IGMP レポートのリーク 158

L

LACP 111, 120, 121, 131, 140, 141, 142, 143, 145
　最小リンク 142
　最大バンドル 141
　システム プライオリティ 143
　ポート プライオリティ 145
　他の機能との相互作用 121
　ホット スタンバイ ポート 140
　モード 120
LACP ホット スタンバイ ポートの設定：例 149

M

MAC アドレステーブル移動更新 159, 162, 167, 169
　設定 167
　設定時の注意事項 162
　説明 159
　デフォルト設定 162
　メッセージの取得および処理 169
mrouter ポート 157
MSTP 14, 36, 38, 39, 40, 41, 42, 43, 44, 45, 46, 48, 55, 56, 57, 59, 60, 62, 64, 65, 67, 68, 70, 71, 72, 73, 75, 76, 80, 81, 89, 90, 91, 93, 95, 101, 102, 103
　BPDU ガード 81, 93
　　イネーブル化 93
　　説明 81
　BPDU フィルタリング 81, 95
　　イネーブル化 95
　　説明 81
　CIST、説明 41
　CIST リージョナル ルート 41, 43
　CIST ルート 42
　CST 42
　　領域間の動作 42
　EtherChannel ガード 89, 101
　　イネーブル化 101
　　説明 89
　IEEE 802.1D との相互運用性 48, 75
　　移行プロセスの再開 75
　　説明 48
　IEEE 802.1s 42, 46
　　実装 46
　　ポートの役割名の変更 46
　　用語 42
　IST 41
　　領域内の動作 41
　MST 領域 40, 41, 44, 56
　　CIST 41
　　IST 40
　　サポートされるスパニングツリーインスタンス 40
　　設定 56
　　説明 40
　　ホップ カウント メカニズム 44
　PortFast 80, 91
　　イネーブル化 91
　　説明 80
　PortFast 対応ポートのシャットダウン 81
　VLAN から MST インスタンスへのマッピング 57
　インターフェイス ステート、ブロッキングからフォワーディングへ 80

MSTP *(続き)*
拡張システム ID 39, 60
セカンダリ ルート デバイスに対する効果 60
予期しない動作 39
ルート デバイスに対する効果 39
境界ポート 36, 45
設定時の注意事項 36
説明 45
サポートされるインスタンス 14
スタック変更、の影響 48
ステータスの表示 76
ステータス、表示 76
設定 56, 59, 60, 62, 64, 65, 67, 68, 70, 71, 72, 73
ネイバー タイプ 73
設定 56, 59, 60, 62, 64, 65, 67, 68, 70, 71, 72, 73
hello タイム 67
MST 領域 56
高速コンバージェンスのリンク タイプ 72
最大エージング タイム 70
最大ホップ カウント 71
セカンダリ ルート デバイス 60
デバイス プライオリティ 65
転送遅延時間 68
パス コスト 64
ポート プライオリティ 62
ルート デバイス 59
設定時の注意事項 38
デフォルト設定 55
モード間の相互運用性と互換性 14, 36
モードのイネーブル化 56
ルート ガード 90, 102
イネーブル化 102
説明 90
ルート スイッチ選択の防止 90
ルート デバイス 39
拡張システム ID の影響 39
設定 39
予期しない動作 39
ループ ガード 91, 103
イネーブル化 103
説明 91

P

PaGP 111
PAgP 116, 119, 131, 139
「EtherChannel」を参照 116
PAgP *(続き)*
学習方式とプライオリティの設定 139
集約ポート ラーナー 139
説明 116
他の機能との相互作用 119
モード 116
PVST+ 13, 14, 15
IEEE 802.1Q トランキングの相互運用性 15
サポートされるインスタンス 14
説明 13

R

RSTP 48, 49, 50, 51, 52, 53, 54, 72, 75
BPDU 52, 53
形式 52
処理 53
IEEE 802.1D との相互運用性 48, 54, 75
移行プロセスの再開 75
説明 48
トポロジの変更 54
アクティブなトポロジ 49
概要 48
高速コンバージェンス 50, 72
エッジ ポートと PortFast 50
クロススタック高速コンバージェンス 50
説明 50
ポイントツーポイント リンク 50, 72
ルート ポート 50
指定スイッチ、定義済み 49
指定ポート、定義済み 49
ポートのロール 49, 51
説明 49
同期 51
ルート ポート、定義済み 49

S

show interfaces switchport 173
STP 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 19, 20, 22, 23, 25, 26, 28, 30, 31, 32, 36, 82, 84, 87, 89, 97, 98, 99, 101
BackboneFast 87, 99
イネーブル化 99
説明 87
BPDU メッセージ交換 3
EtherChannel ガード 89, 101
イネーブル化 101

STP *(続き)*
EtherChannel ガード *(続き)*
説明 89
IEEE 802.1D とブリッジ ID 5
IEEE 802.1D とマルチキャスト アドレス 12
IEEE 802.1Q トランクでの制限 15
IEEE 802.1t と VLAN 識別子 6
UplinkFast 82, 97, 98
イネーブル化 97
説明 82
ディセーブル化 98
VLAN ブリッジ 15
インターフェイス ステート 7, 8, 9, 10
ディセーブル 10
フォワーディング 8, 10
ブロック 9
ラーニング 9
リスニング 9
概要 2
拡張システム ID 1, 5, 20, 22
概要 5
セカンダリ ルート デバイスに対する効果 22
予期しない動作 1
ルート デバイスに対する効果 20
間接リンク障害の検出 87
キープアライブ メッセージ 3
クロススタック UplinkFast 84
説明 84
サポートされるインスタンス 14
サポートされるプロトコル 13
サポートされるモード 13
指定 定義 5
スイッチ 5
指定ポート、定義済み 5
冗長接続 11
スタックのルート ポートの選択 4
スタック変更、の影響 15
ステータスの表示 32
ステータス、表示 32
設定 17, 20, 22, 23, 25, 26, 28, 30, 31
hello タイム 28
最大エージング タイム 30
スパニングツリー モード 17
セカンダリ ルート デバイス 22
デバイス プライオリティ 26
転送遅延時間 28
転送保留カウント 31
STP *(続き)*
設定 *(続き)*
パス コスト 25
ポート プライオリティ 23
ルート デバイス 20
ディセーブル化 19
デフォルト設定 16
モード間の相互運用性と互換性 14, 36
ルート 1, 4
スイッチ 1, 4
選定 4
予期しない動作 1
ルート デバイス 5, 6, 20
拡張システム ID の影響 5, 20
設定 6
ルート ポート選択の高速化 82
ルート ポート、定義済み 4
STP を使用 128
switchport backup interface 174

U

UDLD 179, 180, 181, 182, 183, 184, 185
アグレッシブ 180, 181
アグレッシブ モード 184
メッセージ タイム 184
イネーブル化 184, 185
インターフェイスごと 185
グローバル 184
エコー検出メカニズム 181, 182
概要 180
制約事項 179
ツイスト ペア リンク 181
通常 180
通常モード 180
ディセーブル化 185
インターフェイスごと 185
デフォルト設定 183
ネイバー データベース 181
ネイバー データベース メンテナンス 182
光ファイバ リンク 181
UplinkFast 82, 97, 98
イネーブル化 97
説明 82
ディセーブル化 98

V

VLAN 12, 15
STP および IEEE 802.1Q トランク 15
VLAN ブリッジ STP 15
ダイナミック アドレスのエージング 12

あ

アクティブ リンク 155, 158, 175
宛先 IP アドレスベース転送 123
宛先 IP アドレス ベース転送、EtherChannel 122
宛先 MAC アドレス転送 122
宛先 MAC アドレス転送、EtherChannel 122
アドレス 12
dynamic 12
迅速なエージング 12
デフォルト エージング 12
multicast 12
STP アドレス管理 12

い

一般クエリー 174

え

エージング時間 28, 68
短縮 28, 68
MSTP 用 68
STP 用 28

か

学習方式とプライオリティの設定 139
拡張システム ID 5, 20, 39
MSTP 39
STP 5, 20
拡張ロードバランシング 138
間接リンク障害の検出、STP 87

き

キープアライブ メッセージ 3

く

クロススタック EtherChannel 110, 112, 128, 131, 134
図 110
設定 131
レイヤ 2 インターフェイス上 131
説明 110
クロススタック UplinkFast、STP 84, 85, 86
Fast Uplink Transition Protocol 85
高速コンバージェンス イベント 86
説明 84
通常コンバージェンス イベント 86

こ

高速コンバージェンス 50
高速スパニングツリー プロトコル 38
「RSTP」を参照 38

さ

サービス プロバイダー ネットワーク、MSTP および RSTP 37
最小リンク 142
最大エージング タイム 30, 70
MSTP 70
STP 30
最大バンドル 141
最大ホップ カウント、MSTP 71

し

システム プライオリティ 143
指定 2, 3
スイッチ 3
ポート 2
自動作成の 116, 120
集約ポート ラーナー 139
冗長性 11, 84, 110
EtherChannel 110
STP 11, 84
バックボーン 11
マルチドロップ バックボーン 84
冗長リンクと UplinkFast 97, 98

す

スタック 3, 4, 14
STP 3, 4
ブリッジ ID 3
ルート ポートの選択 4
サポートされる MSTP インスタンス 14
スイッチ 4, 14
スタックの変更、影響 15, 48, 125, 128
EtherChannel 125
MSTP 48
STP 15
クロススタック EtherChannel 128
スタック変更、の影響 125
スパニングツリー 3, 7
状態 7
ポート プライオリティ 3

せ

制約事項 1, 36, 79
MSTP 36
STP 1
オプションのスパニングツリー機能 79
設定 131
レイヤ 2 インターフェイス 131
レイヤ 2 インターフェイス上 131
説明 110, 116

そ

送信元 IP アドレスベース転送 123
送信元 IP アドレス ベース転送、EtherChannel 122
送信元 IP アドレス ベース転送と宛先 IP アドレス ベース転送、EtherChannel 122
送信元 MAC アドレス転送 122
送信元 MAC アドレス転送、EtherChannel 122
送信元 MAC アドレス転送と宛先 MAC アドレス転送、EtherChannel 122

た

代替 2
ポート 2
ダイナミック アドレス 12
「アドレス」を参照 12
単一スイッチ EtherChannel 112

ち

チャネル グループ 114
の番号 114
物理および論理インターフェイスのバインド 114

つ

ツイスト ペア、単方向リンクの検出 180

て

ディセーブル 10
ステート 10
デバイス 10
ルート 10
デバイス プライオリティ 26, 65
MSTP 65
STP 26
デフォルト設定 16, 55, 126, 162, 183
EtherChannel 126
Flex Link 162
MAC アドレステーブル移動更新 162
MSTP 55
STP 16
UDLD 183
転送遅延時間 28, 68
MSTP 68
STP 28
転送方式 122, 136, 138

の

の番号 114

は

パス コスト 3, 25, 64
MSTP 64
STP 25
バックアップ 2
ポート 2

バックアップ インターフェイス 155
「Flex Link」 を参照 155

ひ

光ファイバ、単一方向リンクの検出 180

ふ

フォールバック ブリッジング 3, 15
STP 3
キープアライブ メッセージ 3
VLAN ブリッジ STP 15
フォワーディング 10
ステート 10
物理および論理インターフェイスのバインド 114
プリエンプション遅延デフォルトの設定 162
プリエンプション デフォルト設定 162
ブリッジ識別子（ブリッジID） 5
ブリッジ プロトコル データ ユニット 3
プロキシ レポート 158
ブロック 9
ステート 9

ほ

ポート 3, 10
プライオリティ 3
ルート 10
ポートチャネル インターフェイス 114
の番号 114
ポート プライオリティ 23, 62, 145
MSTP 62
STP 23
他の機能との相互作用 119, 121
ホット スタンバイ ポート 140

ま

マルチキャスト高速コンバージェンス 157
マルチキャスト高速コンバージェンス 173

も

モード 116, 120
モニタリング 170
Flex Link 170

り

リスニング 9
ステート 9
リファレンス 46
リンクの失敗、単一方向の検出 47
リンクの冗長性 155
「Flex Link」 を参照 155

る

ルート 2, 3, 4
スイッチ 3, 4
ポート 2
ルート デバイス 20, 59
MSTP 59
STP 20

れ

レイヤ 2 EtherChannel 設定時の注意事項 129
レイヤ 2 EtherChannel の設定：例のコマンド 147
レイヤ 2 インターフェイス 131
レイヤ 2 インターフェイス上 131
レイヤ 3 EtherChannel の設定：例のコマンド 148
レイヤ 3 EtherChannel 設定時の注意事項 130

ろ

ロード バランシング 122, 136
ロードバランシングの利点 124
ロール 2
ポート 2
論理インターフェイス、説明 114