Cisco NX-OS Layer 2 Switching コンフィギュレーション ガイド Release 4.0

June 18, 2008

Text Part Number: OL-15907-01-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、米国シスコシステムズ発行ドキュメントの参考和訳です。
米国サイト掲載ドキュメントとの差異が生じる場合があるため、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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性や特定の目的への準拠性、権利を侵害しないことに関する、または取り扱い、使用、または取引によって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコシステムズまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco NX-OS Layer 2 Switching コンフィギュレーション ガイド Release 4.0
Copyright © 2008 Cisco Systems, Inc.
All rights reserved.

Copyright © 2008, シスコシステムズ合同会社 .
All rights reserved.

CONTENTS

はじめに xi

対象読者 xi

マニュアルの構成 xii

表記法 xiii

関連資料 xiv

マニュアルの入手方法および Service Request **ツールの使用** xv

Japan TAC Web **サイト** xv

CHAPTER 1 **概要** 1-1

レイヤ 2 **スイッチング** 1-1

VLAN 1-2

プライベート VLAN 1-2

スパニング ツリー 1-3

STP **の概要** 1-3

Rapid PVST+ 1-3

MST 1-4

STP **拡張機能** 1-4

バーチャライゼーションとレイヤ 2 **スイッチング** 1-5

関連資料 1-6

CHAPTER 2 **レイヤ 2 スイッチングの設定** 2-1

レイヤ 2 **スイッチングの概要** 2-2

レイヤ 2 **スイッチング** 2-2

レイヤ 2 **イーサネット スイッチングの概要** 2-2

セグメント間のフレーム スイッチング 2-3

アドレス テーブルの構築およびアドレス テーブルの変更 2-3

バーチャライゼーションのサポート 2-3

レイヤ 2 **スイッチングのライセンス要件** 2-4

MAC **アドレス設定の前提条件** 2-4

注意事項および制限 2-4

レイヤ 2 **スイッチングの設定** 2-5

スタティック MAC **アドレスの設定** 2-5

MAC **テーブルのエージング タイムの設定** 2-6

MAC テーブルからのダイナミック アドレスのクリア 2-7
レイヤ 2 スイッチング設定の確認 2-8
レイヤ 2 スイッチングの設定例 2-8
デフォルト設定 2-9
追加情報 2-9
関連資料 2-9
標準規格 2-9

CHAPTER 3 VLAN の設定 3-1
VLAN について 3-2
VLAN の概要 3-2
VLAN の範囲 3-4
VLAN の作成、削除、および変更 3-5
ハイ アベイラビリティ 3-6
バーチャライゼーションのサポート 3-6
VLAN のライセンス要件 3-7
VLAN 設定の前提条件 3-7
注意事項および制約事項 3-7
VLAN の設定 3-8
VLAN の作成および削除 3-8
VLAN コンフィギュレーション サブモードの開始 3-9
VLAN の設定 3-11
VLAN 設定の確認 3-12
統計情報の表示とクリア 3-13
VLAN の設定例 3-13
デフォルト設定 3-13
追加情報 3-14
関連資料 3-14
標準規格 3-14
MIB 3-14

CHAPTER 4 プライベート VLAN の設定 4-1
プライベート VLAN について 4-2
プライベート VLAN の概要 4-2
プライベート VLAN のプライマリ VLAN とセカンダリ VLAN 4-3
プライベート VLAN ポート 4-3
プライマリ、独立、およびコミュニティ プライベート VLAN 4-4
プライマリ VLAN とセカンダリ VLAN の関連付け 4-6
プライベート VLAN 内のブロードキャスト トラフィック 4-6

プライベート VLAN ポートの分離 4-7
プライベート VLAN および VLAN インターフェイス 4-7
複数のデバイスにまたがるプライベート VLAN 4-7
ハイ アベイラビリティ 4-8
バーチャライゼーションのサポート 4-8
プライベート VLAN のライセンス要件 4-8
プライベート VLAN の前提条件 4-8
注意事項および制限 4-9
セカンダリ VLAN およびプライマリ VLAN の設定 4-9
プライベート VLAN ポートの設定 4-10
他の機能に関連する制限 4-10
プライベート VLAN の設定 4-12
プライベート VLAN の設定時の注意事項 4-12
プライベート VLAN のイネーブル化 4-13
プライベート VLAN としての VLAN の設定 4-14
プライマリ プライベート VLAN へのセカンダリ VLAN の関連付け 4-15
プライマリ VLAN の VLAN インターフェイスへのセカンダリ VLAN のマッピング 4-17
プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定 4-19
プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定 4-20
プライベート VLAN 設定の確認 4-22
プライベート VLAN の統計情報の表示とクリア 4-22
プライベート VLAN の設定例 4-23
デフォルト設定 4-23
追加情報 4-24
関連資料 4-24
標準規格 4-24
MIB 4-24

CHAPTER 5 Rapid PVST+ の設定 5-1
Rapid PVST+ について 5-2
STP 5-3
概要 5-3
トポロジの作成方法 5-3
ブリッジ ID 5-4
BPDU 5-6
ルート ブリッジの選定 5-6
スパニング ツリー トポロジの作成 5-7

Rapid PVST+ 5-7
概要 5-8
Rapid PVST+ BPDU 5-9
提案合意ハンドシェイク 5-10
プロトコル タイマー 5-11
ポート ロール 5-11
ポート ステート 5-12
ポート ロールの同期化 5-14
単一方向リンク障害の検出 5-16
ポート コスト 5-16
ポート プライオリティ 5-17
Rapid PVST+ および IEEE 802.1Q トランク 5-17
Rapid PVST+ とレガシー 802.1D STP の相互運用性 5-18
Rapid PVST+ と 802.1s MST の相互運用性 5-18
ハイ アベイラビリティ 5-18
バーチャライゼーションのサポート 5-19
Rapid PVST+ のライセンス要件 5-20
Rapid PVST+ を設定するための前提条件 5-20
注意事項および制約事項 5-20
Rapid PVST+ の設定 5-21
Rapid PVST+ の設定に関する注意事項 5-21
Rapid PVST+ のイネーブル化 5-21
Rapid PVST+ の VLAN 単位でのディセーブル化またはイネーブル化 5-23
ルート ブリッジ ID の設定 5-24
セカンダリ ルート ブリッジの設定 5-26
VLAN の Rapid PVST+ ブリッジ プライオリティの設定 5-28
Rapid PVST+ ポート プライオリティの設定 5-29
Rapid PVST+ パスコスト方式およびポート コストの設定 5-30
VLAN の Rapid PVST+ hello タイムの設定 5-32
VLAN の Rapid PVST+ 転送遅延時間の設定 5-33
VLAN の Rapid PVST+ 最大エージング タイムの設定 5-34
リンク タイプの指定 5-35
プロトコルの再初期化 5-36
Rapid PVST+ コンフィギュレーションの確認 5-37
Rapid PVST+ 統計情報の表示およびクリア 5-37
Rapid PVST+ の設定例 5-37
デフォルト設定 5-38
追加情報 5-40

関連資料 5-40
標準規格 5-40
MIB 5-40

CHAPTER 6 MST の設定 6-1
MST について 6-2
MST の概要 6-2
MST 領域 6-3
MST BPDU 6-4
MST コンフィギュレーション情報 6-4
IST、CIST、および CST 6-5
IST、CIST、および CST の概要 6-5
MST 領域内のスパニング ツリー動作 6-6
MST 領域間のスパニング ツリー動作 6-6
MST 用語 6-7
ホップ カウント 6-8
境界ポート 6-8
単一方向リンク障害の検出 6-9
ポート コストおよびポート プライオリティ 6-10
IEEE 802.1D との相互運用性 6-10
ハイ アベイラビリティ 6-11
バーチャライゼーションのサポート 6-11
MST のライセンス要件 6-12
MST の前提条件 6-12
注意事項および制約事項 6-13
MST の設定 6-15
MST のイネーブル化 6-15
MST コンフィギュレーション モードの開始 6-16
MST 名の指定 6-18
MST コンフィギュレーション リビジョン番号の指定 6-19
MST 領域のコンフィギュレーションの指定 6-20
VLAN と MSTI のマッピングおよびマッピング解除 6-23
プライベート VLAN のセカンダリ VLAN をプライマリ VLAN と同じ MSTI にマッピングする方法 6-24
ルート ブリッジの設定 6-26
セカンダリ ルート ブリッジの設定 6-27
スイッチ プライオリティの設定 6-29
ポート プライオリティの設定 6-30
ポート コストの設定 6-31

hello タイムの設定 6-33
転送遅延時間の設定 6-34
最大エージング タイムの設定 6-35
最大ホップ カウントの設定 6-36
リンク タイプの指定 6-37
プロトコルの再初期化 6-38
MST コンフィギュレーションの確認 6-40
MST 統計情報の表示およびクリア 6-40
MST の設定例 6-41
デフォルト設定 6-43
追加情報 6-44
関連資料 6-44
標準規格 6-44
MIB 6-44

CHAPTER 7 STP 拡張機能の設定 7-1
STP 拡張機能の概要 7-2
STP ポート タイプ 7-2
STP エッジ ポート 7-3
ブリッジ保証 7-3
BPDU ガード 7-5
BPDU フィルタリング 7-6
ループ ガード 7-6
ルート ガード 7-7
STP 拡張機能の適用 7-7
PVST シミュレーション 7-8
ハイ アベイラビリティ 7-9
バーチャライゼーションのサポート 7-9
STP 拡張機能のライセンス要件 7-9
STP 拡張機能の前提条件 7-9
注意事項および制限 7-10
STP 拡張機能の設定 7-11
スパニング ツリー ポート タイプのグローバル設定 7-11
特定のインターフェイス上でのスパニング ツリー エッジ ポートの設定 7-13
特定のインターフェイス上でのスパニング ツリー ネットワーク ポートの設定 7-14
BPDU ガードのグローバルなイネーブル化 7-16
特定のインターフェイス上での BPDU ガードのイネーブル化 7-17

BPDU フィルタリングのグローバルなイネーブル化 7-18
特定のインターフェイス上での BPDU フィルタリングのイネーブル化 7-20
ループ ガードのグローバルなイネーブル化 7-21
特定のインターフェイス上でのループ ガードまたはルート ガードのイネーブル化 7-23
PVST シミュレーションのグローバル設定 7-25
ポート単位での PVST シミュレーションの設定 7-26
STP 拡張機能の設定の確認 7-28
STP 拡張機能の設定例 7-28
デフォルト設定 7-29
追加情報 7-30
関連資料 7-30
標準規格 7-30
MIB 7-30

APPENDIX A Cisco NX-OS Release 4.0 レイヤ 2 スイッチング機能の設定の上限 A-1

INDEX 索引

はじめに

ここでは、『*Cisco NX-OS Layer 2 Switching Configuration Guide*』の対象読者、マニュアルの構成、および表記法について説明します。また、関連資料の入手方法についても説明します。

ここで説明する内容は、次のとおりです。

- 対象読者（p.xi）
- マニュアルの構成（p.xii）
- 表記法（p.xiii）
- 関連資料（p.xiv）
- マニュアルの入手方法および Service Request ツールの使用（p.xv）

対象読者

このマニュアルは、NX-OS デバイスの設定およびメンテナンスを担当する、経験豊富なネットワーク管理者を対象としています。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	説明
第 1 章「概要」	各機能を要約して説明します。
第 2 章「レイヤ 2 スイッチングの設定」	MAC アドレス テーブルのパラメータの設定情報について説明します。
第 3 章「VLAN の設定」	VLAN 設定の詳細について説明します。
第 4 章「プライベート VLAN の設定」	プライベート VLAN の設定情報について説明します。
第 5 章「Rapid PVST+ の設定」	IEEE 802.1D Spanning Tree Protocol（STP; スパニング ツリー プロトコル）に関する情報、および Per VLAN Rapid Spanning Tree（Rapid PVST+）設定の詳細について説明します。
第 6 章「MST の設定」	Multiple Spanning Tree（MST）設定の詳細情報について説明します。
第 7 章「STP 拡張機能の設定」	シスコ独自の STP 拡張機能であるブリッジ保証、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）ガード、BPDU フィルタリング、ループ ガード、ルート ガード、および PVST シミュレーションの設定の詳細について説明します。
付録 A「Cisco NX-OS Release 4.0 レイヤ 2 スイッチング機能の設定の上限」	レイヤ 2 スイッチング機能の制限について説明します。

表記法

コマンドの説明では、次の表記法を使用しています。

太字	コマンドおよびキーワードは**太字**で示しています。
イタリック体	ユーザが値を指定する引数は、*イタリック体*で示しています。
{ }	波カッコの中の要素は、必須の選択肢です。
[ ]	角カッコの中の要素は、省略可能です。
x | y | z	どれか 1 つを選択する要素は、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリング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ストリングとみなされます。

出力例では、次の表記法を使用しています。

`screen` フォント	システムが表示する端末セッションおよび情報は、`screen` フォントで示しています。
太字の **`screen`** フォント	ユーザが入力しなければならない情報は、**太字**の **`screen`** フォントで示しています。
*イタリック体*の *`screen`* フォント	ユーザが値を指定する引数は、*イタリック体*の *`screen`* フォントで示しています。
< >	パスワードのように出力されない文字は、かぎカッコ（< >）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。

マニュアルの注記には、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。

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

関連資料

Cisco NX-OS のマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html

Cisco NX-OS のマニュアル セットには、次の資料が含まれます。

リリース ノート

『*Cisco NX-OS Release Notes*』Release 4.0

NX-OS コンフィギュレーション ガイド

『*Cisco NX-OS Getting Started with Virtual Device Contexts*』Release 4.0

『*Cisco NX-OS Fundamentals Configuration Guide*』Release 4.0

『*Cisco NX-OS Interfaces Configuration Guide*』Release 4.0

『*Cisco NX-OS Layer 2 Switching Configuration Guide*』Release 4.0

『*Cisco NX-OS Quality of Service Configuration Guide*』Release 4.0

『*Cisco NX-OS Unicast Routing Configuration Guide*』Release 4.0

『*Cisco NX-OS Multicast Routing Configuration Guide*』Release 4.0

『*Cisco NX-OS Security Configuration Guide*』Release 4.0

『*Cisco NX-OS Virtual Device Context Configuration Guide*』Release 4.0

『*Cisco NX-OS Software Upgrade Guide*』Release 4.0

『*Cisco NX-OS Licensing Guide*』Release 4.0

『*Cisco NX-OS High Availability and Redundancy Guide*』Release 4.0

『*Cisco NX-OS System Management Configuration Guide*』Release 4.0

『*Cisco NX-OS XML Management Interface User Guide*』Release 4.0

『*Cisco NX-OS System Messages Reference*』

『*Cisco NX-OS MIB Quick Reference*』

NX-OS コマンド リファレンス

『*Cisco NX-OS Command Reference Master Index*』Release 4.0

『*Cisco NX-OS Fundamentals Command Reference*』Release 4.0

『*Cisco NX-OS Interfaces Command Reference*』Release 4.0

『*Cisco NX-OS Layer 2 Switching Command Reference*』Release 4.0

『*Cisco NX-OS Quality of Service Command Reference*』Release 4.0

『*Cisco NX-OS Unicast Routing Command Reference*』Release 4.0

『*Cisco NX-OS Multicast Routing Command Reference*』Release 4.0

『*Cisco NX-OS Security Command Reference*』Release 4.0

『*Cisco NX-OS Virtual Device Context Command Reference*』Release 4.0

『*Cisco NX-OS High Availability and Redundancy Command Reference*』Release 4.0

『*Cisco NX-OS System Management Command Reference*』Release 4.0

その他のソフトウェアのマニュアル

『*Cisco NX-OS Troubleshooting Guide*』Release 4.0

マニュアルの入手方法および Service Request ツールの使用

マニュアルの入手方法、Service Request の使用、およびその他の情報の取得については、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が掲載されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation* 』を Really Simple Syndication（RSS）フィードとして登録すると、リーダー アプリケーションを使っ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できます。RSS フィードは無料のサービスです。シスコでは現在、RSS バージョン 2.0 をサポートしています。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。

Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register/

CHAPTER 1

概要

Cisco NX-OS デバイスは、本マニュアル『*Cisco NX-OS Layer 2 Switching Configuration Guide*』で説明するレイヤ 2 機能をサポートしています。

(注) レイヤ 2 セキュリティ機能の情報は、『*Cisco NX-OS Security Configuration Guide*』を参照してください。

この章で説明する内容は、次のとおりです。

- レイヤ 2 スイッチング（p.1-1）
- VLAN（p.1-2）
- プライベート VLAN（p.1-2）
- スパニング ツリー（p.1-3）
- バーチャライゼーションとレイヤ 2 スイッチング（p.1-5）
- 関連資料（p.1-6）

レイヤ 2 スイッチング

このデバイスは、レイヤ 2 イーサネット セグメント間の同時パラレル接続をサポートします。イーサネット セグメント間のスイッチド コネクションが維持されるのは、パケットの伝送時間の長さだけです。次のパケットには、別のセグメント間に新しい接続が確立されます。

レイヤ 2 ポートは、パケット上の MAC（メディア アクセス制御）アドレスを、そのパケットのレイヤ 2 ポート情報に関連付けるテーブルを維持します。MAC テーブルのテーブル内エントリの保持期間や、テーブルからのクリアなどの特定の内容を設定できます。

レイヤ 2 インターフェイスはデフォルト VLAN（VLAN1）に属し、初期設定されるとすぐに Spanning Tree Protocol（STP; スパニング ツリー プロトコル）がイネーブルになります。

レイヤ 2 スイッチングのポート モードの設定および MAC アドレス テーブルの設定の詳細については、第 2 章「レイヤ 2 スイッチングの設定」を参照してください。

VLAN

VLAN は、ユーザの物理的な場所に関係なく、機能、プロジェクト チーム、またはアプリケーションによって論理的にセグメント化されるスイッチド ネットワークです。VLAN には、物理 LAN と同じアトリビュートを備えており、物理的に同じ LAN セグメント上に存在しない端末でもグループ化できます。

VLAN には、任意のスイッチを加入させることができ、ユニキャスト、ブロードキャスト、およびマルチキャストのパケットは、その VLAN 内の端末だけに転送され、フラッディングされます。各 VLAN は 1 つの論理ネットワークとみなされ、VLAN に属していないステーション宛てのパケットは、ブリッジまたはルータを経由して転送される必要があります。

デバイスの初回の起動時は、管理ポートを含むすべてのポートがデフォルト VLAN（VLAN1）に割り当てられます。Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）または VLAN インターフェイスは、VLAN 間の通信用として作成されるレイヤ 3 インターフェイスです。

このデバイスは、IEEE 802.1Q 規格に基づき、4094 の VLAN をサポートします。これらの VLAN はいくつかの範囲に分かれています。各範囲の使用法は少しずつ異なります。一部の VLAN はデバイスの内部使用のために予約されるので、設定には使用できません。

（注） ソフトウェア上では、Inter-Switch Link（ISL; スイッチ間リンク）はサポートされません。

VLAN 設定の詳細については、第 3 章「VLAN の設定」を参照してください。

プライベート VLAN

プライベート VLAN は、レイヤ 2 レベルでのトラフィック分離とセキュリティを提供します。

プライベート VLAN は、同じプライマリ VLAN を使用する、プライマリ VLAN とセカンダリ VLAN の 1 つまたは複数のペアで構成されます。セカンダリ VLAN には、独立 VLAN とコミュニティ VLAN の 2 種類があります。独立 VLAN 内のホストは、プライマリ VLAN 内のホストだけと通信します。コミュニティ VLAN 内のホストは、そのコミュニティ VLAN 内のホスト間およびプライマリ VLAN 内のホストとのみ通信でき、独立 VLAN または他のコミュニティ VLAN 内のホストとは通信できません。

セカンダリ VLAN が独立 VLAN であるかコミュニティ VLAN であるかに関係なく、プライマリ VLAN 内のインターフェイスはすべて、1 つのレイヤ 2 ドメインを構成します。つまり、必要な IP サブネットは 1 つだけです。

プライベート VLAN および関連するプライマリ VLAN とセカンダリ VLAN の設定と使用方法については、第 4 章「プライベート VLAN の設定」を参照してください。

スパニング ツリー

ここでは、ソフトウェア上での STP の実装について説明します。スパニング ツリーは、IEEE 802.1w および IEEE 802.1s の規格を意味します。このマニュアルで IEEE 802.1D 規格の STP について記す場合は、802.1D であることを明記します。

ここでは、次の内容について説明します。

- STP の概要（p.1-3）
- Rapid PVST+（p.1-3）
- MST（p.1-4）
- STP 拡張機能（p.1-4）

STP の概要

STP は、レイヤ 2 レベルで、ループフリー（ループを発生させない）ネットワークを提供します。レイヤ 2 LAN ポートは、一定の間隔で、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）と呼ばれる STP フレームを送受信します。ネットワーク デバイスは、これらのフレームを転送せずに、フレームを使用してループフリー パスを構築します。

802.1D は、オリジナルの STP 規格です。基本的なループフリー STP から、多数の改善を経て拡張されました。Per VLAN Spanning Tree（PVST+）では、各 VLAN に個別にループフリー パスを作成できます。また、機器の高速化に対応して、ループフリー コンバージェンス処理も高速化するために、規格全体が再構築されました。802.1w 規格は、高速コンバージェンスが統合された STP で、Rapid Spanning Tree（RSTP）と呼ばれています。現在では、各 VLAN 用の STP に高速コンバージェンス タイムを実装できます。これが、Per VLAN Rapid Spanning Tree（Rapid PVST+）です。

さらに、802.1s 規格の Multiple Spanning Tree（MST）では、複数の VLAN を単一のスパニング ツリー インスタンスにマッピングできます。各インスタンスは、独立したスパニング ツリー トポロジで実行されます。

ソフトウェアは、従来の 802.1D システムで相互運用できますが、システムでは Rapid PVST+ および MST が実行されます。特定の Virtual Device Context（VDC）に、Rapid PVST+ *または* MST の*どちらか*を使用できます。1 つの VDC で両方を使用することはできません。ソフトウェアのデフォルトの STP プロトコルは、Rapid PVST+ です。

（注） ソフトウェアは、拡張システム ID および MAC アドレス リダクションを使用します。これらの機能をディセーブルにすることはできません。

また、シスコでは独自仕様の機能により、STP の動作を拡張しています（拡張機能の概要については、「STP 拡張機能」（p.1-4）を参照してください）。

Rapid PVST+

Rapid PVST+ は、ソフトウェアのデフォルトのスパニング ツリー モードで、デフォルト VLAN および新規作成のすべての VLAN 上で、デフォルトでイネーブルになります。

設定された各 VLAN 上で RSTP の単一インスタンスまたはトポロジが実行され、VLAN 上の各 Rapid PVST+ インスタンスに 1 つのルート デバイスが設定されます。Rapid PVST+ を実行する場合は、VLAN 単位で STP をイネーブルまたはディセーブルに設定できます。

Rapid PVST+ の設定および実行の詳細については、第 5 章「Rapid PVST+ の設定」を参照してください。

MST

ソフトウェアは、MST もサポートしています。MST を使用した複数の独立したスパニング ツリー トポロジにより、データ トラフィック用に複数の転送パスを提供し、ロード バランスを有効にして、多数の VLAN をサポートするために必要なスパニング ツリー インスタンス数を削減できます。

MST には RSTP が統合されているので、高速コンバージェンスもサポートされます。MST では、1 つのインスタンス（転送パス）で障害が発生しても他のインスタンス（転送パス）に影響しないので、ネットワークの耐障害性が向上します。

（注） スパニング ツリー モードを変更すると、変更前のすべてのスパニング ツリー インスタンスが停止し、新しいモードで再開されるため、トラフィックが中断されます。

MST の設定および実行の詳細については、第 6 章「MST の設定」を参照してください。

STP 拡張機能

ソフトウェアは、以下に示すシスコ独自の機能をサポートしています。

- スパニング ツリー ポート タイプ — デフォルトのスパニング ツリー ポート タイプは、標準（normal）です。レイヤ 2 ホストに接続するインターフェイスをエッジ ポートとして、また、レイヤ 2 スイッチまたはブリッジに接続するインターフェイスをネットワーク ポートとして設定できます。
- ブリッジ保証 — ポートをネットワーク ポートとして設定すると、ブリッジ保証によりすべてのポート上に BPDU が送信され、BPDU を受信しないポートはブロッキング ステートに移行します。この拡張機能を使用できるのは、Rapid PVST+ または MST を実行する場合だけです。
- BPDU ガード — BPDU ガードは、BPDU を受信したポートをシャットダウンします。
- BPDU フィルタ — BPDU フィルタは、ポート上での BPDU の送受信を抑制します。
- ループ ガード — ループ ガードは、非指定ポートが STP フォワーディング ステートに移行するのを阻止し、ネットワーク上でのループの発生を防止します。
- ルート ガード — ルート ガードは、ポートが STP トポロジのルートにならないように防御します。

これらの STP 拡張機能の設定および実行の詳細については、第 7 章「STP 拡張機能の設定」を参照してください。

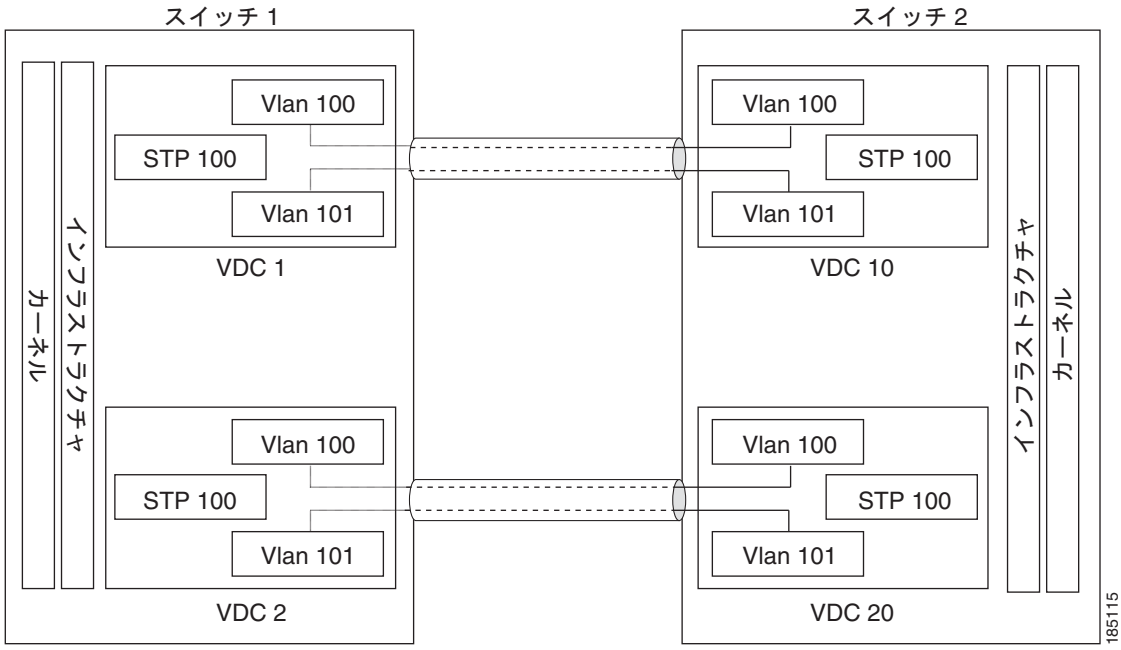
バーチャライゼーションとレイヤ 2 スイッチング

NX-OS ソフトウェアにより、単一スイッチング デバイス上で複数の Virtual Device Context（VDC）がサポートされるようになりました。各 VDC はスタンドアロン デバイスとして処理され、物理インターフェイスなどの特定のリソースがネットワーク管理ロールによって各 VDC に割り当てられます。各 VDC には管理者が割り当てられます。この管理者は、特定の VDC 内で、限定されたシステム情報を表示できます。障害もまた、特定の VDC 内で分離されます。

この VDC コンセプトは、すべてのレイヤ 2 スイッチング機能を含む、Cisco NX-OS 上のすべての機能に適用されます。

各 VDC では、すべてのプロセスが個別に実行されます（図 1-1 を参照）。同じプロセス ID 番号を、別の VDC で再使用できます。たとえば、図 1-1 に示すように、個別の各 VDC で VLAN 100 の ID を再使用できます。

図 1-1　VDC でのレイヤ 2 サービスの使用



各 VDC は、レイヤ 2 サービスを使用できるスタンドアロン デバイスとして動作します。VDC により、複数の論理機能で物理デバイスを共有できます。完全に分離された レイヤ 2 リソースをプロビジョニングして、個々の VDC に割り当てることができます。

複数の VDC を設定すると、各 VDC が物理デバイス リソースのグループになります。各 VDC に、リソースおよびユーザ ロールを割り当てます。VDC を使用すると、システムのリソースを著しく拡張して柔軟に使用できるだけでなく、障害分離も容易になります。

VDC では、プロセスおよび管理環境を分離することにより、論理デバイス間に障害および管理上の境界を確実に定義できます。各 VDC を、独自の設定、リソース、ユーザ、および管理インターフェイスを備えた個別のデバイスとして捉えることができます。

VDC ごとに異なる管理者レベルまたはロールで、各 VDC にアクセスして管理できます。特定のユーザ ロールの範囲外であるコマンドは、そのユーザに対して非表示になるか、コマンドを入力するとエラーが返されます。この機能により、物理デバイス全体にアクセスできるユーザ数を制限し、トラフィック中断の原因となる設定ミスを軽減できます。

（注） VDC およびリソース割り当ての詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide*』を参照してください。

（注） 再起動性およびシームレスな移行については、『*Cisco NX-OS High Availability and Redundancy Guide*』を参照してください。

関連資料

レイヤ 2 スイッチング機能に関連するマニュアルは、次のとおりです。

- 『*Cisco NX-OS Layer 2 Switching Command Reference*』
- 『*Cisco DCNM Layer 2 Switching Configuration Guide*』
- 『*Cisco NX-OS Interfaces Configuration Guide*』
- 『*Cisco NX-OS Security Configuration Guide*』
- 『*Cisco NX-OS Virtual Device Context Configuration Guide*』
- 『*Cisco NX-OS Licensing Guide*』
- 『*Cisco NX-OS High Availability and Redundancy Guide*』
- 『*Cisco NX-OS System Management Configuration Guide*』

CHAPTER 2

レイヤ 2 スイッチングの設定

この章では、NX-OS デバイス上のレイヤ 2 スイッチングについて説明します。

この章の内容は、次のとおりです。

- レイヤ 2 スイッチングの概要（p.2-2）
- レイヤ 2 スイッチングのライセンス要件（p.2-4）
- MAC アドレス設定の前提条件（p.2-4）
- 注意事項および制限（p.2-4）
- レイヤ 2 スイッチングの設定（p.2-5）
- レイヤ 2 スイッチング設定の確認（p.2-8）
- レイヤ 2 スイッチングの設定例（p.2-8）
- デフォルト設定（p.2-9）
- 追加情報（p.2-9）

レイヤ 2 スイッチングの概要

（注）　インターフェイスの作成に関する情報は、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

レイヤ 2 スイッチング ポートは、アクセス ポートまたはトランク ポートとして設定できます。トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張することができます。レイヤ 2 スイッチング ポートはすべて、MAC（メディア アクセス制御）アドレス テーブルを維持します。

（注）　ハイ アベイラビリティ機能の詳細については、『*Cisco NX-OS High Availability and Redundancy Configuration Guide* 』を参照してください。

ここでは、次の内容について説明します。

- レイヤ 2 スイッチング（p.2-2）
- バーチャライゼーションのサポート（p.2-3）

レイヤ 2 スイッチング

ここでは、レイヤ 2 イーサネット スイッチングに関する次の内容について説明します。

- レイヤ 2 イーサネット スイッチングの概要（p.2-2）
- セグメント間のフレーム スイッチング（p.2-3）
- アドレス テーブルの構築およびアドレス テーブルの変更（p.2-3）

レイヤ 2 イーサネット スイッチングの概要

このデバイスは、レイヤ 2 イーサネット セグメント間の同時パラレル接続をサポートします。イーサネット セグメント間のスイッチド コネクションが維持されるのは、パケットの伝送時間の長さだけです。次のパケットには、別のセグメント間に新しい接続が確立されます。

また、このデバイスでは、各デバイス（サーバなど）を独自の 10、100、1000 Mbps、または 10 ギガビットのコリジョン ドメインに割り当てることによって、広帯域デバイスおよび多数のユーザによって発生する輻輳の問題を解決できます。各 LAN ポートが個別のイーサネット コリジョン ドメインに接続されるので、スイッチド環境のサーバは全帯域幅にアクセスできます。

コリジョンはイーサネット ネットワークに著しい輻輳をもたらす原因になるので、効果的なソリューションは全二重方式の通信です。一般的に、10/100 Mbps イーサネットは半二重モードで動作するので、各ステーションは送信または受信のどちらかしか実行できません。これらのインターフェイスを全二重モードに設定すると、2 つのステーション間で同時に送受信を実行できます。両方向で同時にパケットを転送すれば、有効なイーサネット帯域幅は 2 倍になります。1/10 ギガビット イーサネットは、全二重モードでのみ動作します。

セグメント間のフレーム スイッチング

デバイス上の各 LAN ポートは、単一のワークステーション、サーバ、またはワークステーションやサーバがネットワークへの接続時に経由する他のデバイスに接続できます。

信号の劣化を防ぐために、デバイスは各 LAN ポートを個々のセグメントとして処理します。異なる LAN ポートに接続しているステーションが相互に通信する必要がある場合、デバイスは、一方の LAN ポートから他方の LAN ポートにワイヤ速度でフレームを転送し、各セッションが全帯域幅を利用できるようにします。

LAN ポート間のフレーム スイッチングを効率的に行うために、デバイスはアドレス テーブルを維持します。デバイスは、フレームを受信すると、受信した LAN ポートに、送信側ネットワーク デバイスの MAC アドレスを関連付けます。

アドレス テーブルの構築およびアドレス テーブルの変更

デバイスは、受信したフレームの MAC 送信元アドレスを使用して、アドレス テーブルをダイナミックに構築します。デバイスは、アドレス テーブルに存在しない MAC 宛先アドレスのフレームを受信すると、そのフレームの受信ポートを除いて同じ VLAN 内のすべての LAN ポートに、そのフレームをフラッディングします。宛先ステーションから応答があると、デバイスは、関連する MAC 送信元アドレスとポート ID をアドレス テーブルに追加します。以降、デバイスは後続フレームをすべての LAN ポートにフラッディングせずに、1 つの LAN ポートに転送します。

スタティック MAC アドレスと呼ばれる、デバイス上の特定のインターフェイスだけをスタティックに示す MAC アドレスを設定できます。スタティック MAC アドレスは、インターフェイス上でダイナミックに学習された MAC アドレスをすべて書き換えます。ブロードキャストまたはマルチキャストのアドレスは、スタティック MAC アドレスとして設定できません。スタティック MAC エントリは、デバイスのリブート後も保持されます。

アドレス テーブルには、最大 128,000 のアドレス エントリを保管できます。デバイスは設定可能なエージング タイマーによって定義されるエージング メカニズムを使用するので、指定の秒数だけ非アクティブ状態が続いたアドレスは、アドレス テーブルから削除されます。

（注） MAC ポート セキュリティの詳細については、『*Cisco NX-OS Security Configuration Guide*』を参照してください。

バーチャライゼーションのサポート

ソフトウェアは Virtual Device Context（VDC）をサポートしているので、VDC にローカルな MAC アドレスを設定して、運用できます。

（注） VDC およびリソース割り当ての詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide*』を参照してください。

レイヤ 2 スイッチングのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
NX-OS	レイヤ 2 スイッチングのライセンスは不要です。ライセンス パッケージに含まれていない機能は Cisco NX-OS システム イメージにバンドルされ、追加料金なしで提供されます。NX-OS ライセンス機構の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

ただし、VDC を使用するには、Advanced Services ライセンスが必要です。

MAC アドレス設定の前提条件

MAC アドレス設定時の前提条件は、次のとおりです。

- デバイスにログオンしている必要があります。
- 必要に応じて、Advanced Services ライセンスをインストールし、特定の VDC を開始します。

注意事項および制限

MAC アドレスの設定時は、次の注意事項および制限に従ってください。

- MAC アドレス テーブルに保管できるエントリ数は、最大 128,000 です。
- デバイス上に最大 14 の異なるエージング タイムを設定できます。

レイヤ 2 スイッチングの設定

ここでは、次の内容について説明します。

- スタティック MAC アドレスの設定（p.2-5）
- MAC テーブルのエージング タイムの設定（p.2-6）
- MAC テーブルからのダイナミック アドレスのクリア（p.2-7）

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

スタティック MAC アドレスの設定

スタティック MAC アドレスと呼ばれる、デバイス上の特定のインターフェイスだけをスタティックに示す MAC アドレスを設定できます。スタティック MAC アドレスは、インターフェイス上でダイナミックに学習された MAC アドレスをすべて書き換えます。ブロードキャストまたはマルチキャストのアドレスは、スタティック MAC アドレスとして設定できません。

始める前に

スタティック MAC アドレスを設定する前に、適正な VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **mac address-table static** *mac-address* **vlan** *vlan-id* {[**drop** | **interface** {*type slot/port* | | **port-channel** *number*]}
3. **exit**
4. **show mac address-table static**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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 static** *mac-address* **vlan** *vlan-id* {[**drop** | **interface** {*type slot/port*} | **port-channel** *number*]} **例：** `switch(config)# mac-address static 12ab.47dd.ff89 vlan 3 interface ethernet 2/1`	レイヤ 2 MAC アドレス テーブルに追加するスタティック MAC アドレスを指定します。

	コマンド	目的

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show mac address-table static** **例：** `switch# show mac address-table static`	（オプション）スタティック MAC アドレスを表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、レイヤ 2 MAC アドレス テーブルにスタティック エントリを入力する例を示します。

```
switch# config t
switch(config)# mac-address static 12ab.47dd.ff89 vlan 3 interface ethernet 2/1
switch(config)#
```

MAC テーブルのエージング タイムの設定

MAC アドレス エントリ（パケットの送信元 MAC アドレスおよびパケットを学習したポート）を、レイヤ 2 情報を含む MAC テーブルに保管しておく時間を設定できます。

（注） インターフェイス コンフィギュレーション モードまたは VLAN コンフィギュレーション モードで MAC エージング タイムを設定することもできます。

始める前に

MAC テーブルのエージング タイムを設定する前に、適正な VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **mac address-table aging-time** *seconds* [**vlan** *vlan_id*]
3. **exit**
4. **show mac address-table aging-time**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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 aging-time** *seconds* [**vlan** *vlan_id*] **例：** `switch(config)# mac address-table aging-time 600`	エントリが期限切れになり、レイヤ 2 MAC アドレス テーブルから廃棄される前にエージング タイムを指定します。指定できる範囲は 120 ～ 918000 秒です。デフォルトは 1800 秒です。値に 0 を入力すると、MAC エージングはディセーブルになります。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show mac address-table aging-time** **例：** `switch# show mac address-table aging-time`	（オプション）MAC アドレスのエージング タイム設定を表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、レイヤ 2 MAC アドレス テーブルのエントリのエージング タイムを 600 秒（10 分）に設定する例を示します。

```
switch# config t
switch(config)# mac address-table aging-time 600
switch(config)#
```

MAC テーブルからのダイナミック アドレスのクリア

MAC アドレス テーブルにある、すべてのダイナミック レイヤ 2 エントリをクリアできます。

始める前に

ダイナミック MAC テーブルをクリアする前に、適正な VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **clear mac address-table dynamic** {**address** *mac_addr*} {**interface** [**ethernet** *slot/port* | **loopback** *number* | **port-channel** *number*} {**vlan** *vlan_id*}
2. **show mac address-table**

手順の詳細

	コマンド	目的

ステップ 1	**clear mac address-table dynamic** {**address** *mac_addr*} {**interface** [**ethernet** *slot/port* | **loopback** *number* | **port-channel** *number*} {**vlan** *vlan_id*}
	
	例 1：
	`switch# clear mac address-table dynamic`
	
	例 2：
	`switch# clear mac address-table dynamic vlan 5`
		レイヤ 2 の MAC アドレス テーブルから、ダイナミック アドレス エントリをクリアします。
		
		例 1 では、MAC アドレス テーブルからすべてのダイナミック エントリがクリアされます。
		
		例 2 では、MAC アドレス テーブルから、VLAN 5 で学習されたダイナミック MAC アドレスだけがクリアされます。

ステップ 2	**show mac address-table** **例：** `switch# show mac address-table`	（オプション）MAC アドレス テーブルを表示します。

次に、レイヤ 2 MAC アドレス テーブルからダイナミック エントリをクリアする例を示します。

```
switch# clear mac address-table dynamic
switch#
```

レイヤ 2 スイッチング設定の確認

レイヤ 2 スイッチングの設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show mac address-table	MAC アドレス テーブルの情報を表示します。
show mac address-table aging-time	MAC アドレス テーブルに設定されているエージング タイムの情報を表示します。
show mac address-table static	MAC アドレス テーブルのスタティック エントリの情報を表示します。
show interface [<*interface*>**] mac-address**	インターフェイスの MAC アドレスとバーンドイン MAC アドレスを表示します。

これらのコマンドの詳細については、『*Cisco NX-OS Layer 2 Switching Command Reference*』を参照してください。

レイヤ 2 スイッチングの設定例

次に、スタティック MAC アドレスを追加して、MAC アドレスのデフォルトのグローバル エージング タイムを変更する例を示します。

```
switch# configure terminal
switch(config)# mac address-table static 0000.0000.1234 vlan 10 interface ethernet
2/15
switch(config)# mac address-table aging-time 120
```

デフォルト設定

表 2-1 に、レイヤ 2 スイッチングのパラメータのデフォルト設定を示します。

表 2-1　レイヤ 2 スイッチング パラメータのデフォルト値

パラメータ	デフォルト
エージング タイム	1800 秒

追加情報

レイヤ 2 スイッチングの実装に関する追加情報は、次のセクションを参照してください。

- 関連資料（p.2-9）
- 標準規格（p.2-9）

関連資料

関連トピック	マニュアル名
ポート セキュリティ、スタティック MAC アドレス	『*Cisco NX-OS Security Configuration Guide*』
インターフェイス	『*Cisco NX-OS Interfaces Configuration Guide*』
コマンド リファレンス	『*Cisco NX-OS Layer 2 Switching Command Reference*』
ハイ アベイラビリティ	『*Cisco NX-OS High Availability and Redundancy Guide*』
VDC	『*Cisco NX-OS Virtual Device Context Configuration Guide*』
システム管理	『*Cisco NX-OS System Management Configuration Guide*』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco NX-OS Release Notes*』 Release 4.0

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

CHAPTER 3

VLAN の設定

この章では、NX-OS デバイス上での VLAN（仮想 LAN）の設定方法について説明します。

この章の内容は、次のとおりです。

- VLAN について（p.3-2）
- VLAN のライセンス要件（p.3-7）
- VLAN 設定の前提条件（p.3-7）
- 注意事項および制約事項（p.3-7）
- VLAN の設定（p.3-8）
- VLAN 設定の確認（p.3-12）
- 統計情報の表示とクリア（p.3-13）
- VLAN の設定例（p.3-13）
- デフォルト設定（p.3-13）
- 追加情報（p.3-14）

(注) プライベート VLAN の情報については、第 4 章「プライベート VLAN の設定」を参照してください。

VLAN について

VLAN を使用すると、ネットワークを、レイヤ 2 レベルの個別の論理領域として分割できます。また、VLAN をブロードキャスト ドメインとして扱うこともできます。

VLAN には、任意のスイッチ ポートを加入させることができ、ユニキャスト、ブロードキャスト、およびマルチキャストのパケットは、その VLAN 内の端末だけに転送され、フラッディングされます。各 VLAN は 1 つの論理ネットワークであるとみなされます。VLAN に属していないステーション宛てのパケットは、ブリッジまたはルータを経由して転送する必要があります。

ここでは、次の内容について説明します。

- VLAN の概要（p.3-2）
- VLAN の範囲（p.3-4）
- VLAN の作成、削除、および変更（p.3-5）
- ハイ アベイラビリティ（p.3-6）
- バーチャライゼーションのサポート（p.3-6）

VLAN の概要

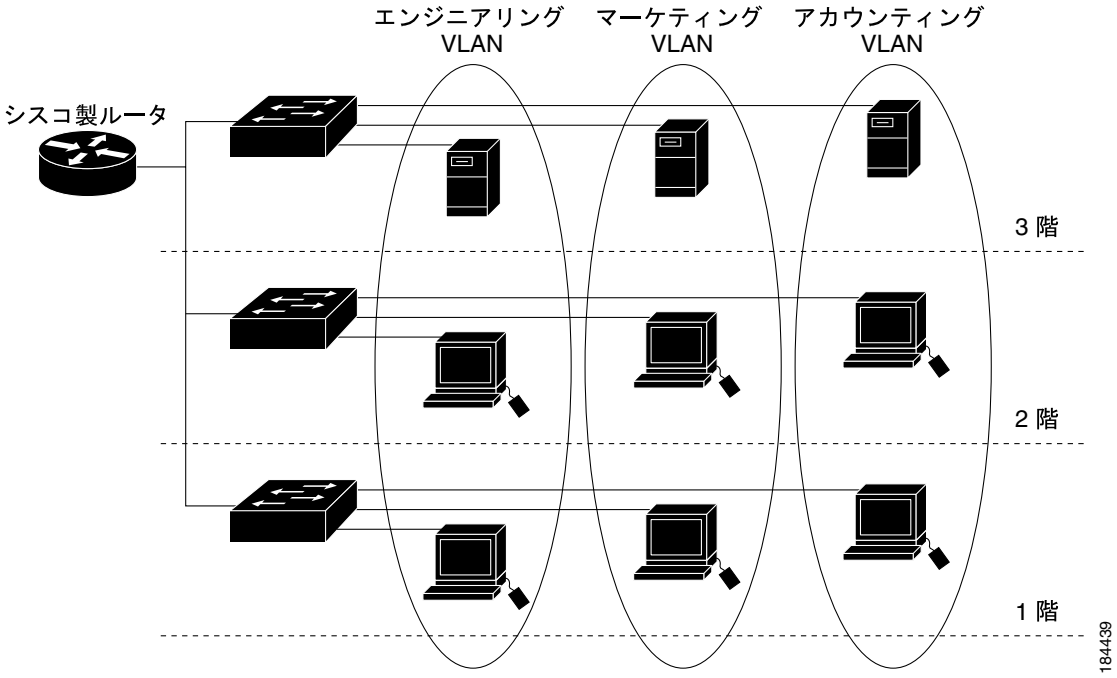
（注） VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）モードは、オフです。他のデバイス上で VTP がオンの場合に VTP ドメインを分割する VTP Protocol Data Unit（PDU; プロトコル データ ユニット）は、すべてのデバイスのインターフェイスで廃棄されます。

VLAN は、ユーザの物理的な場所に関係なく、機能またはアプリケーションによって論理的にセグメント化されるスイッチド ネットワーク内の端末のグループです。VLAN には、物理 LAN と同じアトリビュートが設定されますが、物理的に同じ LAN セグメント上に存在しない端末でもグループ化できます。

VLAN には、任意のスイッチ ポートを加入させることができ、ユニキャスト、ブロードキャスト、およびマルチキャストのパケットは、その VLAN 内の端末だけに転送され、フラッディングされます。各 VLAN は 1 つの論理ネットワークであるとみなされ、VLAN に属していないステーション宛てのパケットは、ルータ経由で転送する必要があります。

図 3-1 に、論理ネットワークとしての VLAN を示します。この図では、エンジニアリング部門の端末が 1 つの VLAN に割り当てられ、マーケティング部門の端末およびアカウンティング部門の端末も、それぞれ別の VLAN に割り当てられています。

図 3-1　論理的に定義されたネットワークとしての VLAN



VLAN は通常、IP サブネットワークと関連付けられます。たとえば、特定の IP サブネットに含まれるすべての端末を同じ VLAN に割り当てます。別の VLAN と通信するには、トラフィックをルーティングする必要があります。

デフォルトでは、新規に作成された VLAN は動作可能です。つまり、新規に作成された VLAN は、非シャットダウンの状態になります。また、VLAN は、トラフィックを転送するアクティブ ステート、またはパケットを転送しない一時停止（suspended）ステートとして設定できます。デフォルトでは、VLAN はアクティブ ステートで、トラフィックを転送します。

Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）は、VLAN 間の通信用として作成されるレイヤ 3 インターフェイスです。SVI は、VLAN インターフェイスとも呼ばれます。VLAN 間でトラフィックをルーティングするには、各 VLAN に VLAN インターフェイスを作成して、設定する必要があります。各 VLAN に必要な VLAN インターフェイスは、1 つだけです。

（注） SVI、レイヤ 3 VLAN インターフェイス、サブインターフェイスの設定、および IP アドレスの割り当ての詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。この機能は、VLAN インターフェイスを設定する前にイネーブルにする必要があります。

VLAN の範囲

（注）　NX-OS デバイスでは、拡張システム ID が常に自動的にイネーブルになります。

このデバイスは、IEEE 802.1Q 規格に従って、各 Virtual Device Context（VDC）で 4094 の VLAN をサポートします。これらの VLAN は、ソフトウェアによっていくつかの範囲に分割され、範囲によって用途が少しずつ異なります。

表 3-1 に VLAN の範囲を示します。

表 3-1　VLAN の範囲

VLAN 番号	範囲	用途
1	標準	シスコ システムズのデフォルトです。この VLAN は使用できますが、変更または削除することはできません。
2 ～ 1005	標準	これらの VLAN は、作成、使用、変更、および削除ができます。
1006 ～ 4094	拡張	これらの VLAN は、作成、名前指定、および使用ができます。次のパラメータは変更できません。 • ステートは必ず、アクティブです。 • VLAN は常にイネーブルです。これらの VLAN はシャットダウンできません。
3068 ～ 4047 および 4094	内部割り当て済み	これらの 80 の VLAN と VLAN 4094 は、内部デバイス用に割り当てられています。内部用に予約されている範囲内の VLAN の作成、削除、または変更はできません。

（注）　VLAN 3968 ～ 4047 および 4094 は、各 VDC の内部使用のために予約されています。これらの VLAN を使用または変更することはできません。

ソフトウェアは、内部 VLAN の使用を必要とするマルチキャストや診断などの機能のために、80 の VLAN 番号のグループを割り当てます。デフォルトでは、VLAN 3968 ～ 4047 が内部用として割り当てられます。また、VLAN 4094 もデバイスによる内部使用のために予約されます。

（注）　マルチキャストの情報については『*Cisco NX-OS Multicast Routing Configuration Guide*』を、診断の情報については『*Cisco NX-OS System Management Configuration Guide*』を参照してください。

予約されたグループ内の VLAN を使用、変更、または削除することはできません。内部的に割り当てられた VLAN および関連用途を表示することはできます。

VLAN の作成、削除、および変更

（注） デフォルトでは、すべての NX-OS ポートがレイヤ 3 ポートです。

VLAN は、各 VDC で 1 ～ 4094 の番号が割り当てられます。スイッチ ポートとして設定したポートはすべて、レイヤ 2 デバイスとしてのスイッチの初回起動時に、デフォルト VLAN に割り当てられます。デフォルト VLAN（VLAN 1）はデフォルト値のみを使用します。デフォルト VLAN のアクティビティを作成、削除、または一時停止することはできません。

VLAN は、番号を割り当てることによって作成します。作成した VLAN は削除したり、アクティブ ステートから一時停止ステートに移行したりできます。既存の VLAN ID を使用して VLAN を作成しようとすると、デバイスで VLAN サブモードが開始されますが、同じ VLAN は再作成されません。

新規に作成した VLAN は、その VLAN にレイヤ 2 ポートが割り当てられるまでは未使用の状態になります。デフォルトでは、すべてのポートが VLAN1 に割り当てられます。

VLAN の範囲に応じて、VLAN（デフォルト VLAN を除く）に次のパラメータを設定できます。

- VLAN 名
- VLAN ステート
- シャットダウンまたは非シャットダウン

（注） VLAN アクセス ポートまたはトランク ポートとしてのポート設定および VLAN へのポート割り当ての詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

特定の VLAN を削除すると、その VLAN に関連付けられていたポートがシャットダウンし、トラフィックの転送が停止します。トランク ポートから特定の VLAN を削除すると、その VLAN だけがシャットダウンし、トラフィックは引き続き、トランク ポート経由で他のすべての VLAN 上で転送されます。

ただし、削除した VLAN の VLAN とポートのマッピングはシステム上にすべて存続しているので、その VLAN を再イネーブル化または再作成すると、*元の*ポート設定が自動的にその VLAN に戻されます。VLAN のスタティック MAC アドレスとエージング タイムは、VLAN を再イネーブル化しても復元されません。

（注） VLAN コンフィギュレーション サブモードで入力したコマンドは、すぐに実行されます。

（注） VLAN 3968 ～ 4047 および 4094 は、各 VDC の内部使用のために予約されています。これらの VLAN を使用または変更することはできません。

ハイ アベイラビリティ

このソフトウェアでは、コールド リブート時に、VLAN のステートフルおよびステートレスの両方の再起動で、ハイ アベイラビリティがサポートされます。ステートフルな再起動では、最大 3 回の再試行がサポートされます。再起動から 10 秒以内に 4 回以上の再試行を行うと、スーパーバイザ モジュールがリロードされます。

ソフトウェアのアップグレードまたはダウングレードは、VLAN に関してはシームレスに実行できます。

（注） ハイ アベイラビリティ機能の詳細については、『*Cisco NX-OS High Availability and Redundancy Configuration Guide*』を参照してください。

バーチャライゼーションのサポート

このソフトウェアは、VDC をサポートしているので、VLAN の設定および運用は各 VDC にローカルになります。

（注） VDC およびリソース割り当ての詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide*』を参照してください。

各 VLAN では、すべてのポートが同じ VDC に存在している必要があります。VDC に十分なリソースが割り当てられていない場合、ソフトウェアによりエラー メッセージが戻されます。

新規の VDC を作成すると、新しいデフォルト VLAN として VLAN1 が自動的に作成され、VLAN 3968 ～ 4047 および 4094 がデバイス用として内部予約されます。

別の VDC で使用している VLAN と同じ番号の VLAN を再使用できます。

1 つ以上の VLAN を、ユーザによる設定を許可または拒否するロールに関連付けることができます。VLAN をロールに関連付けると、対応するインターフェイスも同じチェックの対象になります。たとえば、ロールに VLAN1 へのアクセスが許可されている場合、VLAN1 を使用するインターフェイスへのアクセスも許可されます。インターフェイスに、ロールに関連付けられた VLAN が設定されていない場合、そのインターフェイスはそのロールにアクセスできません。

VLAN のライセンス要件

次の表に、この機能に関するライセンス要件を示します。

製品	ライセンス要件
NX-OS	VLAN のライセンスは不要です。ライセンス パッケージに含まれていない機能は Cisco NX-OS システム イメージにバンドルされ、無料で提供されます。NX-OS ライセンス機構の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

ただし、VDC を使用するには、Advanced Services ライセンスが必要です。

VLAN 設定の前提条件

VLAN 設定時の前提条件は、次のとおりです。

- デバイスにログオンしている必要があります。
- 必要に応じて、Advanced Services ライセンスをインストールし、特定の VDC を開始します。その VDC に十分なリソースが割り当てられていることを確認してください。VDC の作成およびリソース割り当ての詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide*』を参照してください。
- VLAN を変更するには、その VLAN が作成されている必要があります。

注意事項および制約事項

VLAN の作成時は、次の注意事項および制約事項に従ってください。

- 各 VDC の VLAN の最大数は、4094 です。
- 同じ VLAN ID 番号を、別の VDC で再使用できます。たとえば、デフォルト VDC に VLAN10 を作成した場合、新しく作成した VDC（VDC2 など）にまったく別の VLAN10 を作成できます。
- 1 つの VLAN または VLAN 範囲を設定できます。
- 内部使用のために予約された VLAN グループ内の VLAN は、作成、変更、または削除することはできません。
- VLAN1 は、デフォルトの VLAN です。この VLAN を作成、変更、または削除することはできません。
- VLAN 1006 ～ 4094 は常にアクティブ ステートなので、常にイネーブルです。これらの VLAN のステートを一時停止またはシャットダウンすることはできません。

VLAN の設定

ここでは、次の内容について説明します。

- VLAN の作成および削除（p.3-8）
- VLAN コンフィギュレーション サブモードの開始（p.3-9）
- VLAN の設定（p.3-11）

（注） VLAN（アクセス ポートまたはトランク ポート）へのレイヤ 2 インターフェイスの割り当ての詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。デフォルトでは、すべてのインターフェイスが VLAN1 に割り当てられます。

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なることがあるので注意が必要です。

VLAN の作成および削除

デフォルトの VLAN およびデバイス用に内部的に割り当てられた VLAN 以外は、すべての VLAN を作成または削除できます。

作成した VLAN は、自動的にアクティブ ステートになります。

（注） VLAN を削除すると、その VLAN に関連付けられているポートがシャットダウンします。したがって、廃棄されるトラフィック フローやパケットはありません。トランク ポートの場合、ポートはオープンしたままで、削除した VLAN を除く他のすべての VLAN からのトラフィックが引き続き転送されます。

作成する VLAN の範囲内に作成できない VLAN が含まれていると、作成できない VLAN がリストされたメッセージが戻されますが、指定範囲内の他の VLAN はすべて作成されます。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。VDC が異なっていても同じ VLAN 名と ID を使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の要約

1. **config t**
2. **vlan** {*vlan-id* | *vlan-range*}
3. **exit**
4. **show vlan**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t switch(config)#	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	**vlan** {*vlan-id* | *vlan-range*} **例：** switch(config)# vlan 5 switch(config-vlan)#	VLAN または VLAN 範囲を作成します。割り当て済みの VLAN 番号を入力すると、その VLAN の VLAN コンフィギュレーション サブモードが開始されます。内部的に割り当てられている VLAN の番号を入力すると、エラー メッセージが表示されます。ただし、指定した VLAN 範囲に、内部割り当て VLAN 以外の VLAN が含まれている場合は、コマンドは、内部割り当て以外の VLAN に対して*のみ*有効になります。指定できる範囲は、2 ～ 4094 です。VLAN1 はデフォルト VLAN なので、作成または削除はできません。内部使用のために予約されている VLAN を作成または削除することはできません。
ステップ 3	**exit** **例：** switch(config-vlan)# exit switch(config)#	VLAN モードを終了します。
ステップ 4	**show vlan** **例：** switch# show vlan	（任意）VLAN の情報およびステータスを表示します。
ステップ 5	**copy running-config startup-config** **例：** switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、15 ～ 20 の VLAN 範囲を作成する例を示します。

```
switch# config t
switch(config)# vlan 15-20
switch(config-vlan)#
```

（注） VLAN コンフィギュレーション サブモードで、VLAN を作成および削除することもできます。

VLAN コンフィギュレーション サブモードの開始

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

- 名前
- ステート
- シャットダウン

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。VDC が異なっていても同じ VLAN 名と ID を使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の要約

1. **config t**
2. **vlan** {*vlan-id* | *vlan-range*}
3. **exit**
4. **show vlan**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**vlan** {*vlan-id* | *vlan-range*}
	
	例：
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		VLAN コンフィギュレーション サブモードを開始します。このサブモードでは、VLAN または VLAN 範囲に対して、名前の指定、ステートの設定、ディセーブル化、またはシャットダウンを実行できます。
		
		VLAN1 または内部的に割り当てられた VLAN に対しては、これらの値を変更できません。VLAN 1006 ～ 4094 に対して実行できるのは、名前の変更だけです。

ステップ 3	**exit**
	
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		VLAN コンフィギュレーション モードを終了します。

ステップ 4	**show vlan** **例：** `switch# show vlan`	（任意）VLAN の情報およびステータスを表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、VLAN コンフィギュレーション サブモードを開始して、終了する例を示します。

```
switch# config t
switch(config)# vlan 15
switch(config-vlan)# exitswitch(config)#
```

VLAN の設定

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

- 名前
- ステート
- シャットダウン

（注） デフォルト VLAN または内部的に割り当てられた VLAN の作成、削除、または変更はできません。また、特定の VLAN については、これらのパラメータの一部を変更できません。詳細は、「VLAN の範囲」（p.3-4）を参照してください。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。VDC が異なっていても同じ VLAN 名と ID を使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の要約

1. **config t**
2. **vlan** {*vlan-id* | *vlan-range*}
3. **name** *vlan-name*
4. **state** {**active** | **suspend**}
5. **no shutdown**
6. **exit**
7. **show vlan**
8. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**vlan** {*vlan-id* | *vlan-range*}
	
	例：
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		VLAN コンフィギュレーション サブモードを開始します。既存の VLAN ではない場合、指定した VLAN が作成され、VLAN コンフィギュレーション サブモードが開始されます。

ステップ 3	**name** *vlan-name* **例：** `switch(config-vlan)# name accounting`	VLAN 名を指定します。VLAN 名として、32 文字までの英数字を入力できます。VLAN1 または内部的に割り当てられた VLAN の名前は変更できません。デフォルト値は VLANxxxx で、xxxx は VLAN ID 番号と同じ 4 桁の数値（先行ゼロを含む）です。

	コマンド	目的
ステップ 4	**state** {**active** | **suspend**} **例：** switch(config-vlan)# state active	VLAN のステート（アクティブまたは一時停止）を設定します。VLAN ステートを一時停止（suspended）にすると、その VLAN に関連付けられたポートがシャットダウンし、VLAN のトラフィック転送が停止します。デフォルトのステートは、アクティブです。デフォルト VLAN および VLAN 1006 ～ 4094 のステートを一時停止にすることはできません。
ステップ 5	**no shutdown** **例：** switch(config-vlan)# no shutdown	VLAN をイネーブルにします。デフォルト値は、非シャットダウン（イネーブル）です。デフォルト VLAN、VLAN1、VLAN 1006 ～ 4094 はシャットダウンできません。
ステップ 6	**exit** **例：** switch(config-vlan)# exit switch(config)#	VLAN コンフィギュレーション サブモードを終了します。
ステップ 7	**show vlan** **例：** switch# show vlan	（任意）VLAN の情報およびステータスを表示します。
ステップ 8	**copy running-config startup-config** **例：** switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、VLAN 5 に任意のパラメータを設定する例を示します。

```
switch# config t
switch(config)# vlan 5
switch(config-vlan)# name accounting
switch(config-vlan)# state active
switch(config-vlan)# no shutdown
switch(config-vlan)# exit
switch(config)#
```

VLAN 設定の確認

VLAN の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config vlan *vlan-id*	VLAN 情報を表示します。
show vlan [**all-ports** | **brief** | **id** *vlan-id* | **name** *name* | **dot1q tag native**]	VLAN 情報を表示します。
show vlan summary	VLAN 情報の要約を表示します。

これらのコマンドの出力フィールドの詳細については、『*Cisco NX-OS Command Reference*』を参照してください。

統計情報の表示とクリア

VLAN の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
clear vlan [**id** *vlan-id*] **counters**	すべての VLAN または指定した VLAN のカウンタをクリアします。
show vlan counters	各 VLAN のレイヤ 2 パケット情報を表示します。

VLAN の設定例

次に、VLAN を作成して名前を指定し、ステートをアクティブにして、管理上のアップに設定する例を示します。

```
switch# configure terminal
switch(config)# vlan 10
switch(config-vlan)# name test
switch(config-vlan)# state active
switch(config-vlan)# no shutdown
switch(config-vlan)# exit
switch(config)#
```

VLAN のデフォルト設定については、「デフォルト設定」（p.3-13）を参照してください。

デフォルト設定

表 3-2 に、VLAN パラメータのデフォルト設定を示します。

表 3-2　VLAN パラメータのデフォルト値

パラメータ	デフォルト
すべての VLAN	イネーブル
VLAN	VLAN1 スイッチ ポートとして設定したポートは、VLAN1 に割り当てられます。
VLAN ID	1
VLAN 名	• デフォルト VLAN（VLAN1）— default • 他のすべての VLAN — VLAN *vlan-id*
VLAN ステート	アクティブ
STP	イネーブル：Rapid PVST+ がイネーブル

追加情報

VLAN の実装に関する追加情報は、次のセクションを参照してください。

- 関連資料（p.3-14）
- 標準規格（p.3-14）
- MIB（p.3-14）

関連資料

関連トピック	マニュアル名
プライベート VLAN	第 4 章「プライベート VLAN の設定」
Rapid PVST+	第 5 章「Rapid PVST+ の設定」
MST	第 6 章「MST の設定」
STP 拡張機能	第 7 章「STP 拡張機能の設定」
コマンド リファレンス	『*Cisco NX-OS Layer 2 Switching Command Reference*』
DCNM レイヤ 2 スイッチングの設定	『*Cisco DCNM Layer 2 Switching Configuration Guide*』
インターフェイス、VLAN インターフェイス（SVI）、IP アドレス指定、ポート チャネル	『*Cisco NX-OS Interfaces Configuration Guide*』
NX-OS の基本情報	『*Cisco NX-OS Fundamentals Configuration Guide*』
マルチキャスト ルーティング	『*Cisco NX-OS Multicast Routing Configuration Guide*』
ハイ アベイラビリティ	『*Cisco NX-OS High Availability and Redundancy Guide*』
システム管理	『*Cisco NX-OS System Management Configuration Guide*』
VDC	『*Cisco NX-OS Virtual Device Context Configuration Guide*』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco NX-OS Release Notes*』 Release 4.0

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

MIB

MIB	MIB リンク
• CISCO-VLAN-MEMBERSHIP-MIB： vmMembershipTable-MIB vmMembershipSummaryTable-MIB	次の URL から、MIB の検索およびダウンロードができます。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

CHAPTER 4

プライベート VLAN の設定

この章では、プライベート VLAN を設定する手順について説明します。プライベート VLAN は、レイヤ 2 レベルでさらなる保護機能を提供します。

この章の内容は、次のとおりです。

- プライベート VLAN について（p.4-2）
- プライベート VLAN のライセンス要件（p.4-8）
- プライベート VLAN の前提条件（p.4-8）
- 注意事項および制限（p.4-9）
- プライベート VLAN の設定（p.4-12）
- プライベート VLAN 設定の確認（p.4-22）
- プライベート VLAN の統計情報の表示とクリア（p.4-22）
- プライベート VLAN の設定例（p.4-23）
- デフォルト設定（p.4-23）
- 追加情報（p.4-24）

（注） レイヤ 3 VLAN インターフェイスまたは Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）の IP アドレス指定の詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

プライベート VLAN について

（注）　レイヤ 2 ポートは、トランク ポート、アクセス ポート、またはプライベート VLAN ポートとして機能します。

（注）　この機能を設定する前に、プライベート VLAN 機能をイネーブルにする必要があります。

同様のシステム間で直接通信する必要がない特定の状況では、プライベート VLAN により、レイヤ 2 レベルの保護を強化できます。プライベート VLAN は、プライマリ VLAN とセカンダリ VLAN のアソシエーションです。

プライマリ VLAN は、セカンダリ VLAN を関連付けるブロードキャスト ドメインを定義します。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のどちらかです（独立 VLAN およびコミュニティ VLAN の詳細は、「セカンダリ VLAN およびプライマリ VLAN の設定」[p.4-9] を参照してください）。独立 VLAN 上のホストは、プライマリ VLAN 内で関連付けられた混合ポートとだけ通信します。コミュニティ VLAN 上のホストは、同じコミュニティ VLAN 上のホスト間および関連付けられた無差別ポートとだけ通信し、独立ポートまたは他のコミュニティ VLAN 内のポートとは通信しません（プライベート VLAN のポート タイプの詳細は、「プライベート VLAN ポートの設定」[p.4-10] を参照してください）。

統合スイッチングおよびルーティング機能を使用するコンフィギュレーションでは、各プライベート VLAN に単一のレイヤ 3 VLAN インターフェイスまたは SVI を割り当てることにより、ルーティングを提供できます。SVI は、プライマリ VLAN 用に作成します。このようなコンフィギュレーションでは、セカンダリ VLAN はすべて、プライマリ VLAN 上の SVI とのマッピングにより、レイヤ 3 でのみ通信します。セカンダリ VLAN 上の既存の SVI は、すべてサービス停止状態になります。

ここでは、次の内容について説明します。

- プライベート VLAN の概要（p.4-2）
- ハイ アベイラビリティ（p.4-8）
- バーチャライゼーションのサポート（p.4-8）

プライベート VLAN の概要

デバイスでプライベート VLAN 機能を適用するには、プライベート VLAN をイネーブルにする必要があります。

プライベート VLAN モードで動作しているポートがデバイスに設定されている場合は、プライベート VLAN をディセーブルにすることはできません。

（注）　特定の VLAN をプライマリまたはセカンダリのどちらかのプライベート VLAN として設定するには、事前に VLAN が作成しておく必要があります（VLAN の作成については、第 3 章「VLAN の設定」を参照してください）。

ここでは、次の内容について説明します。

- プライベート VLAN のプライマリ VLAN とセカンダリ VLAN（p.4-3）
- プライベート VLAN ポート（p.4-3）
- プライマリ、独立、およびコミュニティ プライベート VLAN（p.4-4）
- プライマリ VLAN とセカンダリ VLAN の関連付け（p.4-6）
- プライベート VLAN 内のブロードキャスト トラフィック（p.4-6）
- プライベート VLAN ポートの分離（p.4-7）
- プライベート VLAN および VLAN インターフェイス（p.4-7）
- 複数のデバイスにまたがるプライベート VLAN（p.4-7）

プライベート VLAN のプライマリ VLAN とセカンダリ VLAN

プライベート VLAN 機能では、VLAN の使用時にユーザが直面する 2 つの問題に対処できます。

- 各 Virtual Device Context（VDC）は、最大 4096 の VLAN をサポートします。各カスタマーに 1 つの VLAN を割り当てると、サービス プロバイダーがサポートできるカスタマー数は制限されます。
- IP ルーティングをイネーブルにするには、各 VLAN にサブネット アドレス空間またはアドレス ブロックを割り当てます。これにより未使用の IP アドレスが無駄になり、IP アドレスの管理に問題が生じます。

プライベート VLAN を使用することにより、スケーラビリティの問題が解決され、IP アドレスの管理が容易になり、カスタマーにレイヤ 2 セキュリティが提供されます。

プライベート VLAN の機能は、VLAN のレイヤ 2 ブロードキャスト ドメインをサブドメインに分割できます。サブドメインは、1 つのプライベート VLAN ペアで、プライマリ VLAN とセカンダリ VLAN で構成されます。プライベート VLAN ドメインには、各サブドメインに 1 ペアずつ、複数のプライベート VLAN ペアを設定できます。プライベート VLAN ドメイン内のすべての VLAN ペアは、同じプライマリ VLAN を共有します。各サブドメインは、セカンダリ VLAN ID で識別します。

（注） プライベート VLAN ドメインに設定できるプライマリ VLAN は 1 つだけです。

セカンダリ VLAN は、同じ VLAN 内のポートをレイヤ 2 で分離します。プライマリ VLAN 内のセカンダリ VLAN には、次の 2 つのタイプがあります。

- 独立 VLAN — 独立 VLAN 内のポートは、レイヤ 2 レベルでは相互に通信できません。
- コミュニティ VLAN — コミュニティ VLAN 内のポートは相互に通信できますが、レイヤ 2 レベルの他のコミュニティ VLAN 内または独立 VLAN 内のポートとは通信できません。

プライベート VLAN ポート

（注） コミュニティ プライベート VLAN および独立プライベート VLAN のポートは、いずれも PVLAN ホスト ポートというラベルが付けられます。PVLAN ホスト ポートは、関連付けられているセカンダリ VLAN のタイプによって、コミュニティ PVLAN ポートまたは独立 PVLAN ポートのどちらかになります。

プライベート VLAN ポートには、次のタイプがあります。

- 無差別 — 無差別ポートは、プライマリ VLAN に属します。無差別ポートは、コミュニティ ホスト ポートおよび独立ホスト ポートを含め、セカンダリ VLAN に属していて、無差別ポートとプライマリ VLAN に*関連付けられている*すべてのインターフェイスと通信できます。プライマリ VLAN には、複数の無差別ポートを設定できます。各無差別ポートには、複数のセカンダリ VLAN を関連付けることができますが、セカンダリ VLAN を関連付けなくてもかまいません。無差別ポートとセカンダリ VLAN が同じプライマリ VLAN 内にあれば、1 つのセカンダリ VLAN を複数の無差別ポートに関連付けることができます。このアソシエーション（関連付け）は、ロード バランシングまたは冗長性のために使用することもできます。セカンダリ VLAN に無差別ポートを関連付けないこともできますが、その場合、セカンダリ VLAN はレイヤ 3 インターフェイスと通信できません。
- 独立 — 独立ポートは、独立セカンダリ VLAN に属すホスト ポートです。このポートは、同じプライベート VLAN ドメイン内の他のポートからレイヤ 2 で完全に分離されていますが、関連付けられた無差別ポートとは通信できます。プライベート VLAN は、無差別ポートからのトラフィックを除き、独立ポート宛のトラフィックをすべてブロックします。独立ポートから受信したトラフィックは、無差別ポートにのみ転送されます。特定の独立 VLAN に複数の独立ポートを設定し、その独立 VLAN 内で各ポートを他のすべてのポートから完全に分離できます。
- コミュニティ — コミュニティ ポートは、コミュニティ セカンダリ VLAN に属すホスト ポートです。コミュニティ ポートは、同じコミュニティ VLAN 内の他のポートおよび関連付けられた無差別ポートと通信します。これらのインターフェイスは、他のコミュニティにある他のすべてのインターフェイスおよびプライベート VLAN ドメイン内のすべての独立ポートから、レイヤ 2 で分離されています。

（注） トランクは、無差別、独立、およびコミュニティの各ポート間のトラフィックを伝送する VLAN をサポートできるので、独立ポートとコミュニティ ポートのトラフィックはトランク インターフェイスを経由してデバイスと送受信されることがあります。

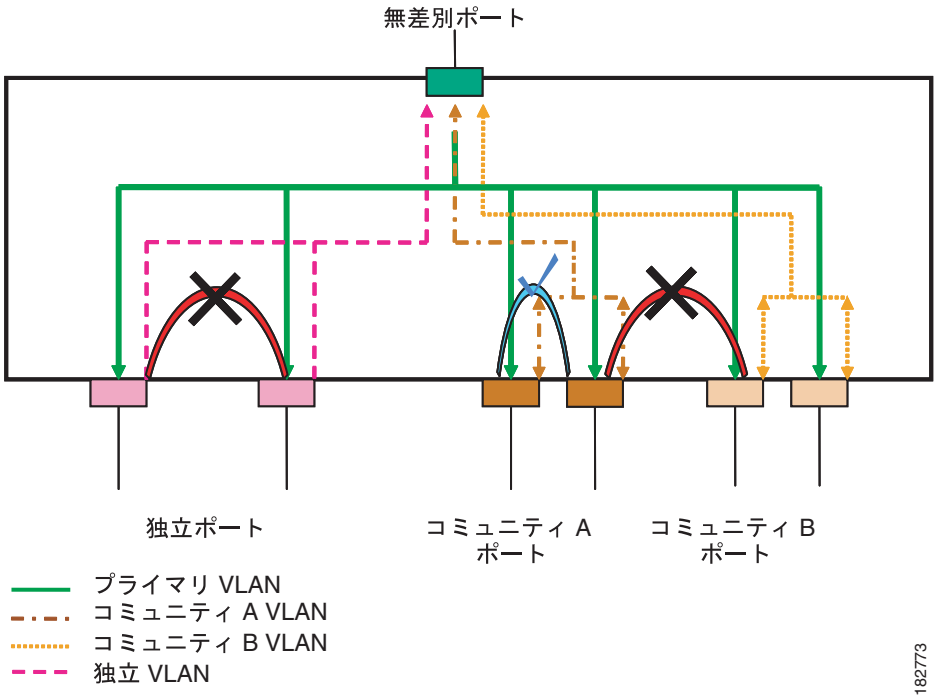
プライマリ、独立、およびコミュニティ プライベート VLAN

プライマリ VLAN にはレイヤ 3 ゲートウェイがあるので、プライベート VLAN の外部と通信するには、セカンダリ VLAN をプライマリ VLAN に関連付けます。プライマリ VLAN および 2 種類のセカンダリ VLAN（独立 VLAN およびコミュニティ VLAN）には、次の特性があります。

- プライマリ VLAN — プライマリ VLAN は、無差別ポートから（独立およびコミュニティ）ホスト ポートおよび他の無差別ポートへのトラフィックを伝送します。
- 独立 VLAN — 独立 VLAN は、ホストから無差別ポートおよびレイヤ 3 ゲートウェイへの単方向アップストリーム トラフィックを伝送するセカンダリ VLAN です。プライベート VLAN ドメインに複数の独立 VLAN を設定し、各 VLAN 内のトラフィックを分離できます。また、各独立 VLAN に複数の独立ポートを設定し、各独立ポートからのトラフィックを完全に分離することもできます。
- コミュニティ VLAN — コミュニティ VLAN は、アップストリーム トラフィックをコミュニティ ポートから無差別ポート ゲートウェイおよび同じコミュニティ内の他のホスト ポートに伝送するセカンダリ VLAN です。1 つのプライベート VLAN ドメイン内に複数のコミュニティ VLAN を設定できます。これらのポートは、同じコミュニティ内のポートとは相互に通信できますが、プライベート VLAN 内の他のコミュニティ VLAN 内または独立 VLAN 内のポートとは通信できません。

図 4-1 に、プライマリまたはプライベート VLAN 内のレイヤ 2 トラフィック フロー、および VLAN のタイプとポートのタイプを示します。

図 4-1　プライベート VLAN のレイヤ 2 トラフィック フロー



（注） プライベート VLAN のトラフィック フローは、ホスト ポートから無差別ポートへの単方向です。無差別ポートから*出力*されるトラフィックは、標準 VLAN 内のトラフィックと同様に処理され、関連付けられたセカンダリ VLAN でトラフィックが分離されることはありません。

無差別ポートは 1 つのプライマリ VLAN の専用ポートになりますが、複数の独立 VLAN および複数のコミュニティ VLAN で使用できます（レイヤ 3 ゲートウェイは通常、無差別ポート経由でデバイスに接続されます）。無差別ポートを使用すると、さまざまなデバイスをアクセス ポイントとしてプライベート VLAN に接続できます。たとえば、無差別ポートを使用して、管理ワークステーションからすべてのプライベート VLAN サーバをモニタ、またはバックアップできます。

プライマリ VLAN には複数の無差別ポートを設定できますが、各プライマリ VLAN に設定できるレイヤ 3 ゲートウェイは *1* つだけです。

スイッチング環境では、個々の端末または共通グループの端末に、個別のプライベート VLAN および関連する IP サブネットを割り当てることができます。端末は、プライベート VLAN の外側と通信する場合、デフォルト ゲートウェイのみと通信する必要があります。

（注） レイヤ 3 ゲートウェイまたは SVI を設定するには、VLAN インターフェイス機能をイネーブルにしておく必要があります。SVI および IP アドレス指定の詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

プライマリ VLAN とセカンダリ VLAN の関連付け

セカンダリ VLAN 内のホスト ポートでプライベート VLAN 外と通信するには、セカンダリ VLAN をプライマリ VLAN に関連付ける必要があります。アソシエーションが正常に動作していない場合、セカンダリ VLAN のホスト ポート（独立ポートおよびコミュニティ ポート）はダウン ステートになります。

（注） セカンダリ VLAN は、1 つのプライマリ VLAN にのみ関連付けることができます。

アソシエーションを正常に動作させるには、次の条件が満たされている必要があります。

- プライマリ VLAN が存在する。
- セカンダリ VLAN が存在する。
- プライマリ VLAN がプライマリ VLAN として設定されている。
- セカンダリ VLAN が、独立 VLAN またはコミュニティ VLAN として設定されている。

（注） アソシエーションが動作しているかどうかを確認するには、**show** コマンドの出力を調べます。アソシエーションが動作していなくても、エラー メッセージは発行されません（設定の確認については、「プライベート VLAN 設定の確認」[p.4-22] を参照してください）。

プライマリ VLAN またはセカンダリ VLAN のどちらかを削除すると、その VLAN に関連付けられているポートは非アクティブになります。**no private-vlan** コマンドを入力すると、VLAN は標準 VLAN モードに戻ります。その VLAN 上のアソシエーションはすべて一時停止されますが、インターフェイスはプライベート VLAN モードのままです。特定の VLAN をプライベート VLAN モードに再変換すると、元のアソシエーションが復元されます。

プライマリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN のすべてのプライベート VLAN アソシエーションが削除されます。ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力した場合には、その VLAN のプライベート VLAN アソシエーションは一時停止するだけです。VLAN を再作成して、元のセカンダリ VLAN として設定すると、アソシエーションが再開されます。

セカンダリ VLAN とプライマリ VLAN 間のアソシエーションを変更するには、最初に現在のアソシエーションを削除してから、新しいアソシエーションを追加します。

プライベート VLAN 内のブロードキャスト トラフィック

プライベート VLAN 内のポートからのブロードキャスト トラフィックは、次のように伝送されます。

- 無差別ポートからのブロードキャスト トラフィックは、プライマリ VLAN 内のすべてのポートに伝送されます。このブロードキャスト トラフィックは、プライベート VLAN パラメータが設定されていないポートも含め、プライマリ VLAN 内のすべてのポートに配信されます。
- 独立ポートからのブロードキャスト トラフィックは、その独立ポートが関連付けられているプライマリ VLAN 内の無差別ポートだけに配信されます。
- コミュニティ ポートからのブロードキャスト トラフィックは、そのポートのコミュニティ内のすべてのポート、およびそのコミュニティ ポートに関連付けられているすべての無差別ポートに配信されます。このブロードキャスト パケットは、プライマリ VLAN 内の他のコミュニティまたは独立ポートには配信されません。

プライベート VLAN ポートの分離

プライベート VLAN を使用して、端末へのアクセスを次のように制御できます。

- 端末に接続している特定のインターフェイスを独立ポートとして設定すると、レイヤ 2 での通信が阻止されます。たとえば、端末がサーバである場合、この設定により、サーバ間のレイヤ 2 通信が阻止されます。
- デフォルト ゲートウェイおよび特定の端末（バックアップ サーバなど）に接続しているインターフェイスを無差別ポートとして設定すると、すべての端末からデフォルト ゲートウェイへのアクセスが許可されます。

プライベート VLAN および VLAN インターフェイス

レイヤ 2 VLAN への VLAN インターフェイスは、Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）とも呼ばれます。レイヤ 3 デバイスは、セカンダリ VLAN ではなく、プライマリ VLAN を介してのみプライベート VLAN と通信します。

VLAN インターフェイスは、プライマリ VLAN に対してのみ設定します。セカンダリ VLAN には VLAN インターフェイスを設定しないでください。VLAN がセカンダリ VLAN として設定されている場合、セカンダリ VLAN の VLAN インターフェイスまたは SVI は非アクティブになります。VLAN インターフェイスの設定が正しくない場合、次のような状況になります。

- アクティブな VLAN インターフェイスまたは SVI が設定された VLAN をセカンダリ VLAN として設定しようとすると、VLAN インターフェイスをディセーブルにするまでは、設定が許可されません。
- セカンダリ VLAN として設定されている VLAN 上で VLAN インターフェイスまたは SVI を作成してイネーブルにしようとすると、その VLAN インターフェイスはディセーブルのままで、システムからエラーが返されます。

プライマリ VLAN がセカンダリ VLAN に関連付けられ、マッピングされている場合、プライマリ VLAN 上のすべての設定がセカンダリ VLAN に伝播されます。たとえば、プライマリ VLAN 上のレイヤ 3 VLAN インターフェイスまたは SVI に IP サブネットを割り当てると、このサブネットはプライベート VLAN 全体の IP サブネット アドレスになります。

（注） VLAN インターフェイスを設定するには、VLAN インターフェイス機能をイネーブルにしておく必要があります。VLAN インターフェイスおよび IP アドレス指定の詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

複数のデバイスにまたがるプライベート VLAN

プライベート VLAN を複数の装置にわたるように拡張するには、プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN を、プライベート VLAN をサポートする他の装置にトランキングします。プライベート VLAN 設定のセキュリティを保持して、プライベート VLAN として設定された VLAN が他の目的に使用されないようにするには、プライベート VLAN ポートが設定されていないデバイスを含め、すべての中間デバイスにプライベート VLAN を設定します。

ハイ アベイラビリティ

このソフトウェアは、コールド リブート時に、プライベート VLAN のステートフルおよびステートレスの両方の再起動において、ハイ アベイラビリティをサポートしています。ステートフルな再起動では、再試行は最大 3 回までサポートされます。再起動から 10 秒以内に 4 回以上の再試行を行うと、スーパーバイザ モジュールがリロードされます。

プライベート VLAN ごとに、ソフトウェアのアップグレードまたはダウングレードをシームレスに実行できます。

（注） ハイ アベイラビリティ機能の詳細については、『*Cisco NX-OS High Availability and Redundancy Configuration Guide* 』を参照してください。

バーチャライゼーションのサポート

ソフトウェアは、Virtual Device Context（VDC）をサポートしています。

（注） VDC およびリソース割り当ての詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide*』を参照してください。

各 VLAN は、プライマリ VLAN およびすべてのセカンダリ VLAN のプライベート VLAN ポートが、すべて同じ VDC に属している必要があります。プライベート VLAN は、複数の VDC に対しては設定できません。

プライベート VLAN のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
NX-OS	プライベート VLAN のライセンスは不要です。ライセンス パッケージに含まれていない機能は Cisco NX-OS システム イメージにバンドルされ、追加料金なしで提供されます。NX-OS ライセンス機構の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

ただし、VDC を使用するには、Advanced Services ライセンスが必要です。

プライベート VLAN の前提条件

プライベート VLAN 設定時の前提条件は、次のとおりです。

- デバイスにログオンしている必要があります。
- 必要に応じて、Advanced Services ライセンスをインストールし、特定の VDC を開始します。
- プライベート VLAN 機能をイネーブルにする必要があります。

注意事項および制限

プライベート VLAN 設定時の注意事項の内容は、次のとおりです。

- セカンダリ VLAN およびプライマリ VLAN の設定（p.4-9）
- プライベート VLAN ポートの設定（p.4-10）
- 他の機能に関連する制限（p.4-10）

セカンダリ VLAN およびプライマリ VLAN の設定

プライベート VLAN の設定時は、次の注意事項に従ってください。

- デフォルト VLAN（VLAN1）または内部的に割り当てられた VLAN を、プライマリ VLAN またはセカンダリ VLAN として設定することはできません。
- プライベート VLAN を設定するには、VLAN コンフィギュレーション（config-vlan）モードを使用する必要があります。
- 1 つのプライマリ VLAN に、複数の独立 VLAN およびコミュニティ VLAN を関連付けることができます。独立 VLAN またはコミュニティ VLAN は、1 つのプライマリ VLAN だけに関連付けることができます。
- プライベート VLAN により、ホストはレイヤ 2 で分離されますが、レイヤ 3 で相互に通信できます。
- セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、プライマリ VLAN の Spanning-Tree Protocol（STP; スパニングツリー プロトコル）パラメータ（ブリッジ プライオリティなど）はセカンダリ VLAN に伝播されます。ただし、他のデバイスに STP パラメータを伝播する必要はありません。プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN のスパニング ツリー トポロジが正確に一致し、これらの VLAN が同じ転送データベースを適切に共有できるかどうかを確認するには、STP 設定を手動でチェックする必要があります。
- 標準トランク ポートの場合、次の事項に注意してください。
  - プライベート VLAN 内の各 VLAN に、個別の STP インスタンスが存在します。
  - プライマリ VLAN およびすべてのセカンダリ VLAN の STP パラメータが一致している必要があります。
  - プライマリ VLAN および関連付けられたすべてのセカンダリ VLAN が、同じ Multiple Spanning Tree（MST）インスタンス内に存在している必要があります。
- 非トランク ポートの場合、次の事項に注意してください。
  - STP が認識するのは、プライベート VLAN ホスト ポートのプライマリ VLAN だけです。STP は、ホスト ポート上のセカンダリ VLAN では実行されません。

（注） ホスト ポートとして設定するすべてのポート上で BPDU ガードをイネーブルにすることを推奨します。この機能は、無差別ポート上ではイネーブルにしないでください。BPDU ガードの設定情報については、第 7 章「STP 拡張機能の設定」を参照してください。

- プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN には、別々の QoS（Quality of Service）を適用できます
- すべてのプライベート VLAN トラフィックに VACL を適用するには、プライマリ VLAN のレイヤ 3 VLAN インターフェイスまたは SVI にセカンダリ VLAN をマッピングしてから、プライマリ VLAN の SVI 上に VACL を設定します。
- プライマリ VLAN の、レイヤ 3 VLAN インターフェイスまたは SVI に適用した VACL は、マッピングが設定されている場合にのみ、関連付けられた独立 VLAN およびコミュニティ VLAN に自動的に適用されます。

- プライマリ VLAN のレイヤ 3 インターフェイスまたは SVI にセカンダリ VLAN をマッピング*せずに*、プライマリ VLAN とセカンダリ VLAN に異なる VACL を設定すると、問題が生じることがあります。
- プライベート VLAN のトラフィックは、異なる VLAN では異なる方向に伝送されるので、マッピングを設定する前に、入力トラフィック用と出力トラフィック用にそれぞれ異なる VACL を設定できます。

（注） プライベート VLAN 内のプライマリ VLAN とすべてのセカンダリ VLAN では、同じ VACL を保持する必要があります。

- DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。プライマリ VLAN 上で DHCP スヌーピングをイネーブルにすると、DHCP 設定がセカンダリ VLAN に伝播されます。セカンダリ VLAN 上に DHCP を設定しても、プライマリ VLAN 上で DHCP がすでに設定されている場合、セカンダリ VLAN 上での設定は有効になりません。
- VLAN をセカンダリ VLAN として設定する前に、セカンダリ VLAN 用のレイヤ 3 インターフェイスまたは SVI をシャットダウンする必要があります。
- 無差別ポートが設定された独立プライベート VLAN 内でのホスト間通信を防ぐには、そのサブネット内のホストの相互通信を拒否する Role-Based ACL（RBACL; ロールベース ACL）を設定します。

プライベート VLAN ポートの設定

プライベート VLAN ポートの設定時は、次の注意事項に従ってください。

- プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN にポートを割り当てる場合には、プライベート VLAN コンフィギュレーション コマンドだけを使用してください。
- プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN として設定する VLAN に割り当てられているレイヤ 2 アクセス ポートは、この VLAN がプライベート VLAN の設定に含まれている場合、非アクティブになります。プライベート VLAN を伝送するレイヤ 2 トランク インターフェイスはアクティブで、STP データベースの一部として保持されます。
- ポートチャネル グループに属すポートを、プライベート VLAN ポート として設定しないでください。ポートがプライベート VLAN の設定に含まれている場合、そのポートのポート チャネル設定は非アクティブになります。
- プライベート VLAN 設定に使用される VLAN を削除すると、その VLAN に関連付けられたプライベート VLAN ポートは非アクティブになります。

他の機能に関連する制限

プライベート VLAN の設定時は、他の機能に関連する設定上の制限を考慮してください。

（注） 状況によっては、エラー　メッセージが表示されずに設定が受け入れられますが、コマンドは無効になります。

- IGMP は、プライマリ VLAN 上でのみ実行され、すべてのセカンダリ VLAN にプライマリ VLAN の設定が使用されます。
- セカンダリ VLAN 内の IGMP 加入要求は、プライマリ VLAN で受信されたものとして処理されます。

- プライベート VLAN は、次の Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能をサポートします。
  - プライベート VLAN ポートを SPAN 送信元ポートとして設定できます。
  - プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN 上で VLAN-based SPAN（VSPAN）を使用したり、単一の VLAN 上で SPAN を使用したりして、出力トラフィックまたは入力トラフィックを個別にモニタすることができます。
- プライベート VLAN ホストまたは無差別ポートは、SPAN 宛先ポートにはできません。
- 宛先 SPAN ポートを、独立ポートにすることはできません（ただし、送信元 SPAN ポートは独立ポートにできます）。
- SPAN は、プライマリ VLAN およびセカンダリ VLAN の両方に対して設定できます。また、出力トラフィックまたは入力トラフィックのうち、どちらか一方だけに対して設定することもできます。
- プライマリ VLAN とセカンダリ VLAN 間のアソシエーションを設定すると、セカンダリ VLAN を学習したダイナミック MAC アドレスがすぐに消去されます。
- プライマリ VLAN とセカンダリ VLAN 間のアソシエーションを設定すると、セカンダリ VLAN 上で作成されたすべてのスタティック MAC アドレスが、プライマリ VLAN に挿入されます。アソシエーションを削除すると、スタティック MAC アドレスはセカンダリ VLAN だけの設定に戻ります。
- プライマリ VLAN とセカンダリ VLAN 間のアソシエーションの設定後に、セカンダリ VLAN 用のスタティック MAC アドレスを作成することはできません。
- プライマリ VLAN とセカンダリ VLAN 間のアソシエーションの設定後、このアソシエーションを削除すると、プライマリ VLAN 上に作成されたすべてのスタティック MAC アドレスは、プライマリ VLAN 上でのみ存続します。
- プライベート VLAN では、ポート セキュリティ機能はサポートされません。

（注） スタティック MAC アドレスの設定の詳細については、『*Cisco NX-OS Security Configuration Guide*』を参照してください。

プライベート VLAN の設定

（注） 特定の VLAN をプライベート VLAN として割り当てる前に、VLAN を作成しておく必要があります。

+ ここでは、次の内容について説明します。

- プライベート VLAN の設定時の注意事項（p.4-12）
- プライベート VLAN のイネーブル化（p.4-13）
- プライベート VLAN としての VLAN の設定（p.4-14）
- プライマリ プライベート VLAN へのセカンダリ VLAN の関連付け（p.4-15）
- プライマリ VLAN の VLAN インターフェイスへのセカンダリ VLAN のマッピング（p.4-17）
- プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定（p.4-19）
- プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定（p.4-20）

（注） レイヤ 3 VLAN インターフェイス（SVI）の IP アドレス指定の詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

プライベート VLAN の設定時の注意事項

プライベート VLAN の設定時は、次の注意事項に従ってください。

- セカンダリ VLAN をプライマリ VLAN と同じ MST にマップするには、**private-vlan synchronize** コマンドを入力します。
- デバイスでプライベート VLAN 機能を適用するには、プライベート VLAN をイネーブルにする必要があります。
- デバイスでこの機能を適用するには、VLAN インターフェイス機能をイネーブルにする必要があります。
- セカンダリ VLAN を設定する前に、セカンダリ VLAN として設定するすべての VLAN の VLAN インターフェイスまたは SVI をシャットダウンします。
- プライベート VLAN 機能の設定を開始する前に、「注意事項および制限」（p.4-9）を参照してください。
- プライベート VLAN モードで動作しているポートがデバイスに設定されている場合は、プライベート VLAN をディセーブルにすることはできません。

プライベート VLAN のイネーブル化

プライベート VLAN 機能を使用するには、デバイス上でプライベート VLAN をイネーブルにする必要があります。

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

手順の要約

1. **config t**
2. **feature private-vlan**
3. **exit**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**feature private-vlan**
	
	例：
	`switch(config)# feature private-vlan`
	`switch(config)#`
		デバイス上でプライベート VLAN 機能をイネーブルにします。
		
		（注） デバイス上にプライベート VLAN モードで動作しているポートが設定されている場合、**no feature private-vlan** コマンドは適用できません。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、デバイス上でプライベート VLAN 機能をイネーブルにする例を示します。

```
switch# config t
switch(config)# feature private-vlan
switch(config)#
```

プライベート VLAN としての VLAN の設定

（注） VLAN をセカンダリ VLAN（コミュニティ VLAN または独立 VLAN のどちらか）として設定する前に、その VLAN のレイヤ 3 VLAN インターフェイスまたは SVI をシャットダウンする必要があります。

VLAN は、プライベート VLAN として設定できます。

プライベート VLAN を作成するには、最初に VLAN を作成して、その VLAN をプライベート VLAN として設定します。

プライベート VLAN 内で、プライマリ VLAN、コミュニティ VLAN、または独立 VLAN として使用するすべての VLAN を作成します。そのあとで、複数の独立 VLAN および複数のコミュニティ VLAN を 1 つのプライマリ VLAN に関連付けます。複数のプライマリ VLAN とアソシエーションを設定できます。つまり、複数のプライベート VLAN を設定できます。

プライマリ VLAN またはセカンダリ VLAN のどちらかを削除すると、その VLAN に関連付けられているポートは非アクティブになります。

始める前に

プライベート VLAN 機能がイネーブルであることを確認してください。

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。異なる VDC で同じ VLAN 名と ID を繰り返し使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の要約

1. **config t**
2. **vlan** {*vlan-id* | *vlan-range*}
3. **private-vlan** {**community** | **isolated** | **primary**}
4. **exit**
5. **show vlan private-vlan** [*type*]
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**vlan** {*vlan-id* | *vlan-range*}
	
	例：
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		VLAN コンフィギュレーション サブモードを開始します。

	コマンド	目的
ステップ 3	**private-vlan** {**community** | **isolated** | **primary**} **例：** `switch(config-vlan)# private-vlan primary`	VLAN を、コミュニティ VLAN 、独立 VLAN、またはプライマリ プライベート VLAN のいずれかに設定します。プライベート VLAN には、1 つのプライマリ VLAN が必要です。コミュニティ VLAN と独立 VLAN は、複数設定できます。
	no private-vlan {**community** | **isolated** | **primary**} **例：** `switch(config-vlan)# no private-vlan primary`	指定した VLAN からプライベート VLAN 設定を削除し、標準 VLAN モードに戻します。プライマリ VLAN またはセカンダリ VLAN のどちらかを削除すると、その VLAN に関連付けられているポートは非アクティブになります。

ステップ 4	**exit**
	
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		VLAN コンフィギュレーション サブモードを終了します。

ステップ 5	**show vlan private-vlan** [*type*] **例：** `switch# show vlan private-vlan`	（オプション）プライベート VLAN の設定を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、VLAN 5 をプライマリ VLAN としてプライベート VLAN に割り当てる例を示します。

```
switch# config t
switch(config)# vlan 5
switch(config-vlan)# private-vlan primary
switch(config-vlan)# exit
switch(config)#
```

プライマリ プライベート VLAN へのセカンダリ VLAN の関連付け

セカンダリ VLAN をプライマリ VLAN に関連付けるときは、次の注意事項に従ってください。

- *secondary-vlan-list* パラメータには、スペースを挿入しないでください。複数の項目は、カンマで区切って入力できます。各項目に、単一のセカンダリ VLAN ID、またはハイフンで連結したセカンダリ VLAN ID の範囲を指定します。
- *secondary-vlan-list* パラメータに、複数のコミュニティ VLAN ID および独立 VLAN ID を指定できます。
- セカンダリ VLAN をプライマリ VLAN に関連付けるには、*secondary-vlan-list* を入力するか、**add** キーワードと *secondary-vlan-list* を入力します。
- セカンダリ VLAN とプライマリ VLAN 間のアソシエーションを消去するには、**remove** キーワードと *secondary-vlan-list* を入力します。
- セカンダリ VLAN とプライマリ VLAN 間のアソシエーションを変更するには、既存のアソシエーションを削除して、新しいアソシエーションを追加します。

プライマリ VLAN またはセカンダリ VLAN のどちらかを削除すると、その VLAN に関連付けられているポートは非アクティブになります。

no private-vlan コマンドを入力すると、VLAN は標準 VLAN モードに戻ります。その VLAN 上のアソシエーションはすべて一時停止されますが、インターフェイスはプライベート VLAN モードのままです。

特定の VLAN をプライベート VLAN モードに再変換すると、元のアソシエーションが復元されます。

プライマリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN のすべてのプライベート VLAN アソシエーションが削除されます。ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力した場合には、その VLAN のプライベート VLAN アソシエーションは一時停止するだけです。VLAN を再作成して、元のセカンダリ VLAN として設定すると、アソシエーションが再開されます。

始める前に

プライベート VLAN 機能がイネーブルであることを確認してください。

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。異なる VDC で同じ VLAN 名と ID を繰り返し使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の要約

1. **config t**
2. **vlan** *primary-vlan-id*
3. [**no**] **private-vlan association** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}
4. **exit**
5. **show vlan private-vlan** [*type*]
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**vlan** *primary-vlan-id*
	
	例：
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		プライベート VLAN の設定を行うプライマリ VLAN の番号を入力します。

ステップ 3	**private-vlan association** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*} **例：** `switch(config-vlan)# private-vlan association 100-105, 109`	セカンダリ VLAN をプライマリ VLAN に関連付けます。
	no private-vlan association **例：** `switch(config-vlan)# no private-vlan association`	プライマリ VLAN からすべてのアソシエーションを削除し、標準 VLAN モードに戻ります。

ステップ 4	**exit**
	
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		VLAN コンフィギュレーション サブモードを終了します。

	コマンド	目的
ステップ 5	**show vlan private-vlan** [**type**] **例：** switch# show vlan private-vlan	（オプション）プライベート VLAN の設定を表示します。
ステップ 6	**copy running-config startup-config** **例：** switch(config)# copy running-config startup-config	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、コミュニティ VLAN 100 ～ 105 および独立 VLAN 109 をプライマリ VLAN 5 に関連付ける例を示します。

```
switch# config t
switch(config)# vlan 5
switch(config-vlan)# private-vlan association 100-105, 109
switch(config-vlan)# exit
switch(config)#
```

プライマリ VLAN の VLAN インターフェイスへのセカンダリ VLAN のマッピング

（注） プライベート VLAN のプライマリ VLAN 上のレイヤ 3 インターフェイス（SVI）への IP アドレス指定の詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

セカンダリ VLAN を、プライマリ VLAN の VLAN インターフェイスにマッピングします。独立 VLAN およびコミュニティ VLAN は、ともにセカンダリ VLAN と呼ばれます。プライマリ VLAN の入力トラフィックをレイヤ 3 で処理するには、セカンダリ VLAN をプライマリ VLAN の VLAN インターフェイスにマッピングします。

（注） VLAN インターフェイスまたは SVI を設定する前に、VLAN インターフェイスをイネーブルにする必要があります。プライマリ VLAN に関連付けられたコミュニティ VLAN または独立 VLAN 上の VLAN インターフェイスは、アウト オブ サービスになります。稼働するのは、プライマリ VLAN 上の VLAN インターフェイスだけです。

始める前に

作業を開始する前に、次の設定を確認してください。

- プライベート VLAN 機能がイネーブルである。
- VLAN インターフェイスまたは SVI 機能がイネーブルである。
- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。異なる VDC で同じ VLAN 名と ID を繰り返し使用できるので、正しい VDC で作業していることを確認する必要があります。
- セカンダリ VLAN のマッピング先となる正しいプライマリ VLAN レイヤ 3 インターフェイス、または SVI で作業をしている。

手順の要約

1. **config t**
2. **interface vlan** *primary-vlan-ID*
3. [**no**] **private-vlan mapping** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}
4. **exit**
5. **show interface private-vlan mapping**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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 vlan** *primary-vlan-ID*
	
	例：
	`switch(config)# interface vlan 5`
	`switch(config-if)#`
		プライベート VLAN の設定を行うプライマリ VLAN の番号を入力します。プライマリ VLAN のインターフェイス コンフィギュレーション モードが開始されます。

ステップ 3	**private-vlan mapping** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*} **例：** `switch(config-if)# private-vlan mapping 100-105, 109`	セカンダリ VLAN を、プライマリ VLAN の SVI またはレイヤ 3 インターフェイスにマッピングします。これにより、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングが可能になります。
	no private-vlan mapping **例：** `switch(config-if)# no private-vlan mapping`	セカンダリ VLAN とプライマリ VLAN 間のレイヤ 3 インターフェイスへのマッピングを消去します。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**show interface vlan private-vlan mapping** **例：** `switch(config)# show interface vlan private-vlan mapping`	（オプション）インターフェイスのプライベート VLAN 情報を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、セカンダリ VLAN 100 ～ 105 および 109 を、プライマリ VLAN 5 のレイヤ 3 インターフェイスまたは SVI にマッピングする例を示します。

```
switch# config t
switch(config)# interface vlan 5
switch(config-if)# private-vlan mapping 100-105, 109
switch(config-if)# exit
switch(config)#
```

プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN のホスト ポートとして設定できます。プライベート VLAN では、ホスト ポートはセカンダリ VLAN（コミュニティ VLAN または独立 VLAN のどちらか）に含まれます。

（注） ホスト ポートとして設定したすべてのインターフェイス上で BPDU ガードをイネーブルにすることを推奨します。BPDU ガードの設定情報については、第 7 章「STP 拡張機能の設定」を参照してください。

設定したホスト ポートを、プライマリ VLAN とセカンダリ VLAN の両方に関連付けます。

始める前に

プライベート VLAN 機能がイネーブルであることを確認してください。

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。異なる VDC で同じ VLAN 名と ID を繰り返し使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の要約

1. **config t**
2. **interface** *type slot/port*
3. **switchport mode private-vlan host**
4. **switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*}
5. **exit**
6. **show interface switchport**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		プライベート VLAN ホスト ポートとして設定するレイヤ 2 ポートを選択します。

ステップ 3	**switchport mode private-vlan host**
	
	例：
	`switch(config-if)# switchport mode private-vlan host`
	`switch(config-if)#`
		レイヤ 2 ポートをプライベート VLAN のホスト ポートとして設定します。

	コマンド	目的
ステップ 4	**switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*} **例：** `switch(config-if)# switchport private-vlan host-association 10 50`	レイヤ 2 ホスト ポートを、プライベート VLAN のプライマリ VLAN およびセカンダリ VLAN に関連付けます。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のどちらでもかまいません。
	no switchport private-vlan host-association **例：** `switch(config-if)# no switchport private-vlan host-association`	ポートからプライベート VLAN のアソシエーションを削除します。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 6	**show interface switchport** **例：** `switch# show interface switchport`	（オプション）スイッチ ポートとして設定されているすべてのインターフェイスの情報を表示します。
ステップ 7	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、レイヤ 2 ポート 2/1 をプライベート VLAN のホスト ポートとして設定し、プライマリ VLAN 10 およびセカンダリ VLAN 50 に関連付ける例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode private-vlan host
switch(config-if)# switchport private-vlan host-association 10 50
switch(config-if)# exit
switch(config)#
```

プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN の無差別ポートとして設定し、その無差別ポートをプライマリ VLAN およびセカンダリ VLAN に関連付けることができます。

始める前に

プライベート VLAN 機能がイネーブルであることを確認してください。

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。異なる VDC で同じ VLAN 名と ID を繰り返し使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の要約

1. **config t**
2. **interface** *type slot/port*
3. **switchport mode private-vlan promiscuous**
4. **switchport private-vlan mapping** {*primary-vlan-id*} {*secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list*}

5. **exit**
6. **show interface switchport**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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** {*type slot/port*}
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		プライベート VLAN 無差別ポートとして設定するレイヤ 2 ポートを選択します。

ステップ 3	**switchport mode private-vlan promiscuous** **例：** `switch(config-if)# switchport mode private-vlan promiscuous`	レイヤ 2 ポートをプライベート VLAN の無差別ポートとして設定します。
ステップ 4	**switchport private-vlan mapping** {*primary-vlan-id*} {*secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list*} **例：** `switch(config-if)# switchport private-vlan mapping 10 50`	レイヤ 2 ポートを無差別ポートとして設定し、このポートをプライマリ VLAN および選択したセカンダリ VLAN のリストに関連付けます。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のどちらでもかまいません。
	no switchport private-vlan mapping **例：** `switch(config-if)# no switchport private-vlan mapping`	プライベート VLAN からマッピングを消去します。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 6	**show interface switchport** **例：** `switch# show interface switchport`	（オプション）スイッチ ポートとして設定されているすべてのインターフェイスの情報を表示します。
ステップ 7	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、レイヤ 2 ポート 2/1 を無差別ポートとして設定し、プライマリ VLAN 10 とセカンダリ独立 VLAN 50 に関連付ける例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode private-vlan promiscuous
switch(config-if)# switchport private-vlan mapping 10 50
switch(config-if)# exit
switch(config)#
```

プライベート VLAN 設定の確認

プライベート VLAN の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config vlan *vlan-id*	VLAN 情報を表示します。
show vlan private-vlan [*type*]	プライベート VLAN の情報を表示します。
show interface private-vlan mapping	インターフェイスのプライベート VLAN 情報を表示します。
show interface switchport	スイッチ ポートとして設定されているすべてのインターフェイスの情報を表示します。

これらのコマンドの出力フィールドの詳細については、『*Cisco NX-OS Lauer 2 Switching Command Reference*』を参照してください。

プライベート VLAN の統計情報の表示とクリア

プライベート VLAN の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
clear vlan [**id** *vlan-id*] **counters**	すべての VLAN または指定した VLAN のカウンタをクリアします。
show vlan counters	各 VLAN のレイヤ 2 パケット情報を表示します。

プライベート VLAN の設定例

次に、3 種類のプライベート VLAN を作成し、セカンダリ VLAN をプライマリ VLAN に関連付け、プライベート VLAN のホスト ポートと無差別ポートを作成して適正な VLAN に関連付け、VLAN インターフェイスまたは SVI を作成して、プライマリ VLAN がネットワーク全体と通信できるように設定する例を示します。

```
switch# configure terminal
switch(config)# vlan 2
switch(config-vlan)# private-vlan primary
switch(config-vlan)# vlan 3
switch(config-vlan)# private-vlan community
switch(config-vlan)# vlan 4
switch(config-vlan)# private-vlan isolated

switch(config-vlan)# vlan 2
switch(config-vlan)# private-vlan association 3,4

switch(config-vlan)# interface ethernet 1/11
switch(config-if)# switchport
switch(config-if)# switchport mode private-vlan host
switch(config-if)# interface ethernet 1/12
switch(config-if)# switchport
switch(config-if)# switchport mode private-vlan promiscuous

switch(config-if)# interface ethernet 1/11
switch(config-if)# switchport private-vlan host-association 2 3
switch(config-if)# interface ethernet 1/12
switch(config-if)# switchport private-vlan mapping 2 3,4

switch(config-if)# interface vlan 2
switch(config-if)# private-vlan mapping 3,4
```

デフォルト設定

表 4-1 に、プライベート VLAN のデフォルト設定を示します。

表 4-1　プライベート VLAN のデフォルト設定

パラメータ	デフォルト
プライベート VLAN	ディセーブル

追加情報

プライベート VLAN の実装に関する追加情報は、次のセクションを参照してください。

- 関連資料（p.4-24）
- 標準規格（p.4-24）
- MIB（p.4-24）

関連資料

関連トピック	マニュアル名
VLAN	第 3 章「VLAN の設定」
レイヤ 2 MAC アドレス	第 2 章「レイヤ 2 スイッチングの設定」
STP 拡張機能	第 7 章「STP 拡張機能の設定」
コマンド リファレンス	『*Cisco NX-OS Layer 2 Switching Command Reference*』
DCNM レイヤ 2 スイッチング コンフィギュレーション	『*Cisco DCNM Layer 2 Switching Configuration Guide*』
VLAN インターフェイス、IP アドレス指定	『*Cisco NX-OS Interfaces Configuration Guide*』
スタティック MAC アドレス、セキュリティ	『*Cisco NX-OS Security Configuration Guide*』
NX-OS の基本情報	『*Cisco NX-OS Security Configuration Guide*』
ハイ アベイラビリティ	『*Cisco NX-OS High Availability and Redundancy Guide*』
システム管理	『*Cisco NX-OS System Management Configuration Guide*』
VDC	『*Cisco NX-OS Virtual Device Context Configuration Guide*』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco NX-OS Release Notes*』 Release 4.0

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

MIB

MIB	MIB リンク
• CISCO-PRIVATE-VLAN-MIB	次の URL から、MIB の検索およびダウンロードができます。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

CHAPTER 5

Rapid PVST+ の設定

この章では、NX-OS デバイスに Rapid per VLAN Spanning Tree（Rapid PVST+）プロトコルを設定する方法について説明します。

ここでは、次の内容を説明します。

- Rapid PVST+ について（p.5-2）
- Rapid PVST+ のライセンス要件（p.5-20）
- Rapid PVST+ を設定するための前提条件（p.5-20）
- 注意事項および制約事項（p.5-20）
- Rapid PVST+ の設定（p.5-21）
- Rapid PVST+ コンフィギュレーションの確認（p.5-37）
- Rapid PVST+ 統計情報の表示およびクリア（p.5-37）
- Rapid PVST+ の設定例（p.5-37）
- デフォルト設定（p.5-38）
- 追加情報（p.5-40）

(注) Multiple Spanning Tree（MST）の詳細については、第 6 章「MST の設定」、STP 拡張の詳細については、第 7 章「STP 拡張機能の設定」を参照してください。

Rapid PVST+ について

（注） レイヤ 2 インターフェイスの作成方法については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

Spanning Tree Protocol（STP; スパニング ツリー プロトコル）は、ネットワークのレイヤ 2 でループのないネットワークを実現するために実装されました。Rapid PVST+ は、VLAN（仮想 LAN）ごとにスパニング ツリー トポロジを 1 つ作成することができる、STP の更新版です。デバイスのデフォルト STP モードは Rapid PVST+ です。

（注） スパニング ツリーは、IEEE 802.1w および IEEE 802.1s を表す場合に使用されます。このマニュアルで IEEE 802.1D STP に関して説明する場合は、具体的に 802.1D と表記されます。

（注） 各 Virtual Device Context（VDC）内では、Rapid PVST+ または MST のいずれかを実行できます。VDC で両方の STP モードを同時に実行することはできません。デフォルトの STP モードは Rapid PVST+ です。

ここでは、VLAN 単位で実装される IEEE 802.1w 標準（Rapid Spanning Tree Protocol［RSTP; 高速スパニング ツリー プロトコル］）である Rapid PVST+ プロトコルについて説明します。Rapid PVST+ は、個別の VLAN でなく、すべての VLAN に対応する単一の STP インスタンスが規定された IEEE 802.1Q VLAN 標準と相互運用されます（「Rapid PVST+ および IEEE 802.1Q トランク」[p.5-17] を参照）。

デバイスのデフォルト VLAN（VLAN1）および新規作成されたすべての VLAN では、Rapid PVST+ がデフォルトでイネーブルです。Rapid PVST+ はレガシー IEEE 802.1D STP が稼働するデバイスと相互運用されます（「Rapid PVST+ とレガシー 802.1D STP の相互運用性」[p.5-18] を参照）。

RSTP は元の STP 標準である 802.1D の改良版であり、高速コンバージェンスを実現します。

ここでは、Rapid PVST+ の概要を示します。内容は次のとおりです。

- STP（p.5-3）
- Rapid PVST+（p.5-7）
- Rapid PVST+ および IEEE 802.1Q トランク（p.5-17）
- Rapid PVST+ とレガシー 802.1D STP の相互運用性（p.5-18）
- Rapid PVST+ と 802.1s MST の相互運用性（p.5-18）
- ハイ アベイラビリティ（p.5-18）
- バーチャライゼーションのサポート（p.5-19）

（注） デバイスは、Rapid PVST+ に対して中断のない完全アップグレードをサポートしています。中断のないアップグレードの詳細については、『*Cisco NX-OS High Availability and Redundancy Guide*』を参照してください。

STP

STP は、ネットワークのループを排除しながらパスの冗長性を提供する、レイヤ 2 リンク管理プロトコルです。

ここでは、STP の基本情報を示します。内容は次のとおりです。

- 概要（p.5-3）
- トポロジの作成方法（p.5-3）
- ブリッジ ID（p.5-4）
- BPDU（p.5-6）
- ルート ブリッジの選定（p.5-6）
- スパニング ツリー トポロジの作成（p.5-7）

概要

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、2 つの端末間で存在できるアクティブ パスは 1 つだけです。STP の動作は透過的なので、端末が単一の LAN セグメントに接続されているのか、それとも複数セグメントからなるスイッチド LAN に接続されているのかを、端末が検知することはできません。

フォールトトレラントなインターネットワークを作成する場合、ネットワーク上のすべてのノード間にループフリー パスを形成する必要があります。STP アルゴリズムは、スイッチド レイヤ 2 ネットワーク上で最良のループフリー パスを算出します。レイヤ 2 LAN ポートは、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）と呼ばれる STP フレームを定期的に送受信します。ネットワーク装置はこれらのフレームを転送しないで、フレームを使用してループフリー パスを構築します。

端末間に複数のアクティブ パスがあると、ネットワーク内でループが発生する原因になります。ネットワークにループが存在する場合、端末が重複したメッセージを受信したり、ネットワーク装置が複数のレイヤ 2 LAN ポート上の端末 MAC（メディア アクセス制御）アドレスを学習したりする可能性があります。

STP は、ルート ブリッジおよびそのルートからレイヤ 2 ネットワーク上のすべてのネットワーク装置へのループフリー パスを備えたツリーを定義します。STP は冗長データ パスを強制的にブロック ステートにします。スパニング ツリーの 1 つのネットワーク セグメントで障害が発生し、冗長パスが存在する場合、STP アルゴリズムはスパニング ツリー トポロジを再計算し、ブロック パスをアクティブにします。

ネットワーク装置上の 2 つのレイヤ 2 LAN ポートがループの一部になっている場合、デバイス上のどちらのポートがフォワーディング ステートになり、どちらのポートがブロッキング ステートになるかは、STP ポート プライオリティおよびポート パス コストの設定によって決まります。STP のポート プライオリティ値は、その場所でポートがトラフィックを送受信する場合の効率を示します。STP ポート パス コスト値は、メディア速度から算出されます。

トポロジの作成方法

スパニング ツリーに参加している LAN 内のすべてのデバイスは、BPDU を交換して、ネットワーク内の他のスイッチに関する情報を収集します。この BPDU 交換により、次の作業が行われます。

- スパニング ツリー ネットワーク トポロジに対して一意のルート スイッチが選定されます。
- LAN セグメントごとに代表スイッチが 1 つ選定されます。

- 冗長スイッチ ポートをバックアップ ステートにすることにより、スイッチド ネットワーク上のループが排除されます。スイッチド ネットワーク内のどの場所からも、ルート デバイスに到達するために必要でないパスは、すべて STP ブロック ステートになります。

アクティブなスイッチド ネットワークのトポロジは、次の要素によって決まります。

- 各デバイスに対応付けられた一意のデバイス ID（デバイスの MAC アドレス）
- 各スイッチ ポートに対応付けられたルートへのパス コスト
- 各スイッチ ポートに対応付けられたポート ID

スイッチド ネットワークでは、論理上、ルート スイッチがスパニング ツリー トポロジの中心です。STP は BPDU を使用して、スイッチド ネットワークのルート スイッチおよびルート ポートを選定します。

ブリッジ ID

各ネットワーク装置上の各 VLAN には、一意の 64 ビットブリッジ ID が設定されています。ブリッジ ID はブリッジ プライオリティ値、拡張システム ID（IEEE 802.1t）、および STP MAC アドレス割り当てで構成されています。

ここでは、次の内容について説明します。

- ブリッジ プライオリティ値（p.5-4）
- 拡張システム ID（p.5-4）
- STP MAC アドレスの割り当て（p.5-5）

ブリッジ プライオリティ値

拡張システム ID がイネーブルの場合、ブリッジ プライオリティは 4 ビット値です。

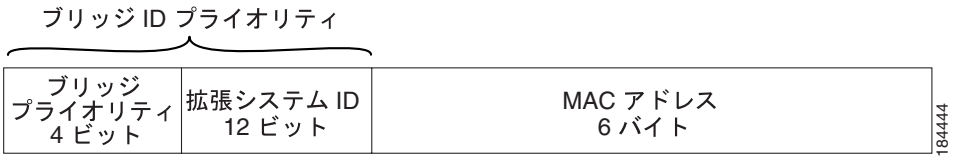
「VLAN の Rapid PVST+ hello タイムの設定」（p.5-32）を参照してください。デバイス ブリッジ ID（ルート ブリッジの ID を判別するためにスパニング ツリー アルゴリズムで使用され、最小値が優先される）に指定できるのは、4096 の倍数のみです。

（注）　このデバイスでは、拡張システム ID は常にイネーブルです。拡張システム ID をディセーブルにすることはできません。

拡張システム ID

12 ビット拡張システム ID フィールドは、ブリッジ ID の一部です（図 5-1 を参照）。

図 5-1　拡張システム ID を含むブリッジ ID



デバイスでは常に 12 ビット拡張システム ID が使用されます。

ブリッジ ID と統合することで、拡張システム ID は VLAN の一意の ID として機能します（表 5-1 を参照）。

表 5-1　拡張システム ID がイネーブルの場合のブリッジ プライオリティ値および拡張システム ID

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

STP MAC アドレスの割り当て

（注） デバイスでは常に MAC アドレス リダクションがイネーブルです。

デバイスでは常に MAC アドレス リダクションがイネーブルであるため、不要なルート ブリッジの選定を防止して、スパニング ツリー トポロジの問題を防ぐには、その他のすべてのレイヤ 2 接続ネットワーク装置でも MAC アドレス リダクションをイネーブルにする必要があります。

MAC アドレス リダクションをイネーブルにすると、ルート ブリッジ プライオリティは、4096 の倍数に VLAN ID を加えた値となります。デバイス ブリッジ ID（ルート ブリッジの ID を判別するためにスパニング ツリー アルゴリズムで使用され、最小値が優先される）に指定できるのは、4096 の倍数のみです。指定できる値は、次のとおりです。

- 0
- 4096
- 8192
- 12288
- 16384
- 20480
- 24576
- 28672
- 32768
- 36864
- 40960
- 45056
- 49152
- 53248
- 57344
- 61440

STP は拡張システム ID と MAC アドレスを使用して、VLAN ごとに一意のブリッジ ID を作成します。

（注） 同じスパニング ツリー ドメイン内の別のブリッジで MAC アドレス リダクション機能が稼働していない場合、ブリッジ ID により細かい値を選択できるため、そのブリッジがルート ブリッジの所有権を取得する可能性があります。

BPDU

ネットワーク装置は STP インスタンス全体に BPDU を送信します。各ネットワーク装置はコンフィギュレーション BPDU を送信して、スパニング ツリー トポロジを伝達および計算します。各コンフィギュレーション BPDU に含まれる最小限の情報は、次のとおりです。

- 送信側ネットワーク装置がルート　ブリッジとみなしているネットワーク装置の固有のブリッジ ID
- ルートまでの STP パス コスト
- 送信側ブリッジのブリッジ ID
- メッセージ エージ
- 送信側ポートの識別子
- 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
- STP 拡張プロトコルの追加情報

ネットワーク装置が Rapid PVST+ BPDU フレームを伝送すると、そのフレームが伝送される VLAN に接続されたすべてのネットワーク装置が BPDU を受信します。ネットワーク装置が BPDU を受信しても、フレームは転送されません。代わりに、フレームに含まれる情報を使用して BPDU が計算されます。トポロジが変更されると、ネットワーク装置は BPDU 交換を開始します。

BPDU 交換によって次の処理が行われます。

- 1 台のネットワーク装置がルート ブリッジとして選定されます。
- パス コストに基づいて、各ネットワーク装置のルート ブリッジまでの最短距離が計算されます。
- LAN セグメントごとに代表ブリッジが選択されます。このネットワーク装置はルート ブリッジに最も近いネットワーク装置であり、このネットワーク装置を経由してルートにフレームが転送されます。
- ルート ポートが選定されます。このポートにより、ブリッジからルート ブリッジまでの最適パスが提供されます。
- スパニング ツリーに含まれるポートが選択されます。

Rapid PVST+ によって BPDU に追加されるフィールドの詳細については、「Rapid PVST+ BPDU」（p.5-9）を参照してください。

ルート ブリッジの選定

VLAN ごとに、最高のブリッジ ID（数値的に最小の ID 値）を持つネットワーク装置がルート ブリッジとして選定されます。すべてのネットワーク装置がデフォルト プライオリティ（32768）に設定されている場合は、VLAN 内で最小の MAC アドレスを持つネットワーク装置がルート ブリッジになります。ブリッジ プライオリティ値はブリッジ ID の最上位ビットを占めます。

ブリッジ プライオリティ値を変更すると、デバイスがルート ブリッジとして選定される確率が変わります。小さな値を設定するとその確率が高くなり、大きな値を設定すると低くなります。

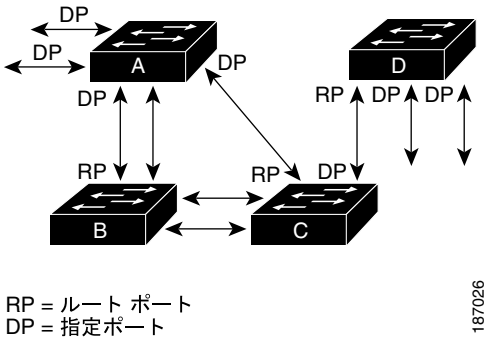
STP ルート ブリッジは、レイヤ 2 ネットワークにおける各スパニング ツリー トポロジの論理上の中心です。レイヤ 2 ネットワーク内のどの場所からも、ルート ブリッジに到達するために必要とされないパスは、すべて STP ブロッキング モードになります。

BPDU には、送信側ブリッジおよびそのポートについて、ブリッジおよび MAC アドレス、ブリッジ プライオリティ、ポート プライオリティ、パス コストなどの情報が含まれます。STP はこの情報を使用して STP インスタンスのルート ブリッジを選定し、ルート ブリッジへのルート ポートを選定し、各レイヤ 2 セグメントの Designated Port（DP; 指定ポート）を判別します。

スパニング ツリー トポロジの作成

図 5-2 では、スイッチ A がルート ブリッジに選定されます。これは、すべてのネットワーク装置でブリッジ プライオリティがデフォルト（32768）に設定されており、スイッチ A の MAC アドレスが最小であるためです。ただし、トラフィック パターン、転送ポートの数、またはリンク タイプによっては、スイッチ A が最適なルート ブリッジであるとはかぎりません。最適なネットワーク装置がルート ブリッジになるように、装置のプライオリティを上げる（数値を下げる）ことで、ルートとして最適なネットワーク装置を使用する、新しい STP トポロジを強制的に再計算させることができます。

図 5-2　スパニング ツリー トポロジ



スパニング ツリー トポロジをデフォルトのパラメータに基づいて計算すると、スイッチド ネットワーク上の送信元から宛先端末までのパスが最適にならない可能性があります。たとえば、現在のルート ポートよりも数値の大きいポートに高速リンクを接続すると、ルート ポートが変更される場合があります。最高速のリンクをルート ポートにすることが重要です。

たとえば、スイッチ B の 1 つのポートが光ファイバ リンクであり、同じスイッチの別のポート（Unshielded Twisted-Pair [UTP; シールドなしツイストペア] リンク）がルート ポートになっていると仮定します。ネットワーク トラフィックを高速の光ファイバ リンクに流した方が効率的です。光ファイバ ポートの STP ポート プライオリティをルート ポートよりも上げると（数値を下げる）、光ファイバ ポートが新しいルート ポートになります。

Rapid PVST+

ここでは、次の内容について説明します。

- 概要（p.5-8）
- Rapid PVST+ BPDU（p.5-9）
- 提案合意ハンドシェイク（p.5-10）
- プロトコル タイマー（p.5-11）
- ポート ロール（p.5-11）
- ポート ステート（p.5-12）
- ポート ロールの同期化（p.5-14）
- 単一方向リンク障害の検出（p.5-16）
- ポート コスト（p.5-16）
- ポート プライオリティ（p.5-17）

概要

Rapid PVST+ は VLAN 単位で実装される IEEE 802.1w（RSTP）標準です。（STP を手動でディセーブルにしないかぎり）設定されている VLAN ごとに 1 つの STP インスタンスが動作します。VLAN 上の各 Rapid PVST+ インスタンスには、それぞれ 1 つのルート スイッチがあります。Rapid PVST+ が稼働している場合、STP は、VLAN 単位でイネーブルまたはディセーブルにできます。

（注） デバイスのデフォルト STP モードは Rapid PVST+ です。

Rapid PVST+ は、ポイントツーポイント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。Rapid PVST+ を使用した場合、スパニング ツリーの再設定は 1 秒以内に実行できます（802.1D STP のデフォルト設定の場合は 50 秒かかります）。PVID は自動的にチェックされます。

（注） Rapid PVST+ は VLAN ごとに STP インスタンスを 1 つサポートします。

Rapid PVST+ を使用すると、STP コンバージェンス時間が短縮されます。デフォルトでは、STP 内の各指定ポートは 2 秒おきに BPDU を送信します。トポロジ内の指定ポートで、hello メッセージが 3 回連続して受信されない場合、または最大エージング タイムが満了した場合、ポートはテーブル内のすべてのプロトコル情報をただちにフラッシュします。ポートで BPDU が受信されなかった回数が 3 に達するか、または最大エージング タイムが満了した場合、ポートは直接接続されたネイバーの指定ポートとの接続が切断されているとみなします。このように、プロトコル情報を短時間で期限切れにすることによって、障害を短時間で検出できます。

Rapid PVST+ には、デバイス、デバイス ポート、または LAN に障害が発生したあとに、短時間で接続を回復する機能があります。エッジ ポート、新規ルート ポート、およびポイントツーポイント リンクで接続されたポートに対して、次のような高速コンバージェンス機能を提供します。

- エッジ ポート — RSTP デバイス上のポートをエッジ ポートに設定すると、そのエッジ ポートは即座にフォワーディング ステートになります（この短時間での移行は、従来は、PortFast というシスコ独自の機能で実現されていました）。単一の端末に接続されるポートのみをエッジ ポートとして設定してください。リンクが変更されても、エッジ ポートによるトポロジ変更は発生しません。

  ポートを STP エッジ ポートとして設定するには、**spanning-tree port type** インターフェイス コンフィギュレーション コマンドを入力します。

（注） レイヤ 2 ホストに接続されたすべてのポートをエッジ ポートとして設定することを推奨します。STP ポート タイプの詳細については、第 7 章「STP 拡張機能の設定」を参照してください。

- ルート ポート — Rapid PVST+ が新規ルート ポートを選択した場合、古いルート ポートをブロックして、即座に新規ルート ポートをフォワーディング ステートに移行します。
- ポイントツーポイント リンク — ポイントツーポイント リンクを介してポートを別のポートに接続してローカル ポートが指定ポートになる場合、ループのないトポロジを実現するために、提案合意ハンドシェイクを使用して相手側ポートと高速移行をネゴシエーションします。

Rapid PVST+ がフォワーディング ステートへの高速移行を実現できるのは、エッジ ポートおよびポイントツーポイント リンク上のみです。リンク タイプを設定できますが、リンク タイプ情報はポートのデュプレックス設定から自動的に取得されます。全二重ポートはポイントツーポイント ポートであるとみなされ、半二重ポートは共有ポートであるとみなされます。

エッジ ポートでトポロジ変更は発生しませんが、その他のすべての指定ポートおよびルート ポートでは、直接接続されたネイバーからの BPDU 受信に 3 回連続で失敗するか、または最大エージング タイムが満了した場合、TC（トポロジ変更）BPDU が生成されます。この時点で、指定ポートまたはルート ポートは TC フラグが設定された BPDU を送信します。該当するポートで TC 時間タイマーが稼働しているかぎり、BPDU に TC フラグは設定されたままです。TC 時間タイマーの値は、hello タイムの設定値に 1 秒を加えた値です。トポロジ変更が最初に検出された場所から、即座にこの情報がトポロジ全体にフラッディングされます。

Rapid PVST+ がトポロジ変更を検出すると、以下の処理が実行されます。

- 必要に応じて、すべての非エッジ ルート ポートおよび指定ポートに対して、hello タイムの 2 倍の値に設定された TC 時間タイマーを開始します。
- これらのすべてのポートに関連付けられた MAC アドレスをフラッシュします。

トポロジ変更通知はトポロジ全体に短時間でフラッディングされます。トポロジ変更が受信されると、ダイナミック エントリはポート単位ですぐに消去されます。

（注） TCA フラグが使用されるのは、そのデバイスが、レガシー 802.1D STP が稼働しているデバイスと相互作用している場合のみです。Rapid PVST+ と 802.1D STP の相互作用の詳細については、「Rapid PVST+ とレガシー 802.1D STP の相互運用性」（p.5-18）を参照してください。

トポロジ変更後、提案合意シーケンスがネットワーク エッジ方向に迅速に伝播され、接続が迅速に復元されます（「ポート ロールの同期化」[p.5-14] を参照）。

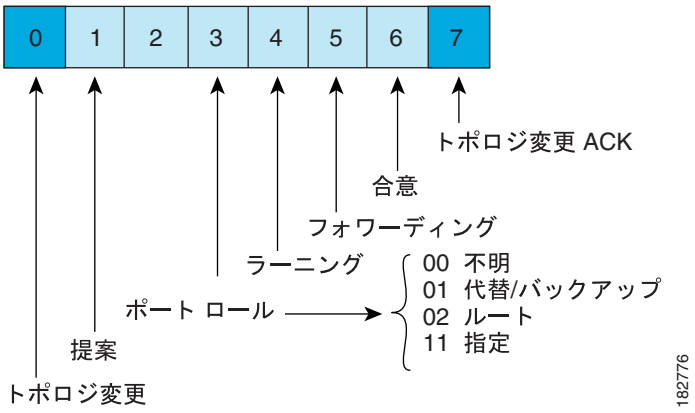
Rapid PVST+ BPDU

Rapid PVST+ および 802.1w では、次の情報を追加するために、フラグ バイトの 6 ビットをすべて使用しています。

- BPDU の送信元ポートのロールおよびステート
- 提案合意ハンドシェイク

図 5-3 に、Rapid PVST+ での BPDU フラグの使用方法を示します。

図 5-3　BPDU 内の Rapid PVST+ フラグ バイト

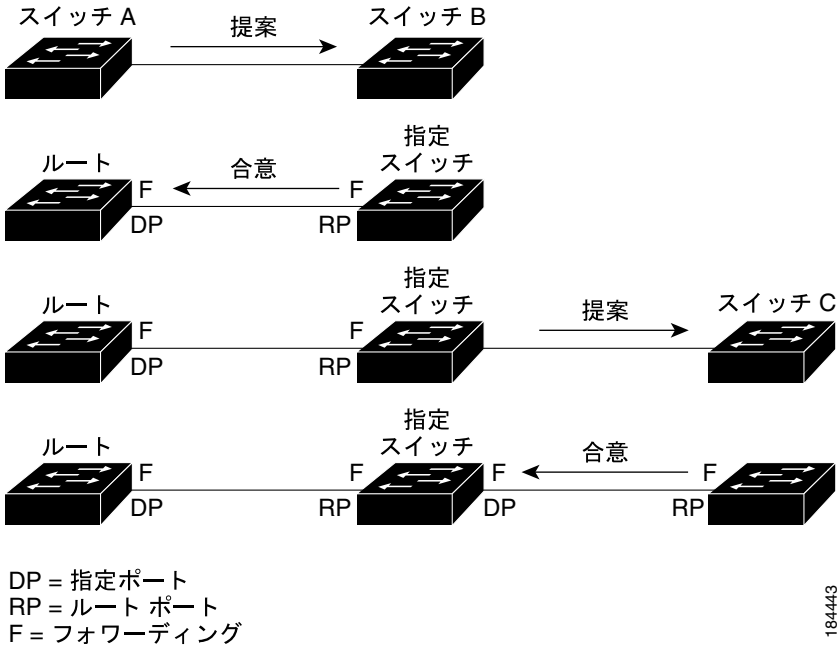


もう 1 つの重要な変更点は、Rapid PVST+ BPDU がタイプ 2、バージョン 2 であるため、デバイスが接続先のレガシー（802.1D）ブリッジを検出できることです。802.1D の BPDU はタイプ 0、バージョン 0 です。

提案合意ハンドシェイク

スイッチ A はポイントツーポイント リンクを介してスイッチ B に接続されており、すべてのポートがブロッキング ステートになります（図 5-4 を参照）。スイッチ A のプライオリティがスイッチ B のプライオリティよりも数値的に小さいと仮定します。

図 5-4　高速コンバージェンスの提案合意ハンドシェイク



デバイス A は提案メッセージ（提案フラグが設定されたコンフィギュレーション BPDU）をデバイス B に送信して、自身を代表デバイスにするように提案します（図 5-4 を参照）。

デバイス B が提案メッセージを受信すると、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、すべての非エッジ ポートを強制的にブロッキング ステートにします。さらに、その新しいルート ポート経由で合意メッセージ（合意フラグが設定された BPDU）を送信します。

デバイス A は、スイッチ B から合意メッセージを受信すると、ただちに自身の指定ポートをフォワーディング ステートにします。デバイス B はすべての非エッジ ポートをブロックしており、さらにスイッチ A と B はポイントツーポイント リンクで接続されているため、ネットワークにループは形成されません（ポート ステートの詳細については、「ポート ステート」[p.5-12] を参照）。

デバイス C がデバイス B に接続された場合も、同様の一連のハンドシェイク メッセージが交換されます。デバイス C はデバイス B に接続されたポートをルート ポートとして選択し、リンクの両端はすぐにフォワーディング ステートに移行します。このハンドシェイク プロセスを繰り返すたびに、もう 1 つのデバイスがアクティブ トポロジに追加されます。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はルートからスパニング ツリーのリーフに進みます。

スイッチはポートのデュプレックス モードからリンク 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みなされ、半二重ポートは共有接続とみなされます。**spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを入力すると、デュプレックス設定で制御されたデフォルト設定を上書きすることができます。

この提案合意ハンドシェイクが開始されるのは、非エッジ ポートがブロッキング ステートからフォワーディング ステートに移行した場合のみです。ハンドシェイク プロセスは、トポロジ全体に段階的に拡散します。

プロトコル タイマー

表 5-2 に、Rapid PVST+ のパフォーマンスに影響するプロトコル タイマーを示します。

表 5-2　Rapid PVST+ プロトコル タイマー

変数	説明
hello タイマー	ネットワーク装置間で BPDU をブロードキャストする頻度を決定します。デフォルトは 2 秒で、指定できる範囲は 1 ～ 10 です。
転送遅延タイマー	ポートが転送を開始するまでの、リスニング ステートおよびラーニング ステートが継続する時間を決定します。このタイマーは通常、プロトコルで使用されません。ただし、802.1D スパニング ツリーと相互運用する場合は、使用されます。デフォルトは 15 秒で、指定できる範囲は 4 ～ 30 秒です。
最大エージング タイマー	ポートで受信したプロトコル情報がネットワーク装置によって保管される時間を決定します。このタイマーは通常、プロトコルで使用されません。ただし、802.1D スパニング ツリーと相互運用する場合は、使用されます。デフォルトは 20 秒で、指定できる範囲は 6 ～ 40 秒です。

ポート ロール

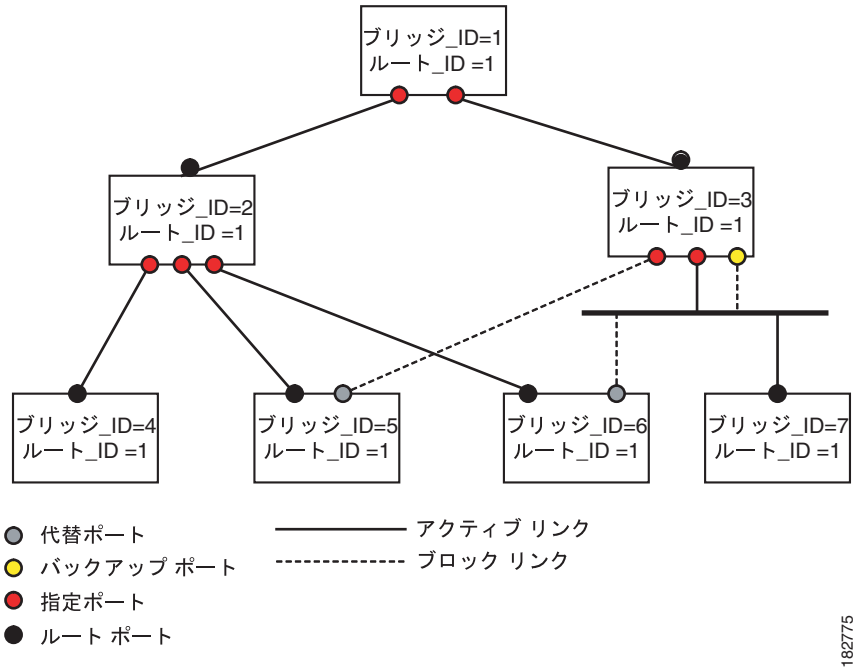
Rapid PVST+ では、ポート ロールを割り当ててアクティブ トポロジを学習することで、スパニング ツリーの高速コンバージェンスを実現します。「ルート ブリッジの選定」（p.5-6）で説明しているように、Rapid PVST+ は、802.1D STP を利用して、最も高いスイッチ プライオリティ（最小プライオリティ値）を持つデバイスをルート ブリッジとして選択します。Rapid PVST+ は、次に示すポート ロールの 1 つを各ポートに割り当てます。

- ルート ポート — デバイスがルート ブリッジにパケットを転送する際に最適なパス（最小コスト）を提供します。
- 指定ポート — LAN からルート ブリッジにパケットを転送する際に最小パス コストになる指定デバイスに接続します。指定デバイスが LAN に接続されるポートを指定ポートと呼びます。
- 代替ポート — 現在のルート ポートが提供するルート ブリッジへの代替パスを提供します。また、トポロジ内の別のデバイスへのパスを提供します。
- バックアップ ポート — 指定ポートが提供する、スパニング ツリーのリーフへの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 リンクで接続されている場合、または 1 つのデバイスに共有 LAN セグメントへの接続が複数ある場合のみ、使用できます。バックアップ ポートは、トポロジ内のデバイスに対する別のパスを提供します。
- ディセーブル ポート — スパニング ツリーの処理における役割が指定されていないポートです。

ネットワーク全体で一貫したポート ロールがある安定したトポロジでは、Rapid PVST+ により各ルート ポートおよび指定ポートは即座にフォワーディング ステートに移行し、すべての代替ポートおよびバックアップ ポートは常にブロッキング ステートになります。指定ポートは、ブロッキング ステートから開始します。ポート ステートにより、フォワーディング プロセスおよびラーニング プロセスの動作が制御されます。

ルート ポートまたは指定ポートのロールが割り当てられたポートは、アクティブ トポロジに含まれます。代替ポートまたはバックアップ ポートのロールが割り当てられたポートは、アクティブ トポロジから除外されます（図 5-5 を参照）。

図 5-5　ポート ロールを示すトポロジ例



ポート ステート

ここでは、Rapid PVST+ および MST のポート ステートについて説明します。内容は次のとおりです。

- Rapid PVST+ のポート ステートの概要（p.5-12）
- ブロッキング ステート（p.5-13）
- ラーニング ステート（p.5-13）
- フォワーディング ステート（p.5-14）
- ディセーブル ステート（p.5-14）
- ポート ステートの概要（p.5-14）

Rapid PVST+ のポート ステートの概要

プロトコル情報がスイッチド LAN を通過するとき、伝播遅延が生じることがあります。その結果、スイッチド ネットワークのさまざまな時点および場所でトポロジの変化が発生します。レイヤ 2 LAN ポートがスパニング 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可能性があります。ポートは新しいトポロジ情報がスイッチド LAN 経由で伝播されるまで待機し、それからフレーム転送を開始する必要があります。

Rapid PVST+ または MST を使用する NX-OS の各レイヤ 2 LAN ポートは、次の 4 つのステートのいずれかになります。

- ブロッキング — レイヤ 2 LAN ポートがフレーム転送に参加していない状態です。

- ラーニング — レイヤ 2 LAN ポートがフレーム転送に参加する準備をしている状態です。
- フォワーディング — レイヤ 2 LAN ポートはフレームを転送します。
- ディセーブル — レイヤ 2 LAN ポートが STP に参加せず、フレームを転送していない状態です。

Rapid PVST+ をイネーブルにすると、デバイス上のすべてのポート、VLAN、およびネットワークは、電源投入時に必ずブロッキング ステートを経て、それからラーニングという移行ステートに進みます。設定が適切であれば、各レイヤ 2 LAN ポートはフォワーディング ステートまたはブロッキング ステートで安定します。

STP アルゴリズムによってレイヤ 2 LAN ポートがフォワーディング ステートになると、次の処理が行われます。

1. レイヤ 2 LAN ポートがブロッキング ステートになり、ラーニング ステートに移行するように指示するプロトコル情報を待ちます。
2. レイヤ 2 LAN ポートが転送遅延タイマーの満了を待ち、満了した時点でラーニング ステートになり、転送遅延タイマーをリセットします。
3. ラーニング ステートで、レイヤ 2 LAN ポートはフレーム転送を引き続きブロックしながら、転送データベースの端末のロケーション情報を学習します。
4. レイヤ 2 LAN ポートは、転送遅延タイマーの終了とともにフォワーディング ステートになり、学習およびフレーム転送が両方ともイネーブルになります。

ブロッキング ステート

ブロッキング ステートのレイヤ 2 LAN ポートは、フレーム転送に参加しません。

ブロッキング ステートのレイヤ 2 LAN ポートの動作は、次のとおりです。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- アドレス データベースに、端末のロケーション情報は組み込みません（ブロッキング状態のレイヤ 2 LAN ポートに関する学習は行われないため、アドレス データベースは更新されません）。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから送られた BPDU を受信し、処理して送信します。
- コントロール プレーン メッセージを受信して応答します。

ラーニング ステート

ラーニング ステートのレイヤ 2 LAN ポートは、フレームの MAC アドレスを学習して、フレーム転送に参加するための準備を行います。レイヤ 2 LAN ポートは、ブロッキング ステートからラーニング ステートを開始します。

ラーニング ステートのレイヤ 2 LAN ポートの動作は、次のとおりです。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- 端末のロケーション情報をアドレス データベースに組み込みます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから送られた BPDU を受信し、処理して送信します。
- コントロール プレーン メッセージを受信して応答します。

フォワーディング ステート

フォワーディング ステートのレイヤ 2 LAN ポートはフレームを転送します。レイヤ 2 LAN ポートは、ラーニング ステートからフォワーディング ステートを開始します。

フォワーディング ステートのレイヤ 2 LAN ポートの動作は、次のとおりです。

- 接続セグメントから受信したフレームを転送します。
- 転送用に他のポートからスイッチングされたフレームを転送します。
- 端末のロケーション情報をアドレス データベースに組み込みます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから受信した BPDU を処理します。
- コントロール プレーン メッセージを受信して応答します。

ディセーブル ステート

ディセーブル ステートのレイヤ 2 LAN ポートは、フレーム転送または STP に参加しません。ディセーブル ステートのレイヤ 2 LAN ポートは事実上、動作することはありません。

ディセーブル ステートのレイヤ 2 LAN ポートの動作は、次のとおりです。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- アドレス　データベースに、端末のロケーション情報は組み込みません（学習は行われないため、アドレス データベースは更新されません）。
- ネイバーから BPDU を受信しません。
- システム モジュールから送信用の BPDU を受信しません。

ポート ステートの概要

表 5-3 に、ポートの有効な動作ステートと Rapid PVST+ ステート、およびポートがアクティブ トポロジに含まれるかどうかを示します。

表 5-3　ポート ステートとアクティブ トポロジ

動作ステータス	ポート ステート	アクティブ トポロジ内のポートの有無
イネーブル	ブロッキング	なし
イネーブル	ラーニング	あり
イネーブル	フォワーディング	あり
ディセーブル	ディセーブル	なし

ポート ロールの同期化

デバイスのポートの 1 つが提案メッセージを受信し、そのポートが新しいルート ポートとして選択されると、Rapid PVST+ は他のすべてのポートを新しいルート情報に強制的に同期化させます。

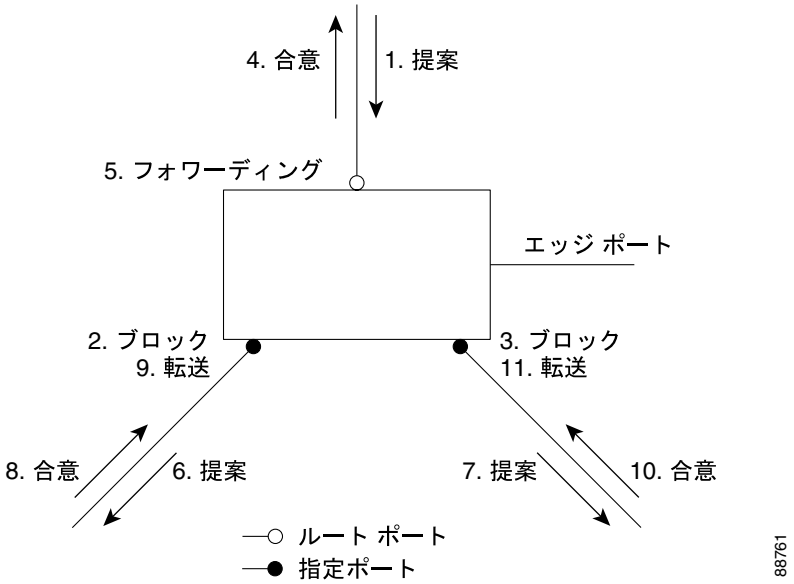
他のポートがすべて同期化されると、デバイスはルート ポートで受信した上位のルート情報と同期化されます。次のいずれかの場合は、デバイスの個別のポートが同期されます。

- ポートがブロッキング ステートの場合
- エッジ ポート（ネットワークのエッジ上に設定されているポート）の場合

指定ポートがフォワーディング ステートであり、エッジ ポートとして設定されていない場合、Rapid PVST+ によって新しいルート情報に強制的に同期化されると、その指定ポートはブロッキング ステートに移行します。一般に、Rapid PVST+ がポートをルート情報に強制的に同期させ、ポートが上記のいずれの条件も満たしていない場合、そのポートのステートはブロッキングに設定されます。

デバイスはすべてのポートが同期されたことを確認すると、そのルート ポートに対応する指定デバイスに合意メッセージを送信します。ポイントツーポイント リンクによって接続されたスイッチがそれぞれのポート ロールについて合意すると、Rapid PVST+ はポートのステートを即座にフォワーディング ステートに移行させます。図 5-6 に、このイベント シーケンスを示します。

図 5-6　高速コンバージェンス時のイベント シーケンス



ここでは、次の内容について説明します。

- 上位 BPDU 情報の処理（p.5-15）
- 不良 BPDU 情報の処理（p.5-16）

上位 BPDU 情報の処理

上位 BPDU は、現在ポートに格納されているものよりも上位のルート情報（小さいスイッチ ID、低いパス コストなど）を持つ BPDU です。

ポートが上位 BPDU を受信すると、Rapid PVST+ は再構成を開始します。そのポートが新しいルート ポートとして提案され選択されると、Rapid PVST+ はすべての非エッジ、指定ポートを強制的に同期化します。

受信した BPDU が提案フラグの設定された Rapid PVST+ BPDU である場合、デバイスは他のすべてのポートを同期化してから合意メッセージを送信します。以前のポートがブロッキング ステートになるとすぐに、新しいルート ポートがフォワーディング ステートに移行します。

ポートで上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、Rapid PVST+ によりポートはブロッキング ステートに設定され、合意メッセージが送信されます。指定ポートは、転送遅延タイマーが満了するまで、提案フラグが設定された BPDU を送信し続けます。転送遅延タイマーが満了すると、指定ポートはフォワーディング ステートに移行します。

不良 BPDU 情報の処理

不良 BPDU は、現在ポートに格納されているものよりも下位のルート情報（大きいスイッチ ID、高いパス コストなど）を持つ BPDU です。

指定ポートが不良 BPDU を受信すると、その指定ポートは自身の情報を即座に応答します。

単一方向リンク障害の検出

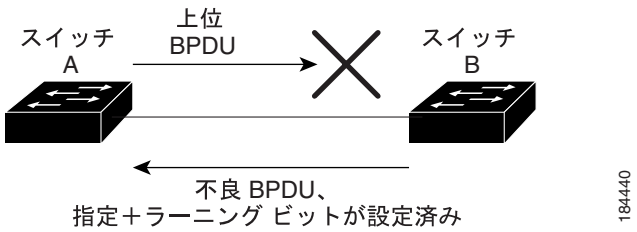
ソフトウェアは、受信した BPDU のポート ロールとステートの一貫性をチェックし、Unidirectional Link Detection（UDLD; 単一方向リンク検出）機能を使用して、ブリッジング ループが発生する可能性のある単一方向リンク障害を検出します。この機能は、異議メカニズムに基づいています。

UDLD の詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

指定ポートが矛盾を検出するとロールは維持されますが、状態は廃棄ステートに戻ります。これは、接続に矛盾が生じた場合、ブリッジング ループを開始するよりも接続を中断する方が好ましいためです。

図 5-7 に、ブリッジング ループの一般的な原因となる単一方向リンク障害を示します。スイッチ A はルート ブリッジで、その BPDU はデバイス B へのリンクで損失されます。802.1w 標準の BPDU には、送信ポートのロールとステートが含まれます。スイッチ A はこの情報を使用して、スイッチ B がスイッチ A の送信した上位 BPDU に反応せず、スイッチ B がルート ポートではなく、指定ポートであることを検出できます。その結果、スイッチ A はスイッチ B のポートをブロックする（またはブロックし続ける）ので、ブリッジング ループが回避されます。

図 5-7　単一方向リンク障害の検出



（注）　ブリッジ保証機能の詳細については、第 7 章「STP 拡張機能の設定」も参照してください。

ポート コスト

（注）　Rapid PVST+ はデフォルトで、ショート（16 ビット）パスコスト方式を使用してコストを計算します。ショート パスコスト方式の場合は、1 ～ 65535 の任意の値を割り当てることができます。ただし、ロング（32 ビット）パスコスト方式を使用するようにデバイスを設定すると、1 ～ 200,000,000 の任意の値を割り当てることができます。パスコスト計算方式はグローバルに設定されます。

STP ポート パスコストのデフォルト値は、LAN インターフェイスのメディア速度およびパスコスト計算方式から決定されます（表 5-4 を参照）。ループが発生すると、STP はポート コストを考慮して、フォワーディング ステートにする LAN インターフェイスを選択します。

表 5-4　デフォルトのポート コスト

帯域幅	ポート コストのショート パス コスト方式	ポート コストのロング パス コスト方式
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 ギガビット イーサネット	4	20,000
10 ギガビット イーサネット	2	2,000

STP に最初に選択させたい LAN インターフェイスには低いコスト値を、最後に選択させたい LAN インターフェイスには高いコスト値を割り当てることができます。すべての LAN インターフェイスが同じコスト値を使用している場合には、STP は LAN インターフェイス番号が最も小さい LAN インターフェイスをフォワーディング ステートにして、残りの LAN インターフェイスをブロックします。

アクセス ポートでは、ポート単位でポート コストを割り当てます。トランク ポートでは、VLAN 単位でポート コストを割り当てます。トランク ポートのすべての VLAN に同じポート コストを設定できます。

ポート プライオリティ

複数のポートのパス コストが同じである場合に、冗長パスが発生すると、Rapid PVST+ はポート プライオリティを考慮して、フォワーディング ステートにする LAN ポートを選択します。Rapid PVST+ に最初に選択させたい LAN ポートには低いプライオリティ値を、最後に選択させたい LAN ポートには最も高いプライオリティ値を割り当てることができます。

すべての LAN ポートが同じプライオリティ値を使用している場合には、Rapid PVST+ は LAN ポート番号が最も小さい LAN ポートをフォワーディング ステートにして、残りの LAN ポートをブロックします。プライオリティの有効範囲は 0 ～ 224（デフォルトは 128）で、32 単位で設定できます。NX-OS デバイスは LAN ポートがアクセス ポートとして設定されている場合にはポート プライオリティ値を使用し、LAN ポートがトランク ポートとして設定されている場合には VLAN ポート プライオリティ値を使用します。

Rapid PVST+ および IEEE 802.1Q トランク

802.1Q トランクによって、ネットワークの STP の構築方法に、いくつかの制約が課されます。802.1Q トランクを使用して接続しているシスコのネットワーク装置では、トランク上で許容される VLAN ごとに 1 つの STP インスタンスが維持されます。しかし、他社製の 802.1Q ネットワーク装置では、トランク上で許容されるすべての VLAN に対して 1 つの STP インスタンス（Common Spanning Tree [CST]）しか維持されません。

802.1Q トランクを使用してシスコのネットワーク装置を他社製のネットワーク装置に接続する場合、シスコのネットワーク装置は、トランクの 802.1Q VLAN の STP インスタンスを、他社製の 802.1Q ネットワーク装置の STP インスタンスと統合します。ただし、シスコのネットワーク装置によって維持される VLAN 別の STP 情報はすべて、他社製の 802.1Q ネットワーク装置のクラウドによって切り離されます。シスコのネットワーク装置を隔てている他社製の 802.1Q 装置のクラウドは、ネットワーク装置間の単一トランク リンクとして処理されます。

802.1Q トランクの詳細については、『*Cisco NX-OS Interface Configuration Guide*』を参照してください。

Rapid PVST+ とレガシー 802.1D STP の相互運用性

Rapid PVST+ は、レガシー 802.1D プロトコルが稼働しているデバイスと相互運用できます。BPDU バージョン 0 を受信したデバイスは、802.1D が稼働している装置と相互運用していることを認識します。Rapid PVST+ の BPDU はバージョン 2 です。受信した BPDU が 802.1w BPDU バージョン 2 であり、提案フラグが設定されている場合、デバイスはその他のすべてのポートが同期化されたあとに、合意メッセージを送信します。BPDU が 802.1D BPDU バージョン 0 の場合、デバイスは提案フラグを設定せずにポートの転送遅延タイマーを開始します。新しいルート ポートは、フォワーディング ステートに移行するために 2 倍の転送遅延時間を必要とします。

デバイスは、次のように、レガシー 802.1D デバイスと相互運用します。

- 通知 — 802.1D BPDU と異なり、802.1w は TCN BPDU を使用しません。ただし、802.1D スイッチと相互運用性を保つために、NX-OS デバイスは TCN BPDU の処理と生成を行います。
- 確認 — 802.1w デバイスは、指定ポートで 802.1D デバイスから TCN メッセージを受信すると、TCA ビットが設定された 802.1D コンフィギュレーション BPDU で応答します。ただし、802.1D デバイスに接続されたルート ポートで TC 時間タイマー（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 が設定されたコンフィギュレーション BPDU を受信した場合、TC 時間タイマーがリセットされます。

  この処理方法は、802.1D スイッチにのみ必要です。802.1w BPDU には TCA ビットが設定されません。
- プロトコルの移行 — 802.1D スイッチとの下位互換性を保つために、802.1w は 802.1D コンフィギュレーション BPDU と TCN BPDU をポート単位で選択的に送信します。

  ポートが初期化されると、移行遅延タイマーが開始され（802.1w BPDU を送信する最短時間を指定）、802.1w BPDU が送信されます。このタイマーがアクティブの間、デバイスは目的のポートで受信されたすべての BPDU を処理し、プロトコル タイプは無視します。

  ポートの移行遅延タイマーの期限が切れたあとに、デバイスが 802.1D BPDU を受信した場合、デバイスは 802.1D デバイスに接続されたと認識し、802.1D BPDU のみの使用を開始します。ただし、802.1w デバイスがポートで 802.1D BPDU を使用している場合、タイマー満了後に 802.1w BPDU を受信すると、デバイスはタイマーを再起動し、そのポートで 802.1w BPDU の使用を開始します。

（注） 同じ LAN セグメント上のすべてのデバイスで、インターフェイスごとにプロトコルを再初期化する場合は、Rapid PVST+ を再初期化する必要があります。詳細については、「プロトコルの再初期化」（p.5-36）を参照してください。

Rapid PVST+ と 802.1s MST の相互運用性

Rapid PVST+ は IEEE 802.1s MST 標準とシームレスに相互運用されます。ユーザ設定は不要です。このシームレスな相互運用性をディセーブルにするための PVST シミュレーションの詳細については、第 7 章「STP 拡張機能の設定」を参照してください。

ハイ アベイラビリティ

ソフトウェアは Rapid PVST+ に対してハイ アベイラビリティをサポートしています。ただし、Rapid PVST+ を再起動した場合、統計情報およびタイマーは復元されません。タイマーは再起動し、統計情報は 0 から開始します。

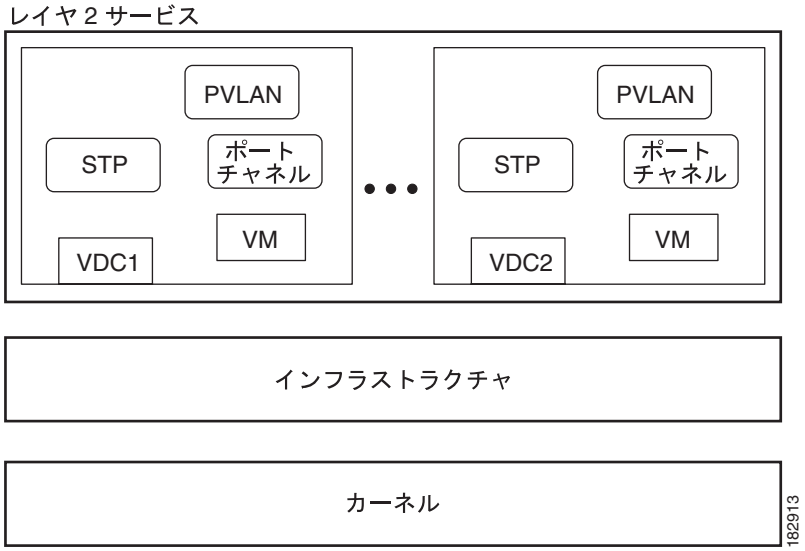
(注)　ハイ アベイラビリティ機能の詳細については、『*Cisco NX-OS High Availability and Redundancy Configuration Guide*』を参照してください。

バーチャライゼーションのサポート

(注)　VDC およびリソース割り当ての詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide*』を参照してください。

システムでは VDC をサポートしています。VDC を使用すると、VDC ごとに独立したレイヤ 2 バーチャライゼーションが実現し、VDC ごとに独立した STP 2 が実行されます（図 5-8 を参照）。

図 5-8　VDC ごとに個別の STP



VDC ごとに独自の Rapid PVST+ が使用されます。NX-OS ソフトウェアを使用している場合、複数の VDC にわたって Rapid PVST+ を設定することはできません。ただし、1 つの VDC で Rapid PVST+ を実行し、別の VDC で MST を実行することはできます。正しい VDC を開始していることを確認してから、Rapid PVST+ または MST パラメータを設定してください。

たとえば、VDC1 で MST、VDC2 で Rapid PVST+、VDC3 で MST を稼働させることができます。

Rapid PVST+ のライセンス要件

次の表に、この機能に関するライセンス要件を示します。

製品	ライセンス要件
NX-OS	Rapid PVST+ にライセンスは不要です。ライセンス パッケージに含まれていない機能は Cisco NX-OS システム イメージにバンドルされ、無料で提供されます。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

ただし、VDC を使用する場合は、Advanced Services ライセンスが必要です。

Rapid PVST+ を設定するための前提条件

Rapid PVST+ には次の前提条件があります。

- デバイスにログオンする必要があります。
- 必要に応じて、Advanced Services ライセンスをインストールし、目的の VDC を開始します。
- デフォルト以外の VDC で作業する場合は、目的の VDC を作成しておく必要があります。

注意事項および制約事項

Rapid PVST を設定する場合は、次の制限および制約事項に従ってください。

- VDC ごとの Rapid PVST+ の総数は 4000 です。
- VLAN およびポートの最大数は 75,000 です。
- 各 VDC で一度にアクティブにできるのは、Rapid PVST+ または MST のいずれか 1 つのみです。
- ポート チャネリング — ポート チャネル バンドルは、単一ポートとみなされます。ポート コストは、このチャネルに割り当てられたすべての設定済みポート コストの合計値です。
- プライベート VLAN：
  - トランク ポートでは、プライマリおよびセカンダリ プライベート VLAN は 2 つの異なる論理ポートです。両方の VLAN に、まったく同じ STP トポロジが*必要です*。
  - アクセス ポートでは、STP はプライマリ VLAN のみを認識します。
- レイヤ 2 ホストに接続されたすべてのポートを STP エッジ ポートとして設定することを推奨します。STP ポート タイプの詳細については、第 7 章「STP 拡張機能の設定」を参照してください。
- STP は常にイネーブルのままにしておきます。
- タイマーは変更しないでください。安定性が低下することがあります。
- ユーザ トラフィックが管理 VLAN に流れないようにして、管理 VLAN とユーザ データを常に分離するようにしてください。
- プライマリおよびセカンダリ ルート スイッチの場所として、ディストリビューション レイヤおよびコア レイヤを選択します。
- 802.1Q トランクを介して 2 台のシスコ製デバイスを接続すると、トランク上で許容される VLAN ごとにスパニング ツリー BPDU が交換されます。トランクのネイティブ VLAN 上の BPDU は、タグなしの状態で、予約済み 802.1D スパニング ツリー マルチキャスト MAC アドレス（01-80-C2-00-00-00）に送信されます。トランクのすべての VLAN 上の BPDU は、タグ付きの状態で、予約済み Cisco Shared Spanning Tree Protocol（SSTP）マルチキャスト MAC アドレス（01-00-0c-cc-cc-cd）に送信されます。

Rapid PVST+ の設定

PVST+ プロトコルに 802.1 w 標準を適用した Rapid PVST+ が、デバイスのデフォルトの STP 設定です。

Rapid PVST+ は VLAN 単位でイネーブルになります。デバイスは VLAN ごとに個別の STP インスタンスを維持します（STP をディセーブルに設定した VLAN を除きます）。デフォルト VLAN、およびユーザが作成した各 VLAN では、Rapid PVST+ がデフォルトでイネーブルです。

ここでは、次の内容について説明します。

- Rapid PVST+ の設定に関する注意事項（p.5-21）
- Rapid PVST+ のイネーブル化（p.5-21）
- Rapid PVST+ の VLAN 単位でのディセーブル化またはイネーブル化（p.5-23）
- ルート ブリッジ ID の設定（p.5-24）
- セカンダリ ルート ブリッジの設定（p.5-26）
- VLAN の Rapid PVST+ ブリッジ プライオリティの設定（p.5-28）
- Rapid PVST+ ポート プライオリティの設定（p.5-29）
- Rapid PVST+ パスコスト方式およびポート コストの設定（p.5-30）
- VLAN の Rapid PVST+ hello タイムの設定（p.5-32）
- VLAN の Rapid PVST+ 転送遅延時間の設定（p.5-33）
- VLAN の Rapid PVST+ 最大エージング タイムの設定（p.5-34）
- リンク タイプの指定（p.5-35）
- プロトコルの再初期化（p.5-36）

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なることがあるので注意が必要です。

Rapid PVST+ の設定に関する注意事項

正しい VDC を開始していることを確認します（『*Cisco NX-OS Virtual Device Context Configuration Guide*』を参照）。

Rapid PVST+ のイネーブル化

Rapid PVST+ をディセーブル化した VLAN がある場合は、指定した VLAN で Rapid PVST+ を再度イネーブルにする必要があります。デバイスで MST がイネーブルな場合に、Rapid PVST+ を使用するには、そのデバイスで Rapid PVST+ をイネーブルにする必要があります。

「Rapid PVST+ の VLAN 単位でのディセーブル化またはイネーブル化」（p.5-23）を参照してください。

デフォルトの STP モードは Rapid PVST+ です。同じ VDC 上で MST と Rapid PVST+ を同時に実行することはできません。

ただし、特定の VDC で Rapid PVST+ を実行し、別の VDC で MST を実行することはできます。

（注） 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 インスタンスが前のモードで停止して新規モードで再開されるため、トラフィックが中断されます。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree mode rapid-pvst**
3. **exit**
4. **show running-config spanning-tree all**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree mode rapid-pvst** **例：** `switch(config)# spanning-tree mode rapid-pvst`	デバイスで Rapid PVST+ をイネーブルにします。デフォルトのスパニング ツリー モードは Rapid PVST+ です。 **（注）** 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 インスタンスが前のモードで停止して新規モードで開始されるため、トラフィックが中断されます。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show running-config spanning-tree all** **例：** `switch# show running-config spanning-tree all`	（任意）現在稼働している STP コンフィギュレーションの情報を表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、デバイス上で Rapid PVST+ をイネーブルにする例を示します。

```
switch# config t
switch(config)# spanning-tree mode rapid-pvst
switch(config)# exit
switch#
```

（注）　Rapid PVST+ はデフォルトでイネーブルに設定されているので、**show running** コマンドを入力して設定の結果を表示しても、Rapid PVST+ をイネーブルにするために入力したコマンドは表示されません。

Rapid PVST+ の VLAN 単位でのディセーブル化またはイネーブル化

Rapid PVST+ は VLAN 単位でイネーブルまたはディセーブルにできます。

（注）　デフォルト VLAN、およびユーザが作成したすべての VLAN では、Rapid PVST+ がデフォルトでイネーブルです。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **[no] spanning-tree vlan** *vlan-range*
3. **exit**
4. **show spanning-tree**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree vlan** *vlan-range* **例：** `switch(config)# spanning-treev lan 5`	Rapid PVST+（デフォルト STP）を VLAN 単位でイネーブルにします。*vlan-range* 値には、予約済みの VLAN 値を除く 2 ～ 4094 の値を指定できます。
	no spanning-tree vlan *vlan-range* **例：** `switch(config)# no spanning-tree vlan 5`	指定された VLAN で Rapid PVST+ をディセーブルにします。このコマンドについては、次の「注意」を参照してください。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show spanning-tree** **例：** `switch# show spanning-tree`	（任意）STP コンフィギュレーションを表示します。

	コマンド	目的
ステップ 5	**copy running-config startup-config** **例：** switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、VLAN 5 で STP をイネーブルにする例を示します。

```
switch# config t
switch(config)# spanning-tree vlan 5
switch(config)# exit
switch#
```

（注） VLAN 内のすべてのスイッチおよびブリッジでスパニング ツリーがディセーブルになっている場合以外は、VLAN 上でスパニング ツリーをディセーブルにしないでください。VLAN 内の一部のスイッチおよびブリッジでスパニング ツリーをディセーブルに設定し、同じ VLAN 内の残りのスイッチおよびブリッジではイネーブルのままにしておくことはできません。このような設定にすると、スパニング ツリーがイネーブルのスイッチおよびブリッジが、ネットワークの物理的トポロジに関して不完全な情報を得るので、予想外の結果が生じる可能性があります。

注意 物理的なループの存在しないトポロジであっても、スパニング ツリーをディセーブルにすることは推奨できません。スパニング ツリーは、設定およびケーブル接続の誤りに対するセーフガードの役割を果たします。VLAN 内に物理的なループが存在しないことを保証できる場合以外は、VLAN でスパニング ツリーをディセーブルにしないでください。

（注） STP はデフォルトでイネーブルに設定されているので、**show running** コマンドを入力して設定の結果を表示しても、STP をイネーブルにするために入力したコマンドは表示されません。

ルート ブリッジ ID の設定

NX-OS デバイスは、Rapid PVST+ が有効なアクティブ VLAN ごとに、STP インスタンスを個別に維持します。VLAN ごとに、最小のブリッジ ID を持つネットワーク装置が、その VLAN のルート ブリッジになります。

ルート ブリッジになるように VLAN インスタンスを設定するには、ブリッジ プライオリティをデフォルト値（32768）から非常に小さな値へと変更します。

spanning-tree vlan *vlan_ID* **primary root** コマンドを入力すると、デバイスは各 VLAN の現在のルート ブリッジのブリッジ プライオリティを確認します。24576 という値を設定するとデバイスが指定された VLAN のルートになる場合、デバイスはその VLAN のブリッジ プライオリティを 24576 に設定します。指定された VLAN のルート ブリッジのブリッジ プライオリティが 24576 より小さい場合、デバイスは指定された VLAN のブリッジ プライオリティを最小のブリッジ プライオリティより 4096 小さい値に設定します

（注） ルート　ブリッジになるために必要な値が　4096　より小さい場合は、**spanning-tree vlan** *vlan_ID* **primary root** コマンドは失敗します。ソフトウェアがブリッジ プライオリティをこれ以上小さくできない場合、デバイスは次のメッセージを戻します。

```
Error: Failed to set root bridge for VLAN 1
It may be possible to make the bridge root by setting the priority
for some (or all) of these instances to zero.
```

注意 STP の各インスタンスのルート ブリッジは、バックボーン スイッチまたはディストリビューション デバイスでなければなりません。アクセス デバイスを STP のプライマリ 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（すなわち、レイヤ 2 ネットワーク上の任意の 2 つの端末間における最大ブリッジ ホップ数）を指定するには、**diameter** キーワードを入力します。ネットワーク直径を指定すると、ソフトウェア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 タイムを自動的に選びます。その結果、STP の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-time** キーワードを入力すると、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。

（注） ルート　ブリッジとして設定されているデバイスを使用する場合、**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、および最大エージング タイムを手動で設定しないでください。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree vlan** *vlan-range* **root primary** [**diameter** *dia* [**hello-time** *hello-time*]]
3. **exit**
4. **show spanning-tree**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t switch(config)#	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	**spanning-tree vlan** *vlan-range* **root primary** [**diameter** *dia* [**hello-time** *hello-time*]] **例：** switch(config)# spanning-tree vlan 5 root primary diameter 4	NX-OS デバイスをプライマリ ルート ブリッジとして設定します。*vlan-range* 値には 2 ～ 4094 を指定できます（予約済みの VLAN 値を除く）。*dia* のデフォルトは 7 です。*hello-time* には 1 ～ 10 秒 を指定でき、デフォルト値は 2 秒です。
ステップ 3	**exit** **例：** switch(config)# exit switch#	コンフィギュレーション モードを終了します。
ステップ 4	**show spanning-tree** **例：** switch# show spanning-tree	（任意）STP コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** **例：** switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、デバイスを VLAN 5 のルート ブリッジとして設定し、ネットワーク直径を 4 に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree vlan 5 root primary diameter 4
switch(config)# exit
switch#
```

セカンダリ ルート ブリッジの設定

NX-OS デバイスをセカンダリ ルートとして設定すると、STP ブリッジ プライオリティはデフォルト値（32768）から変更されます。その結果、プライマリ ルート ブリッジに障害が発生した場合に（ネットワーク上の他のネットワーク装置がデフォルトのブリッジ プライオリティ 32768 を使用していると仮定して）、このデバイスが指定された VLAN のルート ブリッジになる可能性が高くなります。STP により、ブリッジ プライオリティは 28672 に設定されます。

レイヤ 2 ネットワークの直径（すなわち、レイヤ 2 ネットワーク上の任意の 2 つの端末間における最大ブリッジ ホップ数）を指定するには、**diameter** キーワードを入力します。ネットワークの直径を指定すると、NX-OS 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 タイムを自動的に選択します。その結果、STP の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-time** キーワードを入力すると、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。

この方法で、複数のデバイスに複数のバックアップ ルート ブリッジを設定できます。プライマリ ルート ブリッジを設定するときに使用したものと同じネットワーク直径および hello タイムを入力してください。

（注） ルート ブリッジとして設定されているデバイスを使用する場合、**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、および最大エージング タイムを手動で設定しないでください。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree vlan** *vlan-range* **root secondary** [**diameter** *dia* [**hello-time** *hello-time*]]
3. **exit**
4. **show spanning-tree vlan**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree vlan** *vlan-range* **root secondary** [**diameter** *dia* [**hello-time** *hello-time*]] **例：** `switch(config)# spanning-tree vlan 5 root secondary diameter 4`	NX-OS デバイスをセカンダリ ルート ブリッジとして設定します。*vlan-range* 値には 2 ～ 4094 を指定できます（予約済みの VLAN 値を除く）。*dia* のデフォルトは 7 です。*hello-time* には 1 ～ 10 秒 を指定でき、デフォルト値は 2 秒です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show spanning-tree vlan** *vlan_id* **例：** `switch# show spanning-tree vlan 5`	（任意）指定された VLAN の STP コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、デバイスを VLAN 5 のセカンダリ ルート ブリッジとして設定し、ネットワーク直径を 4 に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree vlan 5 root secondary diameter 4
switch(config)# exit
switch#
```

VLAN の Rapid PVST+ ブリッジ プライオリティの設定

VLAN の Rapid PVST+ ブリッジ プライオリティを設定できます。この方法で、ルート ブリッジを設定することもできます。

（注） この設定を使用する場合は、注意してください。ブリッジ　プライオリティを変更するには、プライマリ ルートおよびセカンダリ ルートを設定することを推奨します。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree vlan** *vlan-range* **priority** *value*
3. **exit**
4. **show spanning-tree vlan** *vlan_id*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree vlan** *vlan-range* **priority** *value* **例：** `switch(config)# spanning-tree vlan 5 priority 8192`	VLAN のブリッジ プライオリティを設定します。指定できる値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。これ以外の値は拒否されます。デフォルト値は 32768 です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show spanning-tree vlan** *vlan_id* **例：** `switch# show spanning-tree vlan 5`	（任意）指定された VLAN の STP コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、GigabitEthernet ポート 1/4 の VLAN 5 のプライオリティを 8192 に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree vlan 5 priority 8192
switch(config)# exit
switch#
```

Rapid PVST+ ポート プライオリティの設定

Rapid PVST+ に最初に選択させたい LAN ポートには低いプライオリティ値を、最後に選択させたい LAN ポートには最も高いプライオリティ値を割り当てることができます。すべての LAN ポートが同じプライオリティ値を使用している場合には、Rapid PVST+ は LAN ポート番号が最も小さい LAN ポートをフォワーディング ステートにして、残りの LAN ポートをブロックします。

デバイスは LAN ポートがアクセス ポートとして設定されている場合にはポート プライオリティ値を使用し、LAN ポートがトランク ポートとして設定されている場合には VLAN ポート プライオリティ値を使用します。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree** [**vlan** *vlan-list*] **port-priority** *priority*
4. **exit**
5. **show spanning-tree interface** {**ethernet** *slot/port* | **port channel** *channel-number*}
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定します。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	**spanning-tree** [**vlan** *vlan-list*] **port-priority** *priority* **例：** `switch(config-if)# spanning-tree port-priority 160`	LAN インターフェイスのポート プライオリティを設定します。*priority* 値には 0 ～ 224 を指定できます。値が小さいほど、プライオリティは高くなります。有効なプライオリティ値は、0、32、64、96、128、160、192、224 です。その他の値はすべて拒否されます。デフォルト値は 128 です。

	コマンド	目的
ステップ 4	**exit** **例：** switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 5	**show spanning-tree interface** {**ethernet** *slot/port* | **port channel** *channel-number*} **例：** switch# show spanning-tree interface ethernet 2/10	（任意）指定されたインターフェイスの STP コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** **例：** switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、イーサネット アクセス ポート 1/4 のポート プライオリティを 160 に設定する例を示します。

```
switch# config t
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree port-priority 160
switch(config-if)# exit
switch(config)#
```

Rapid PVST+ パスコスト方式およびポート コストの設定

アクセス ポートでは、ポートごとにポート コストを割り当てることができます。トランク ポートでは、VLAN ごとにポート コストを割り当てることができます。トランク上のすべての VLAN に同じポート コストを設定できます。

（注） Rapid PVST+ モードでは、ショートまたはロング パスコスト方式を使用できます。パスコスト方式の設定は、インターフェイス サブモードまたはコンフィギュレーション サブモードで行います。デフォルト パスコスト方式はショートです。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree pathcost method** {**long** | **short**}
3. **interface** *type slot/port*
4. **spanning-tree** [**vlan** *vlan-id*] **cost** [*value* | *auto*]
5. **exit**
6. **show spanning-tree pathcost method**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree pathcost method** {**long** | **short**} **例：** `switch(config)# spanning-tree pathcost method long`	Rapid PVST+ パスコスト計算に使用される方式を選択します。デフォルトは、ショート方式です。

ステップ 3	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)`
		設定するインターフェイスを指定します。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** [**vlan** *vlan-id*] **cost** [*value* | *auto*] **例：** `switch(config-if)# spanning-tree cost 1000`	LAN インターフェイスのポート コストを設定します。ポート コスト値には、パスコスト計算方式に応じて、次の値を指定できます。 • ショート — 1 ～ 65535 • ロング — 1 ～ 200000000 **(注)** このパラメータは、アクセス ポートではポート単位で、トランク ポートではVLAN 単位で設定できます。 デフォルトの **auto** では、パスコスト計算方式およびメディア速度に基づいてポート コストが設定されます。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 6	**show spanning-tree pathcost method** **例：** `switch# show spanning-tree pathcost method`	（任意）STP パスコスト方式を表示します。
ステップ 7	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、イーサネット アクセス ポート 1/4 のポート コストを 1000 に設定する例を示します。

```
switch# config t
switch (config)# spanning-tree pathcost method long
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree cost 1000
switch(config-if)# exit
switch(config)#
```

VLAN の Rapid PVST+ hello タイムの設定

VLAN の Rapid PVST+ hello タイムを設定できます。

（注） この設定を使用する場合は、注意してください。スパニング ツリーが中断されることがあります。hello タイムを変更するには、通常、プライマリ ルートおよびセカンダリ ルートを設定することを推奨します。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree vlan** *vlan-range* **hello-time** *value*
3. **exit**
4. **show spanning-tree vlan** *vlan_id*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree vlan** *vlan-range* **hello-time** *value* **例：** `switch(config)# spanning-tree vlan 5 hello-time 7`	VLAN の hello タイムを設定します。hello タイム値には 1 ～ 10 を指定できます。デフォルトは 2 秒です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show spanning-tree vlan** *vlan_id* **例：** `switch# show spanning-tree vlan 5`	（任意）STP コンフィギュレーションを VLAN 単位で表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、VLAN 5 の hello タイムを 7 秒に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree vlan 5 hello-time 7
switch(config)# exit
switch#
```

VLAN の Rapid PVST+ 転送遅延時間の設定

Rapid PVST+ を使用している場合は、転送遅延時間を VLAN 単位で設定できます。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree vlan** *vlan-range* **forward-time** *value*
3. **exit**
4. **show spanning-tree vlan** *vlan_id*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree vlan** *vlan-range* **forward-time** *value* **例：** `switch(config)# spanning-tree vlan 5 forward-time 21`	VLAN の転送遅延時間を設定します。転送遅延時間値には 4 ～ 30 秒を指定できます。デフォルトは 15 秒です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show spanning-tree vlan** *vlan_id* **例：** `switch# show spanning-tree vlan 5`	（任意）STP コンフィギュレーションを VLAN 単位で表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、VLAN 5 の転送遅延時間を 21 秒に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree vlan 5 forward-time 21
switch(config)# exit
switch#
```

VLAN の Rapid PVST+ 最大エージング タイムの設定

Rapid PVST+ を使用している場合は、最大エージング タイムを VLAN 単位で設定できます。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree vlan** *vlan-range* **max-age** *value*
3. **exit**
4. **show spanning-tree vlan** *vlan_id*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree vlan** *vlan-range* **max-age** *value* **例：** `switch(config)# spanning-tree vlan 5 max-age 36`	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 タイム値には 6 ～ 40 秒を指定できます。デフォルトは 20 秒です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show spanning-tree vlan** *vlan_id* **例：** `switch# show spanning-tree vlan 5`	（任意）STP コンフィギュレーションを VLAN 単位で表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、VLAN 5 の最大エージング タイムを 36 秒に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree vlan 5 max-age 36
switch(config)# exit
switch#
```

リンク タイプの指定

高速接続（802.1w 標準）は、ポイントツーポイント リンク上にのみ確立されます。デフォルトでは、リンク タイプが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。つまり、全二重ポートはポイントツーポイント接続とみなされ、半二重ポートは共有接続とみなされます。

リモート デバイスの単一ポートに、ポイントツーポイントで物理的に接続されている半二重リンクがある場合、リンク タイプのデフォルト設定を上書きして高速移行をイネーブルにできます。

リンクを共有に設定すると、STP は 802.1D にフォール バックします。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **interface** *type slot*/*port*
3. **spanning-tree link-type** {*auto* | *point-to-point* | *shared*}
4. **exit**
5. **show spanning-tree**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定します。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	**spanning-tree link-type** {*auto* | *point-to-point* | *shared*} **例：** `switch(config-if)# spanning-tree link-type point-to-point`	リンク タイプをポイントツーポイント リンクまたは共有リンクに設定します。デフォルト値は、次のようにデバイス接続から読み取られます。半二重リンクは共有、全二重リンクはポイントツーポイントです。リンク タイプが共有の場合、STP は 802.1D にフォール バックします。デフォルトの auto では、インターフェイスのデュプレックス設定に基づいてリンク タイプが設定されます。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

	コマンド	目的
ステップ 5	**show spanning-tree** **例：** switch# show spanning-tree	（任意）STP コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** **例：** switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、リンク タイプをポイントツーポイント リンクに設定する例を示します。

```
switch# config t
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree link-type point-to-point
switch(config-if)# exit
switch(config)#
```

プロトコルの再初期化

Rapid PVST+ が稼働するブリッジにレガシー ブリッジが接続されている場合は、1 つのポートから 802.1D BPDU を送信できます。ただし、STP プロトコルを移行しても、レガシー デバイスが代表スイッチでないかぎり、レガシー デバイスがリンクから削除されたかどうかを判別することはできません。デバイス全体で、または指定されたインターフェイスで、プロトコル ネゴシエーションを再初期化する（隣接デバイスと強制的に再ネゴシエーションを行う）ことができます。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **clear spanning-tree detected-protocols** [**interface** {**ethernet** *slot/port* | **port channel** *channel-number*}]

手順の詳細

	コマンド	目的
ステップ 1	**clear spanning-tree detected-protocol** [**interface** {**ethernet** *slot/port* | **port channel** *channel-number*}] **例：** switch# clear spanning-tree detected-protocol	デバイス上のすべてのインターフェイス、または指定されたインターフェイスで、Rapid PVST+ を再初期化します。

次に、スロット 2 のイーサネット インターフェイス ポート 8 で、Rapid PVST+ を再初期化する例を示します。

```
switch# clear spanning-tree detected-protocol interface ethernet 2/8
switch#
```

Rapid PVST+ コンフィギュレーションの確認

Rapid PVST+ コンフィギュレーション情報を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
show running-config spanning-tree [all]	STP 情報を表示します。
show spanning-tree summary	STP の概要を表示します。
show spanning-tree detail	STP の詳細を表示します。
show spanning-tree {**vlan** *vlan-id* | **interface** {[**ethernet** *slot/port*] | [**port-channel** *channel-number*]}} [**detail**]	VLAN またはインターフェイス単位の STP 情報を表示します。
show spanning-tree vlan *vlan-id* **bridge**	STP ブリッジの情報を表示します。

これらのコマンドの出力フィールドの詳細については、『*Cisco NX-OS Layer 2 Switching Command Reference*』を参照してください。

Rapid PVST+ 統計情報の表示およびクリア

Rapid PVST+ コンフィギュレーション情報を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
clear spanning-tree counters [**interface** *type/slot* | **vlan** *vlan-id*]	STP のカウンタをクリアします。
show spanning-tree {**vlan** ***vlan-id*** | **interface** {[**ethernet** *slot/port*] | [**port-channel** *channel-number*]}} **detail**	送受信された BPDU などの STP 情報を、インターフェイスまたは VLAN 別に表示します。

Rapid PVST+ の設定例

次に、Rapid PVST+ の設定例を示します。

```
switch# configure terminal
switch(config)# spanning-tree port type edge bpduguard default
switch(config)# spanning-tree port type edge bpdufilter default
switch(config)# spanning-tree port type network default
switch(config)# spanning-tree vlan 1-10 priority 24576
switch(config)# spanning-tree vlan 1-10 hello-time 1
switch(config)# spanning-tree vlan 1-10 forward-time 9
switch(config)# spanning-tree vlan 1-10 max-age 13

switch(config)# interface Ethernet 3/1 switchport
switch(config-if)# spanning-tree port type edge
switch(config-if)# exit

switch(config)# interface Ethernet 3/2
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# spanning-tree guard root
switch(config-if)# exit
switch(config)#
```

STP ポート タイプ、BPDU ガード、ルート ガード、および BPDU フィルタ機能の詳細については、第 7 章「STP 拡張機能の設定」を参照してください。

デフォルト設定

表 5-5 に、Rapid PVST+ パラメータのデフォルト設定を示します。

表 5-5　デフォルト Rapid PVST+ パラメータ

パラメータ	デフォルト
スパニング ツリー	すべての VLAN でイネーブル
スパニング ツリー モード	Rapid PVST+ **注意**　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 インスタンスが前のモードで停止して新規モードで開始されるため、トラフィックが中断されます。
VLAN	VLAN 1 に割り当てられたすべてのポート
拡張システム ID	常にイネーブル
MAC アドレス リダクション	常にイネーブル
ブリッジ ID プライオリティ	32769（デフォルト VLAN 1 のデフォルト ブリッジ プライオリティに拡張システム ID を加えた値）
ポート ステート	ブロッキング（コンバージェンスが発生すると、即座に変更される）
ポート ロール	指定（コンバージェンスが発生すると、変更される）
ポート /VLAN プライオリティ	128
パスコスト計算方式	ショート
ポート /VLAN コスト	auto デフォルトのポート コストは、次のように、メディア速度およびパスコスト計算方式から判別されます。 • 10 Mbps： — ショート：100 — ロング：2,000,000 • 100 Mbps： — ショート：19 — ロング：200,000 • 1 ギガビット イーサネット： — ショート：4 — ロング：20,000 • 10 ギガビット イーサネット： — ショート：2 — ロング：2,000
hello タイム	2 秒
転送遅延時間	15 秒

表 5-5　デフォルト Rapid PVST+ パラメータ（続き）

パラメータ	デフォルト
最大エージング タイム	20 秒
リンク タイプ	auto デフォルト リンク タイプは、次のようにデュプレックスから判別されます。 • 全二重：ポイントツーポイント リンク • 半二重：共有リンク

追加情報

Rapid PVST+ の実装に関する追加情報は、次のセクションを参照してください。

- 関連資料（p.5-40）
- 標準規格（p.5-40）
- MIB（p.5-40）

関連資料

関連トピック	マニュアル名
VLAN	第 3 章「VLAN の設定」
MST	第 6 章「MST の設定」
STP 拡張機能	第 7 章「STP 拡張機能の設定」
コマンド リファレンス	『*Cisco NX-OS Layer 2 Switching Command Reference*』
DCNM レイヤ 2 スイッチングの設定	『*Cisco DCNM Layer 2 Switching Configuration Guide*』
レイヤ 2 インターフェイス	『*Cisco NX-OS Interfaces Configuration Guide*』
NX-OS の基本情報	『*Cisco NX-OS Fundamentals Configuration Guide*』
ハイ アベイラビリティ	『*Cisco NX-OS High Availability and Redundancy Guide*』
システム管理	『*Cisco NX-OS System Management Configuration Guide*』
VDC	『*Cisco NX-OS Virtual Device Context Configuration Guide*』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco NX-OS Release Notes*』 Release 4.0

標準規格

標準規格	タイトル
IEEE 802.1Q-2006（従来の名称は IEEE 802.1s）、IEEE 802.1D-2004（従来の名称は IEEE 802.1w）、IEEE 802.1D、IEEE 802.1t	—

MIB

MIB	MIB リンク
• CISCO-STP-EXTENSION-MIB • BRIDGE-MIB	次の URL から、MIB の検索およびダウンロードができます。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

CHAPTER 6

MST の設定

この章では、NX-OS デバイスに Multiple Spanning Tree（MST）を設定する方法について説明します。

（注） レイヤ 2 インターフェイスの作成方法については、『*Cisco NX-OS Interface Configuration Guide*』を参照してください。

IEEE 802.1s 標準の MST を使用すると、スパニング ツリー インスタンスに複数の VLAN（仮想 LAN）を割り当てることができます。MST はデフォルトのスパニング ツリー モードではありません。Rapid per VLAN Spanning Tree（Rapid PVST+）がデフォルト モードです。名前、リビジョン番号、および VLAN/ インスタンス間マッピングが同じ MST Instance（MSTI; MST インスタンス）が組み合わされて、MST 領域を形成します。MST 領域は、領域外のスパニング ツリー構成からは、単一ブリッジとして認識されます。MST が隣接デバイスから IEEE 802.1D Spanning Tree Protocol（STP; スパニング ツリー プロトコル）メッセージを受信すると、該当するインターフェイスとの境界が形成されます。

（注） スパニング ツリーは、IEEE 802.1w および IEEE 802.1s を表す場合に使用されます。IEEE 802.1D STP に関する説明の場合は、具体的に 802.1D と表記されます。

ここでは、次の内容を説明します。

- MST について（p.6-2）
- MST のライセンス要件（p.6-12）
- MST の前提条件（p.6-12）
- 注意事項および制約事項（p.6-13）
- MST の設定（p.6-15）
- MST コンフィギュレーションの確認（p.6-40）
- MST 統計情報の表示およびクリア（p.6-40）
- MST の設定例（p.6-41）
- デフォルト設定（p.6-43）
- 追加情報（p.6-44）

（注） STP および Rapid PVST+ の詳細については、第 5 章「Rapid PVST+ の設定」、STP 拡張機能の詳細については、第 7 章「STP 拡張機能の設定」を参照してください。

MST について

（注）　レイヤ 2 インターフェイスの作成方法については、『*Cisco NX-OS Interface Configuration Guide*』を参照してください。

IEEE 802.1s 標準の MST を使用すると、スパニング ツリー インスタンスに複数の VLAN を割り当てることができます。MST はデフォルトのスパニング ツリー モードではありません。Rapid PVST+ がデフォルト モードです。名前、リビジョン番号、および VLAN/ インスタンス間マッピングが同じ MSTI が組み合わされて、MST 領域を形成します。MST 領域は、領域外のスパニング ツリー構成からは、単一ブリッジとして認識されます。MST が隣接デバイスから IEEE 802.1D Spanning Tree Protocol（STP; スパニング ツリー プロトコル）メッセージを受信すると、該当するインターフェイスとの境界が形成されます。

（注）　スパニング ツリーは、IEEE 802.1w および IEEE 802.1s を表す場合に使用されます。このマニュアルで IEEE 802.1D STP に関して説明する場合は、具体的に 802.1D と表記されます。

ここでは、次の内容について説明します。

- MST の概要（p.6-2）
- MST 領域（p.6-3）
- MST BPDU（p.6-4）
- MST コンフィギュレーション情報（p.6-4）
- IST、CIST、および CST（p.6-5）
- ホップ カウント（p.6-8）
- 境界ポート（p.6-8）
- 単一方向リンク障害の検出（p.6-9）
- ポート コストおよびポート プライオリティ（p.6-10）
- IEEE 802.1D との相互運用性（p.6-10）
- ハイ アベイラビリティ（p.6-11）
- バーチャライゼーションのサポート（p.6-11）

MST の概要

（注）　MST をイネーブルにする必要があります。デフォルトのスパニング ツリー モードは、Rapid PVST+ です。

MST は、複数の VLAN をスパニング ツリー インスタンスにマッピングします。各インスタンスには他のスパニング ツリー インスタンスとは別のスパニング ツリー トポロジがあります。このアーキテクチャにより、データ トラフィック用に複数の転送パスが提供され、ロード バランスが有効化され、多くの VLAN をサポートするために必要な STP インスタンスの数を軽減します。MST では、1 つのインスタンス（転送パス）で障害が発生しても他のインスタンス（転送パス）に影響しないため、ネットワークの耐障害性が向上します。

各 MSTI で IEEE 802.1w 標準が使用されるため、明示的なハンドシェイクを通して高速コンバージェンスを実現することができます。これによって、IEEE 802.1D 転送遅延がなくなり、ルート ブリッジ ポートと指定ポートが迅速にフォワーディング ステートへ移行します（明示的なハンドシェイク合意については、第 5 章「Rapid PVST+ の設定」を参照）。

デバイス上では、常に MAC アドレス リダクションがイネーブルです（MAC アドレス リダクションの詳細については、第 5 章「Rapid PVST+ の設定」を参照）。この機能をディセーブルにすることはできません。

MST は、スパニング ツリー動作を改善し、以下の STP バージョンと後方互換性を維持しています。

- 元の 802.1D スパニング ツリー
- Rapid PVST+

（注）
- IEEE 802.1w は Rapid Spanning Tree Protocol（RSTP）を定義し、IEEE 802.1D に組み込まれています。
- IEEE 802.1s は MST を定義し、IEEE 802.1Q に組み込まれています。

MST 領域

MSTI にデバイスを参加させるには、常に同じ MST コンフィギュレーション情報を使用してスイッチを設定する必要があります（「MST コンフィギュレーション情報」[p.6-4] を参照）。

同じ MST コンフィギュレーションを持つ、相互接続されたデバイスの集合を MST 領域といいます。MST 領域は、同じ MST コンフィギュレーションを持つ、リンクされた MST ブリッジのグループです。

MST コンフィギュレーションは、各デバイスが属する MST 領域を制御します。このコンフィギュレーションには、領域名、リビジョン番号、VLAN/MSTI 割り当てマッピングが含まれます。

領域には、同じ MST コンフィギュレーションを持つメンバーを 1 つ以上格納できます。各メンバーには、802.1w Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）を処理する機能が必要です。ネットワーク内の MST 領域数に制限はありません。

各デバイスは、単一の MST 領域内で、インスタンス 0 を含む最大 65 個の MSTI をサポートできます。インスタンスは 1 ～ 4094 の任意の番号で識別されます。インスタンス 0 は、Internal Spanning Tree（IST; 内部スパニング ツリー）という特殊なインスタンス専用です。1 つの VLAN を同時に 2 つの MSTI に割り当てることはできません。（IST の詳細については、「IST、CIST、および CST」[p.6-5] を参照）。

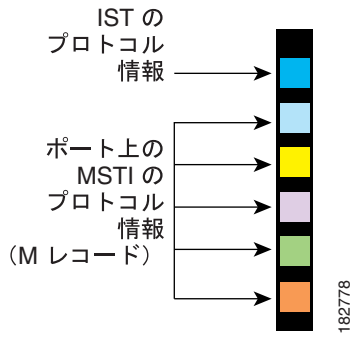
MST 領域は、隣接 MST 領域やその他の Rapid PVST+ 領域、および 802.1D STP からは、単一ブリッジとして認識されます。

（注）　ネットワークを多数の領域に分割することは推奨できません。

MST BPDU

各デバイスで使用できる MST BPDU は、インターフェイスごとに 1 つのみです。この BPDU が、デバイス上の各 MSTI の M レコードを伝達します（図 6-1 を参照）。MST 領域の BPDU を送信するのは、IST のみです。すべての M レコードは、IST から伝送される、この特定の BPDU にカプセル化されます（IST の詳細については、「IST、CIST、および CST の概要」[p.6-5] を参照）。MST BPDU はすべてのインスタンスの情報を伝送するため、MST をサポートするために処理しなければならない BPDU の数は、Rapid PVST+ と比べて大幅に削減されます。

図 6-1　MSTI の M レコードを含む MST BPDU



MST コンフィギュレーション情報

単一の MST 領域内にあるすべてのデバイスで MST コンフィギュレーションを同一にする必要がある場合は、ユーザ側で設定します。

設定できる MST コンフィギュレーションのパラメータは、次の 3 つです。

- 名前 — MST 領域を識別する 32 文字のストリング（ヌル パディング、ヌルで終了）
- リビジョン番号 — 現在の MST コンフィギュレーションのリビジョンを識別する、符号なし 16 ビット数

（注） MST コンフィギュレーションの一部としてリビジョン番号が必要な場合は、リビジョン番号を設定する必要があります。リビジョン番号は、MST コンフィギュレーションをコミットするたびに、自動的に増えるわけではありません。

- VLAN/MSTI マッピング — 各 Virtual Device Context（VDC）でサポートされる 4094 個の各 VLAN を指定インスタンスに対応付ける、4094 個のエレメントを含むテーブル。先頭エレメント（0）および最終エレメント（4095）は 0 に設定されています。エレメント番号 X の値は、VLAN X のマッピング先インスタンスを表します。

（注） VLAN/MSTI マッピングを変更すると、MST が再コンバージェンスされます。

MST BPDU には、上記の 3 つのコンフィギュレーション パラメータが含まれています。MST ブリッジが自身の領域に MST BPDU を受け入れるのは、これらの 3 つのコンフィギュレーション パラメータが完全に一致する場合のみです。特定のコンフィギュレーション属性が異なる場合、MST ブリッジはこの BPDU が別の MST 領域から伝送されたとみなします。

IST、CIST、および CST

ここでは、IST、Common and Internal Spanning-Tree（CIST）、および Common Spanning Tree（CST）について説明します。

- IST、CIST、および CST の概要（p.6-5）
- MST 領域内のスパニング ツリー動作（p.6-6）
- MST 領域間のスパニング ツリー動作（p.6-6）
- MST 用語（p.6-7）

IST、CIST、および CST の概要

すべての STP インスタンスが独立している Rapid PVST+（詳細については第 5 章「Rapid PVST+ の設定」を参照）と異なり、MST は IST、CIST、および CST スパニング ツリーを次のように確立して、維持します。

- IST は 1 つの MST 領域で稼働するスパニング ツリーです。

  MST は各 MST 領域内でその他のスパニング ツリーを確立して、維持します。これらのスパニング ツリーは、MSTI といいます。

  インスタンス 0 は領域の特殊インスタンスで、IST と呼ばれています。IST は必ずすべてのポート上にあります。IST（インスタンス 0）は削除できません。デフォルトでは、すべての VLAN が IST に割り当てられています。他のすべての MSTI には 1 ～ 4094 の番号が割り当てられます。

  IST は BPDU を送受信する唯一の STP インスタンスです。他のすべての MSTI 情報は、MST レコード（M レコード）内に含まれ、MST BPDU 内でカプセル化されています。

  同じ領域内にあるすべての MSTI は同じプロトコル タイマーを共有しますが、各 MSTI にはルート ブリッジ ID、ルート パス コストなどの独自のトポロジ パラメータがあります。

  MSTI は領域に対してローカルです。たとえば、領域 A と B が相互接続されている場合でも、領域 A の MSTI 9 は 領域 B の MSTI 9 から独立しています。領域の境界をまたいで使用されるのは、CST 情報のみです。
- CST は MST 領域と、ネットワーク上で稼働できる 802.1D および 802.1w STP の任意のインスタンスを相互接続します。CST はブリッジ型ネットワークの STP インスタンスの 1 つです。すべての MST 領域と、802.1w および 802.1D インスタンスが含まれます。
- CIST は、各 MST 領域にある IST の集合です。CIST は、MST 領域の内部では IST と同じであり、MST 領域の外部では CST と同じです。

MST 領域内で計算されたスパニング ツリーは、スイッチド ドメイン全体を含む CST のサブツリーとみなされます。CIST は 802.1w、802.1s、802.1D 標準をサポートするスイッチ間で動作するスパニング ツリー アルゴリズムによって形成されます。MST 領域内にある CIST は領域外にある CST と同じです。

詳細については、「MST 領域内のスパニング ツリー動作」（p.6-6）および「MST 領域間のスパニング ツリー動作」（p.6-6）を参照してください。

MST 領域内のスパニング ツリー動作

IST は領域内のすべての MST のスイッチを接続します。IST が収束すると、IST のルートが CIST 領域のルートになります（図 6-2 を参照）。CIST リージョナル ルートは、ネットワーク内に領域が 1 つしかない場合は CIST ルートでもあります。CIST ルートが領域外にある場合、領域の境界にある MST デバイスの 1 つが CIST リージョナル ルートとして選択されます。

MST のデバイスは初期化時に、自身を CIST ルートおよび CIST リージョナル ルートとして識別する BPDU を送信します。その際、CIST ルートへのパス コストと CIST リージョナル ルートへのパス コストは 0 に設定されています。また、デバイスは、すべての MSTI を初期化し、自身がこれらすべてのルートであることを示します。デバイスが現在ポートに格納されているものよりも上位の MSTI ルート情報（小さいスイッチ ID、低いパス コストなど）を受信すると、CIST リージョナル ルートとしての主張を撤回します。

初期化中に、MST 領域内に独自の CIST リージョナル ルートを持つ多くのサブ領域が形成される場合があります。スイッチは、同じ領域内のネイバーから上位の IST 情報を受信すると、古いサブ領域を脱退して、真の CIST リージョナル ルートが含まれている新しいサブ領域に加入します。このようにして、真の CIST リージョナル ルートが含まれているサブ領域以外のサブ領域はすべて縮小します。

MST 領域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。領域内にある任意の 2 つのスイッチは、共通 CIST リージョナル ルートに収束する場合、MSTI に対するポート ロールのみを同期します。

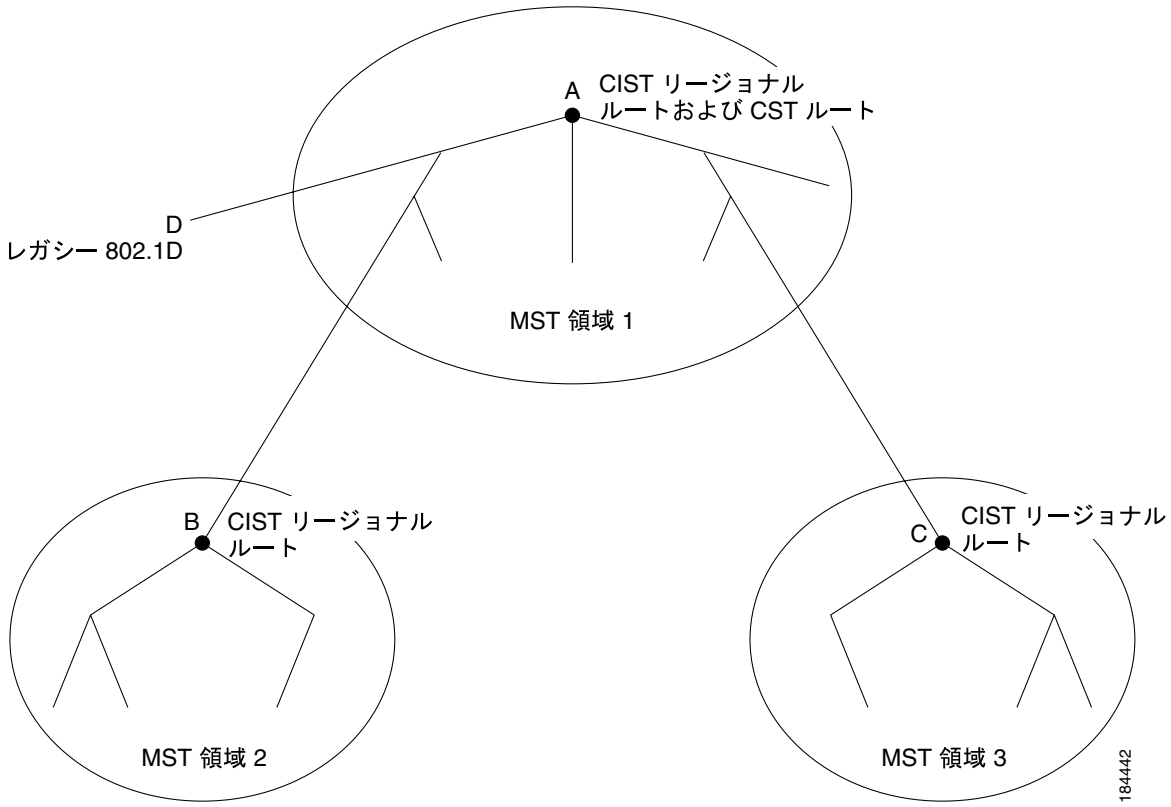
MST 領域間のスパニング ツリー動作

ネットワーク内に複数の領域、または 802.1 w や 802.1D STP インスタンスがある場合、MST はネットワーク内のすべての MST 領域、およびすべての 802.1w と 802.1D STP スイッチを含む CST を確立して、維持します。MSTI は領域の境界で IST と結合して CST になります。

IST は領域内のすべての MST のスイッチを接続し、スイッチ ドメイン全体を含んだ CIST 内のサブツリーとして認識されます。サブツリーのルートは CIST リージョナル ルートです。MST 領域は、隣接する STP のスイッチおよび MST 領域からは仮想デバイスとして認識されます。

図 6-2 に、3 つの MST 領域および 802.1D デバイス（D）があるネットワークを示します。領域 1 の CIST リージョナル ルート（A）は CIST ルートでもあります。領域 2 の CIST リージョナル ルート（B）および領域 3 の CIST リージョナル ルート（C）は、CIST 内の各サブツリーのルートです。

図 6-2　MST 領域、CIST リージョナル ルート、および CST ルート



BPDU を送受信するのは CST インスタンスのみです。MSTI は自身のスパニング ツリー情報を BPDU に（M レコードとして）追加し、同じ MST 領域内の隣接スイッチと相互作用して、最終的なスパニング ツリー トポロジを計算します。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 インスタンスにのみ設定されますが、すべての MSTI に影響します。スパニング ツリー トポロジに関連するパラメータ（スイッチ プライオリティ、ポート VLAN コスト、ポート VLAN プライオリティなど）は CST インスタンスと MSTI の両方で設定できます。

MST デバイスは、バージョン 3 BPDU を使用します。802.1D STP にフォール バックした MST デバイスは、802.1D 専用デバイスと通信する場合、802.1D BPDU のみを使用します。MST デバイスは、MST デバイスと通信する場合、MST BPDU を使用します。

MST 用語

MST の命名規則には、一部の内部パラメータまたはリージョナル パラメータの識別情報が含まれています。これらのパラメータは、ネットワーク全体で使用されている外部パラメータとは違い、MST 領域のみで使用されます。CIST はネットワーク全体にまたがる唯一のスパニング ツリー インスタンスなので、CIST パラメータでは、内部修飾子や領域の修飾子ではなく、外部修飾子が必要です。MST 用語を次に示します。

- CIST ルートは CIST のルート ブリッジで、ネットワーク全体にまたがる一意のインスタンスです。
- CIST 外部ルート パス コストは、CIST ルートのコストです。このコストは、MST 領域内では変化しません。MST 領域は CIST に対して単一のデバイスのように見えます。CIST 外部ルート パス コストは、これらの仮想スイッチとどの領域にも属さないスイッチとの間で計算されたルート パス コストです。

- CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。それ以外の場合は、領域内で CIST ルートに最も近いデバイスが CIST リージョナル ルートです。CIST リージョナル ルートは IST のルート ブリッジとして動作します。
- CIST 内部ルート パス コストは、領域内の CIST リージョナル ルートのコストです。このコストは、IST（インスタンス 0）にのみ関連します。

ホップ カウント

MST 領域内の STP トポロジを計算する場合、MST はコンフィギュレーション BPDU のメッセージ有効期間および最大エージング タイムの情報を使用しません。その代わりに、ルートへのパス コストおよび IP Time to Live（TTL; 存続可能時間）メカニズムに似たホップカウント メカニズムを使用します。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用することで、領域内の最大ホップを設定して、それをその領域内にある IST およびすべての MSTI に適用できます。

ホップ カウントは、メッセージ有効期間情報と同じ結果（再設定の開始）となります。インスタンスのルート ブリッジは、常にコスト 0 でホップ カウントが最大値に設定されている BPDU（または M レコード）を送信します。デバイスがこの BPDU を受信すると、受信 BPDU の残存ホップ カウントから 1 だけ差し引いた値を残存ホップ カウントとする BPDU を生成し、これを伝播します。ホップ カウントが 0 になると、デバイスは BPDU を廃棄して、ポートに維持された情報を期限切れにします。

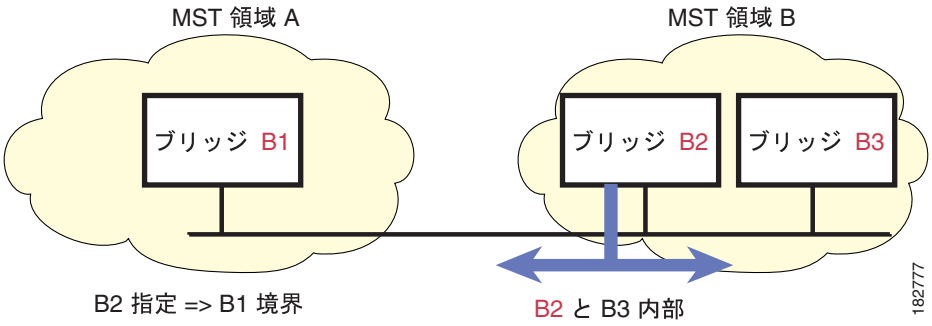
BPDU の 802,1w 部分に格納されているメッセージ有効期間および最大エージング タイムの情報は、領域全体で同じです（IST の場合のみ）。同じ値が、境界にある領域の指定ポートによって伝播されます。

最大エージング タイムは、デバイスがスパニング ツリー設定メッセージを受信せずに再設定を試行するまで待機する秒数です。

境界ポート

境界ポートは LAN に接続されたポートです。この LAN の代表ブリッジは、MST コンフィギュレーションが異なる（したがって、MST 領域が異なる）ブリッジ、または Rapid PVST+ や 802.1D STP ブリッジです。指定ポートは、STP ブリッジを検出した場合、またはコンフィギュレーションの異なる MST ブリッジや Rapid PVST+ ブリッジから合意メッセージを受信した場合に、自身が境界上にあることを認識します。この定義により、領域の内側にある 2 つのポートが異なる領域に属するポートとセグメントを共有することができるので、内部メッセージと外部メッセージの両方をポートで受信できる可能性があります（図 6-3 を参照）。

図 6-3　MST 境界ポート



境界では、MST ポートの役割は重要でありません。、MST ポート ステートは強制的に IST ポート ステートと同じに設定されます。ポートに境界フラグが設定されている場合、MST ポートのロール選択プロセスによって、境界にポート ロールが割り当てられ、IST ポートと同じステートが割り当てられます。境界の IST ポートは、バックアップ ポート ロール以外のあらゆるポート ロールを担うことができます（境界ポートのステートおよびロード バランシングに関する重要な情報については、「注意事項および制約事項」[p.6-13] を参照）。

単一方向リンク障害の検出

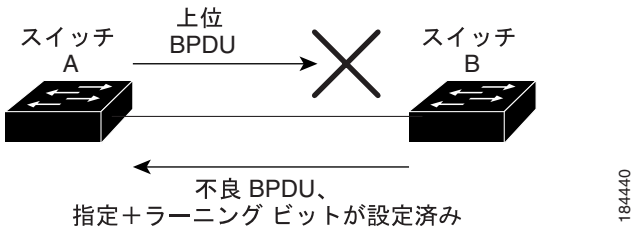
現在、IEEE MST 標準に単一方向リンク障害の検出機能はありませんが、標準に準拠した実装には組み込まれています。この機能のベースとなるのは、異議メカニズムです。ソフトウェアは、受信した BPDU のポート ロールとステートの一貫性をチェックして、ブリッジング ループが発生する可能性のある単一方向リンク障害を検出します。

（注） Unidirectional Link Detection（UDLD; 単一方向リンク検出）の詳細については、『*Cisco NX-OS Fundamentals Configuration Guide*』を参照してください。

指定ポートが矛盾を検出するとロールは維持されますが、状態は廃棄ステートに戻ります。これは、接続に矛盾が生じた場合、ブリッジング ループを開始するよりも接続を中断する方が好ましいためです。

図 6-4 に、ブリッジング ループの一般的な原因となる単一方向リンク障害を示します。スイッチ A はルート ブリッジで、その BPDU はデバイス B へのリンクで損失されます。Rapid PVST+（802.1w）および MST BPDU には、送信ポートのロールとステートが含まれます。デバイス A はこの情報を使用して、デバイス B が A の送信した上位 BPDU に反応せず、デバイス B がルート ポートではなく、指定ポートであることを検出できます。その結果、デバイス A は B のポートをブロックする（またはブロックし続ける）ので、ブリッジング ループが回避されます。

図 6-4　単一方向リンク障害の検出



（注） ブリッジ保証機能の詳細については、第 7 章「STP 拡張機能の設定」も参照してください。

ポート コストおよびポート プライオリティ

スパニング ツリーはポート コストを使用して、指定ポートを決定します。値が低いほど、ポート コストは小さくなります。スパニング ツリーはコストが最小のパスを選択します。デフォルト ポート コストは、次のように、インターフェイスの帯域幅から取得されます。

- 10 Mbps — 2,000,000
- 100 Mbps — 200,000
- 1 ギガビット イーサネット — 20,000
- 10 ギガビット イーサネット — 2,000

ポート コストを設定すると、選択されるポートが影響を受けます。

（注） MST では常にロング パスコスト計算方式が使用されるため、有効値は 1 ～ 200,000,000 です。

コストが同じポートを差別化するために、ポート プライオリティが使用されます。値が小さいほど、プライオリティは高くなります。デフォルトのポート プライオリティは 128 です。プライオリティに設定できる値は、0 ～ 224 です（32 単位で増分）。

IEEE 802.1D との相互運用性

MST が稼働しているデバイスは、802.1D STP スイッチと相互運用できるようにする内蔵プロトコル移行機能をサポートします。このデバイスが 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、そのポートからは 802.1D BPDU のみを送信します。また、MST デバイスは、802.1D BPDU、異なる領域と関連する MST BPDU（バージョン 3）、または 802.1w BPDU（バージョン 2）を受信するときに、ポートが領域の境界にあることを検出できます。

ただし、デバイスが 802.1D BPDU を受信しなくなっても、自動的に MST モードに戻ることはありません。これは、802.1D デバイスが指定デバイスでない場合、802.1D デバイスがリンクから削除されているかどうかを検出できないためです。また、デバイスは、このデバイスに接続されているデバイスがその領域に加入した場合、引き続きポートに境界ロールを割り当てる可能性もあります。

プロトコル移行プロセスを再起動する（隣接スイッチと強制的に再ネゴシエーションする）には、**clear spanning-tree detected-protocols** コマンドを入力します。

リンク上のすべての Rapid PVST+ スイッチ（およびすべての 8021.D STP スイッチ）は、802.1w BPDU の場合と同様に、MST BPDU を処理できます。MST スイッチは、境界ポートでバージョン 0 コンフィギュレーションと Topology Change Notification（TCN; トポロジ変更通知）BPDU、またはバージョン 3 MST BPDU のいずれかを送信できます。境界ポートは、指定デバイスが単一のスパニング ツリー デバイスであるか、または異なる MST コンフィギュレーションを持つデバイスである LAN に接続されます。

（注） MST は、MST ポートでシスコの先行標準 MSTP を受信した場合、必ず先行標準 MSTP と相互運用されます。明示的な設定は不要です。

ハイ アベイラビリティ

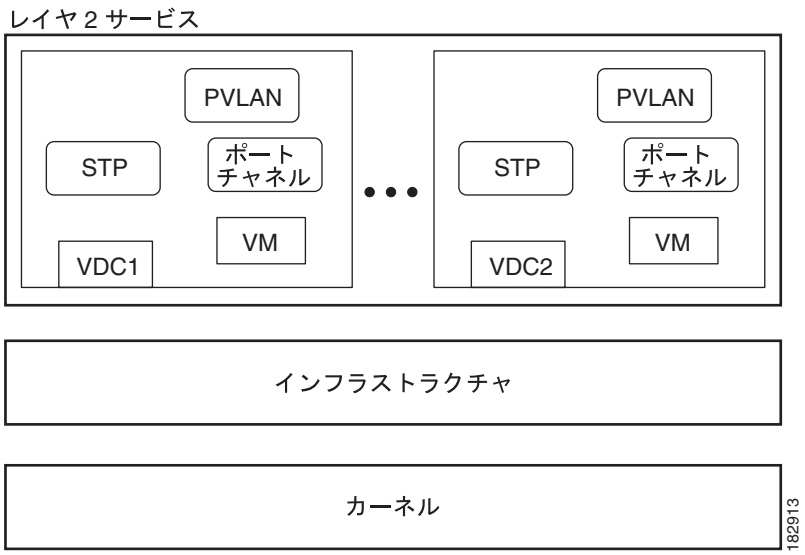
ソフトウェアは MST に対してハイ アベイラビリティをサポートしています。ただし、MST を再起動した場合、統計情報およびタイマーは復元されません。タイマーは再起動し、統計情報は 0 から開始します。

（注） ハイ アベイラビリティ機能の詳細については、『*Cisco NX-OS High Availability and Redundancy Configuration Guide*』を参照してください。

バーチャライゼーションのサポート

システムでは VDC がサポートされ、VDC ごとに個別の STP が実行されます（図 6-5 を参照）。

図 6-5　VDC ごとに個別の STP



特定の VDC で Rapid PVST+ を実行し、別の VDC で MST を実行することができます。VDC ごとに独自の MST があります。作業している VDC が正しいことを確認してください。

たとえば、VDC1 で MST、VDC2 で Rapid PVST+、VDC 3 で MST を実行することができます。

（注） 異なる VDC 内の MST は区別されます。つまり、VDC ごとに MST 領域を設定する必要があります。

（注） VDC およびリソース割り当ての詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide*』を参照してください。

MST のライセンス要件

次の表に、この機能に関するライセンス要件を示します。

製品	ライセンス要件
NX-OS	MST のライセンスは不要です。ライセンス パッケージに含まれていない機能は Cisco NX-OS システム イメージにバンドルされ、無料で提供されます。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

ただし、VDC を使用する場合は、Advanced Services ライセンスが必要です。

MST の前提条件

MST には次の前提条件があります。

- デバイスにログオンする必要があります。
- DCNM を使用して STP パラメータを設定する前に、デバイスのコマンドラインに **logging-level spanning-tree 6** NX-OS グローバル コマンドを入力して、ロギング レベルを設定する必要があります。ロギング レベルの詳細については、『*Cisco NX-OS System Management Configuration Guide*』を参照してください。
- 必要に応じて、Advanced Services ライセンスをインストールし、目的の VDC を開始します。
- デフォルト以外の VDC で作業する場合は、目的の VDC を作成しておく必要があります。

注意事項および制約事項

（注）　VLAN/MSTI マッピングを変更すると、MST が再コンバージェンスされます。

MST を使用する場合は、次の注意事項に従ってください。

- MST をイネーブルにする必要があります。デフォルトのスパニング ツリー モードは、Rapid PVST+ です。
- 1 つの VLAN を同時に 2 つの MSTI に割り当てることはできません。
- 1 つのデバイスに最大 65 個の MSTI を設定できます。
- VLAN およびポートの最大数は 75,000 です。
- デフォルトでは、すべての VLAN が MSTI 0（IST）にマッピングされます（VLAN を特定の MSTI にマッピングする方法については、「VLAN と MSTI のマッピングおよびマッピング解除」[p.6-23] を参照）。
- システムのプライベート VLAN で作業する場合は、すべてのセカンダリ VLAN がプライマリ VLAN と同じ MSTI にマッピングされていることを確認してください。

  セカンダリおよびプライマリ VLAN を同期化して、同じ MSTI に設定する方法については、「プライベート VLAN のセカンダリ VLAN をプライマリ VLAN と同じ MSTI にマッピングする方法」（p.6-24）を参照してください。
- ロード バランスは、MST 領域の*内部*でのみ実行できます。
- MSTI にマッピングされたすべての VLAN が、トランクによって伝送されているか、または伝送から除外されていることを確認します。
- STP は常にイネーブルのままにしておきます。
- タイマーは変更しないでください。安定性が低下することがあります。
- ユーザ トラフィックが管理 VLAN に流れないようにして、管理 VLAN とユーザ データを常に分離するようにしてください。
- プライマリおよびセカンダリ ルート スイッチの場所として、ディストリビューション レイヤおよびコア レイヤを選択します。
- ポート チャネリング — ポート チャネル バンドルは、単一ポートとみなされます。ポート コストは、このチャネルに割り当てられたすべての設定済みポート コストの合計値です。

（注）　ソフトウェアは、MST に対して中断のない完全アップグレードをサポートします。中断のないアップグレードの詳細については、『*Cisco NX-OS High Availability and Redundancy Configuration Guide*』を参照してください。

- VLAN を MSTI にマッピングすると、この VLAN が以前の MSTI から自動的に削除されます。
- 1 つの MSTI に任意の個数の VLAN をマッピングできます。
- Rapid PVST+ と MST クラウド、または PVST+ と MST クラウドとの間でロード バランスを実現するには、すべての MST 境界ポートがフォワーディング ステートでなければなりません。MST クラウドの CIST リージョナル ルートが CST のルートでなければなりません。MST クラウドが複数の MST 領域で構成されている場合、MST 領域の 1 つに CST ルートが含まれていなければならず、その他のすべての MST 領域では MST クラウド内に含まれるルートへのパスが、Rapid PVST+ または PVST+ クラウドよりも良好なものでなければなりません。
- ネットワークを多数の領域に分割しないでください。ただし、そのような状況が避けられないような場合には、スイッチド LAN を非レイヤ 2 装置と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。

- プライベート VLAN で作業する場合は、**private-vlan synchronize** コマンドを入力して、セカンダリ VLAN を、プライマリ VLAN と同じ MSTI にマッピングします。
- MST コンフィギュレーション サブモードで作業している場合は、次の注意事項に従ってください。
  - コマンド リファレンスの各行によって未適用の領域設定が作成されます。
  - 未適用の領域設定は、現在の領域の設定から開始されます。
  - 変更をコミットしないで、MST コンフィギュレーション サブモードを終了するには、**abort** コマンドを入力します。
  - MST コンフィギュレーション サブモードを終了し、サブモード終了前に行われたすべての変更をコミットするには、**exit** または **end** コマンドを入力するか、または **Ctrl + z** キーを押します。

MST の設定

ここでは、次の内容について説明します。

- MST のイネーブル化（p.6-15）
- MST コンフィギュレーション モードの開始（p.6-16）
- MST 名の指定（p.6-18）
- MST コンフィギュレーション リビジョン番号の指定（p.6-19）
- MST 領域のコンフィギュレーションの指定（p.6-20）
- VLAN と MSTI のマッピングおよびマッピング解除（p.6-23）
- プライベート VLAN のセカンダリ VLAN をプライマリ VLAN と同じ MSTI にマッピングする方法（p.6-24）
- ルート ブリッジの設定（p.6-26）
- セカンダリ ルート ブリッジの設定（p.6-27）
- スイッチ プライオリティの設定（p.6-29）
- ポート プライオリティの設定（p.6-30）
- ポート コストの設定（p.6-31）
- hello タイムの設定（p.6-33）
- 転送遅延時間の設定（p.6-34）
- 最大エージング タイムの設定（p.6-35）
- 最大ホップ カウントの設定（p.6-36）
- リンク タイプの指定（p.6-37）
- プロトコルの再初期化（p.6-38）

（注） Cisco IOS の CLI に慣れている場合、この機能のシスコ ソフトウェア コマンドは従来の Cisco IOS コマンドと異なることがあるので注意が必要です。

MST のイネーブル化

MST をイネーブルにできます。デフォルトは、Rapid PVST+ です。

同じ VDC 上で MST と Rapid PVST+ を同時に実行することはできません。

（注） 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 インスタンスが前のモードで停止して新規モードで再開されるため、トラフィックは中断されます。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree mode mst**
3. **exit**

4. **show running-config spanning-tree all**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree mode mst** **例：** `switch(config)# spanning-tree mode mst`	デバイス上で MST をディセーブルにして、Rapid PVST+ に戻します。
	no spanning-tree mode mst **例：** `switch(config)# no spanning-tree mode mst`	デバイス上で MST をディセーブルにして、Rapid PVST+ に戻します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show running-config spanning-tree all** **例：** `switch# show running-config spanning-tree all`	（任意）現在稼働している STP コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、デバイス上で MST をイネーブルにする例を示します。

```
switch# config t
switch(config)# spanning-tree mode mst
switch(config)# exit
switch#
```

（注） 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 インスタンスが前のモードで停止して新規モードで再開されるため、トラフィックは中断されます。

MST コンフィギュレーション モードの開始

デバイスに MST 名、VLAN/ インスタンス間マッピング、および MST リビジョン番号を設定するには、MST コンフィギュレーション モードを開始します。

複数のデバイスが同じ MST 領域内にある場合は、これらのデバイスの MST 名、VLAN/ インスタンス間マッピング、および MST リビジョン番号を*同一*にする必要があります。

（注） MST コンフィギュレーション モードでは、コマンド リファレンスの各行によって未適用の領域設定が作成されます。また、未適用の領域設定は、*現在の*領域の設定から開始されます。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **[no] spanning-tree mst configuration**
3. **exit**
   または
   abort
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree mst configuration**
	
	例：
	`switch(config)# spanning-tree mst configuration`
	`switch(config-mst)#`
		システム上で、MST コンフィギュレーション サブモードを開始します。次に示す MST コンフィギュレーション パラメータを割り当てるには、MST コンフィギュレーション サブモードを開始する必要があります。
		• MST 名
		• VLAN/MSTI 間マッピング
		• MST リビジョン番号
		• プライベート　VLAN　での、プライマリ VLAN とセカンダリ VLAN の同期

	no spanning-tree mst configuration **例：** `switch(config-mst)# no spanning-tree mst configuration`	MST 領域設定を次のデフォルト値に戻します。 • 領域名は空の文字列です。 • どの MSTI にも VLAN はマッピングされません（すべての VLAN は CIST インスタンスにマッピングされます）。 • リビジョン番号は 0 です。

ステップ 3	**exit**
	
	例：
	`switch(config-mst)# exit`
	`switch(config)#`
		すべての変更をコミットし、MST コンフィギュレーション サブモードを終了します。

	abort
	
	例：
	`switch(config-mst)# abort`
	`switch(config)#`
		変更をコミットしないで、MST コンフィギュレーション サブモードを終了します。

ステップ 4	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、デバイスで MST コンフィギュレーション サブモードを開始する例を示します。

```
switch# config t
switch(config)# spanning-tree mst configuration
switch(config-mst)#
```

次に、デバイスで変更をコミットし、MST コンフィギュレーション サブモードを終了する例を示します。

```
sswitch(config-mst)# exit
switch(config)#
```

次に、デバイスで変更を*コミットしない*で、MST コンフィギュレーション サブモードを終了する例を示します。

```
sswitch(config-mst)# abort
switch(config)#
```

MST 名の指定

ブリッジに領域名を設定できます。複数のブリッジが同じ MST 領域内にある場合は、これらのブリッジの MST 名、VLAN/ インスタンス間マッピング、および MST リビジョン番号を*同一*にする必要があります。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree mst configuration**
3. **name** *name*
4. **exit**
   または
   abort
5. **show spanning-tree mst**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree mst configuration**
	
	例：
	`switch(config)# spanning-tree mst configuration`
	`switch(config-mst)#`
		MST コンフィギュレーション サブモードを開始します。

	コマンド	目的
ステップ 3	**name** *name* **例：** `switch(config-mst)# name accounting`	MST 領域の名前を指定します。*name* 文字列は、最大 32 文字で大文字と小文字を区別します。デフォルトは空の文字列です。

ステップ 4	**exit**
	
	例：
	`switch(config-mst)# exit`
	`switch(config)#`
		すべての変更をコミットし、MST コンフィギュレーション サブモードを終了します。

	abort
	
	例：
	`switch(config-mst)# abort`
	`switch(config)#`
		変更をコミットしないで、MST コンフィギュレーション サブモードを終了します。

ステップ 5	**show spanning-tree mst** **例：** `switch# show spanning-tree mst`	（任意）MST コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、MST 領域の名前を設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst configuration
switch(config-mst)# name accounting
switch(config-mst)#
```

MST コンフィギュレーション リビジョン番号の指定

ブリッジにリビジョン番号を設定します。複数のブリッジが同じ MST 領域内にある場合は、これらのブリッジの MST 名、VLAN/ インスタンス間マッピング、および MST リビジョン番号を*同一*にする必要があります。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree mst configuration**
3. **revision** *version*
4. **exit**
   または
   abort
5. **show spanning-tree mst**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree mst configuration**
	
	例：
	`switch(config)# spanning-tree mst configuration`
	`switch(config-mst)#`
		MST コンフィギュレーション サブモードを開始します。

ステップ 3	**revision** *version* **例：** `switch(config-mst)# revision 5`	MST 領域のリビジョン番号を指定します。指定できる範囲は 0 ～ 65535、デフォルト値は 0 です。

ステップ 4	**exit**
	
	例：
	`switch(config-mst)# exit`
	`switch(config)#`
		すべての変更をコミットし、MST コンフィギュレーション サブモードを終了します。

	abort
	
	例：
	`switch(config-mst)# abort`
	`switch(config)#`
		変更をコミットしないで、MST コンフィギュレーション サブモードを終了します。

ステップ 5	**show spanning-tree mst** **例：** `switch# show spanning-tree mst`	（任意）MST コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、MSTI 領域のリビジョン番号を 5 に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst configuration
switch(config-mst)# revision 5
switch(config-mst)#
```

MST 領域のコンフィギュレーションの指定

複数のデバイスを同じ MST 領域に設定するには、同じ VLAN/ インスタンス間マッピング、同じコンフィギュレーション リビジョン番号、および同じ MST 名を設定する必要があります。

1 つの領域では、1 つのメンバーまたは同じ MST コンフィギュレーションを持つ複数のメンバーを有することができます。各メンバーには IEEE 802.1w RSTP BPDU を処理する能力がなければなりません。ネットワーク内の MST 領域の数に制限はありませんが、各領域がサポートできる MSTI の数は最大で 65 です。1 つの VLAN を同時に 2 つの MSTI に割り当てることはできません。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree mst configuration**
3. **instance** *instance-id* **vlan** *vlan-range*
4. **name** *name*
5. **revision** *version*
6. **exit**
   または
   abort
7. **show spanning-tree mst**
8. **copy running-config startup-config**

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree mst configuration**
	
	例：
	`switch(config)# spanning-tree mst configuration`
	`switch(config-mst)#`
		MST コンフィギュレーション サブモードを開始します。

ステップ 3	`switch(config-mst)#` **instance** *instance-id* **vlan** *vlan-range* **例：** `switch(config-mst)# instance 1 vlan 10-20`	次のように VLAN を MSTI にマッピングします。 • *instance-id* の範囲は 1 ～ 4094 です。 • **vlan** *vlan-range* の範囲は、1 ～ 4094 です。 VLAN を MSTI にマッピングすると、マッピングは差分で実行されます。コマンドに指定された VLAN は以前にマッピングされた VLAN に追加されるか、または VLAN から削除されます。 VLAN 範囲を指定する場合には、ハイフンを使用します。たとえば VLAN 1 ～ 63 を MSTI 1 にマッピングする場合は、**instance 1 vlan 1-63** を入力します。 一連の VLAN を指定する場合には、カンマを入力します。たとえば VLAN 10、20、30 を MSTI 1 にマッピングする場合は、**instance 1 vlan 10, 20, 30** を入力します。
ステップ 4	`switch(config-mst)#` **name** *name* **例：** `switch(config-mst)# name region1`	インスタンス名を指定します。*name* 文字列は、最大 32 文字で大文字と小文字を区別します。
ステップ 5	`switch(config-mst)#` **revision** *version* **例：** `switch(config-mst)# revision 1`	設定の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。

	コマンド	目的

ステップ 6	**exit**
	
	例：
	`switch(config-mst)# exit`
	`switch(config)#`
		すべての変更をコミットし、MST コンフィギュレーション サブモードを終了します。

	abort
	
	例：
	`switch(config-mst)# abort`
	`switch(config)#`
		変更をコミットしないで、MST コンフィギュレーション サブモードを終了します。

ステップ 7	**show spanning-tree mst** **例：** `switch# show spanning-tree mst`	（任意）MST コンフィギュレーションを表示します。
ステップ 8	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

デフォルトに戻すには、以下のように実行します。

- デフォルトの MST 領域設定に戻るには、**no spanning-tree mst configuration** グローバル コンフィギュレーション コマンドを入力します。
- デフォルトの VLAN/ インスタンス間マッピングに戻るには、**no instance** *instance_id* **vlan** *vlan-range* MST コンフィギュレーション コマンドを入力します。
- デフォルトの名前に戻すには、**no name** MST コンフィギュレーション コマンドを入力します。
- デフォルトのリビジョン番号に戻るには、**no revision** MST コンフィギュレーション コマンドを入力します。
- Rapid PVST+ を再度イネーブルにするには、**no spanning-tree mode** または **spanning-tree mode rapid-pvst** グローバル コンフィギュレーション コマンドを入力します。

次に、MST コンフィギュレーション モードを開始して、VLAN 10 ～ 20 を MSTI 1 にマッピングし、その領域の名前を *region1* に設定し、コンフィギュレーション リビジョンを 1 に設定し、未適用の設定を表示し、変更を適用して、グローバル コンフィギュレーション モードに戻る例を示します。

```
switch(config)# spanning-tree mst configuration
switch(config-mst)# instance 1 vlan 10-20
switch(config-mst)# name region1
switch(config-mst)# revision 1
switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instances configured 2
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------

switch(config-mst) exit
switch(config)#
```

VLAN と MSTI のマッピングおよびマッピング解除

複数のブリッジが同じ MST 領域内にある場合は、これらのブリッジの MST 名、VLAN/ インスタンス間マッピング、および MST リビジョン番号を*同一*にする必要があります。

（注） VLAN/MSTI マッピングを変更すると、MST が再コンバージェンスされます。

（注） MSTI はディセーブルにできません。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree mst configuration**
3. **[no] instance** *instance-id* **vlan** *vlan-range*
4. **exit**
   または
   abort
5. **show spanning-tree mst**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree mst configuration**
	
	例：
	`switch(config)# spanning-tree mst configuration`
	`switch(config-mst)#`
		MST コンフィギュレーション サブモードを開始します。

	コマンド	目的
ステップ 3	**instance** *instance-id* **vlan** *vlan-range* **例：** `switch(config-mst)# instance 3 vlan 200`	次のように VLAN を MSTI にマッピングします。 • *instance_id* の範囲は 1 ～ 4094 です。 インスタンス 0 は、各 MST 領域の IST 専用です。 • *vlan-range* の範囲は 1 ～ 4094 です。 VLAN を MSTI にマッピングすると、マッピングは差分で実行されます。コマンドに指定された VLAN は以前にマッピングされた VLAN に追加されるか、または VLAN から削除されます。
	no instance *instance-id* **vlan** *vlan-range* **例：** `switch(config-mst)# no instance 3 vlan 200`	指定されたインスタンスを削除し、VLAN をデフォルト MSTI（CIST）に戻します。

ステップ 4	**exit**
	
	例：
	`switch(config-mst)# exit`
	`switch(config)#`
		すべての変更をコミットし、MST コンフィギュレーション サブモードを終了します。

	abort
	
	例：
	`switch(config-mst)# abort`
	`switch(config)#`
		変更をコミットしないで、MST コンフィギュレーション サブモードを終了します。

ステップ 5	**show spanning-tree mst** **例：** `switch# show spanning-tree mst`	（任意）MST コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、VLAN 200 を MSTI 3 にマッピングする例を示します。

```
switch# config t
switch(config)# spanning-tree mst configuration
switch(config-mst)# instance 3 vlan 200
switch(config-mst)#
```

プライベート VLAN のセカンダリ VLAN をプライマリ VLAN と同じ MSTI にマッピングする方法

システムのプライベート VLAN で作業する場合は、すべてのセカンダリ VLAN が同じ MSTI 内、および対応するプライマリ VLAN 内になければなりません。この同期化を自動実行するには、コマンドを入力します。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree mst configuration**
3. **private-vlan synchronize**
4. **exit**
   または
   abort
5. **show spanning-tree mst**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree mst configuration**
	
	例：
	`switch(config)# spanning-tree mst configuration`
	`switch(config-mst)#`
		MST コンフィギュレーション サブモードを開始します。

ステップ 3	**private-vlan synchronize** **例：** `g-mst)# private-vlan synchronize`	すべてのプライベート VLAN で、すべてのセカンダリ VLAN を同じ MSTI および対応するプライマリ VLAN に自動的にマッピングします。

ステップ 4	**exit**
	
	例：
	`switch(config-mst)# exit`
	`switch(config)#`
		すべての変更をコミットし、MST コンフィギュレーション サブモードを終了します。

	abort
	
	例：
	`switch(config-mst)# abort`
	`switch(config)#`
		変更をコミットしないで、MST コンフィギュレーション サブモードを終了します。

ステップ 5	**show spanning-tree mst** **例：** `switch# show spanning-tree mst`	（任意）MST コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、すべてのプライベート VLAN で、すべてのセカンダリ VLAN を同じ MSTI および対応するプライマリ VLAN に自動的にマッピングする例を示します。

```
switch# config t
switch(config)# spanning-tree mst configuration
switch(config-mst)# private-vlan synchronize
switch(config-mst)#
```

ルート ブリッジの設定

ルート ブリッジになるデバイスを設定できます。

ルート ブリッジになるために必要な値が 4096 より小さい場合は、**spanning-tree vlan** *vlan_ID* **primary root** コマンドは失敗します。ソフトウェアがブリッジ プライオリティをこれ以上小さくできない場合、デバイスは次のメッセージを戻します。

```
Error: Failed to set root bridge for VLAN 1
It may be possible to make the bridge root by setting the priority
for some (or all) of these instances to zero.
```

（注） 各 MSTI のルート ブリッジは、バックボーンまたはディストリビューション デバイスでなければなりません。アクセス デバイスをスパニング ツリーのプライマリ ルート ブリッジとして設定しないでください。

レイヤ 2 ネットワークの直径（すなわち、レイヤ 2 ネットワーク上の任意の 2 つの端末間における最大レイヤ 2 ホップ数）を指定するには、MSTI 0（IST）でのみ利用可能な **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、デバイス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** キーワードを入力すると、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。

（注） デバイスがルート ブリッジとして設定されている場合、**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、および最大エージング タイムを手動で設定しないでください。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]]
3. **exit**
4. **show spanning-tree mst**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 2	**spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]] **例：** `switch(config)# spanning-tree mst 5 root primary`	次のように、デバイスをルート ブリッジとして設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られたインスタンス範囲、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 1 ～ 4094 です。 • **diameter** *net-diameter* には、任意の 2 つの端末間における最大レイヤ 2 ホップ数を指定します。デフォルトは 7 です。このキーワードを使用できるのは MSTI 0 のみです。 • **hello-time** *seconds* には、ルート ブリッジによって作成されるコンフィギュレーション メッセージの間隔を秒単位で指定します。指定できる範囲は 1 ～ 10 秒です。デフォルトは 2 秒です。
	no spanning-tree mst *instance-id***root** **例：** `switch(config)# no spanning-tree mst 5 root`	スイッチのプライオリティ、直径、hello タイムをデフォルト値に戻します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show spanning-tree mst** **例：** `switch# show spanning-tree mst`	（任意）MST コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、デバイスを MSTI 5 のルート スイッチに設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst 5 root primary
switch(config)#
```

セカンダリ ルート ブリッジの設定

複数のバックアップ ルート ブリッジを設定するには、次のコマンドを複数のデバイスに対して実行します。**spanning-tree mst root primary** グローバル コンフィギュレーション コマンドを使用してプライマリ ルート ブリッジを設定する際に使用したのと同じネットワーク直径および hello-time 値を入力します。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]]
3. **exit**
4. **show spanning-tree mst**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]] **例：** `switch(config)# spanning-tree mst 5 root secondary`	次のように、デバイスをセカンダリ ルート ブリッジとして設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られたインスタンス範囲、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 1 ～ 4094 です。 • **diameter** *net-diameter* には、任意の 2 つの端末間における最大レイヤ 2 ホップ数を指定します。デフォルトは 7 です。このキーワードを使用できるのは MSTI 0 のみです。 • **hello-time** *seconds* には、ルート ブリッジによって作成されるコンフィギュレーション メッセージの間隔を秒単位で指定します。指定できる範囲は 1 ～ 10 秒です。デフォルトは 2 秒です。
	no spanning-tree mst *instance-id* **root** **例：** `switch(config)# no spanning-tree mst 5 root`	スイッチのプライオリティ、直径、hello タイムをデフォルト値に戻します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show spanning-tree mst** **例：** `switch# show spanning-tree mst`	（任意）MST コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、デバイスを MSTI 5 のセカンダリ ルートスイッチに設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst 5 root secondary
switch(config)#
```

スイッチ プライオリティの設定

指定されたデバイスがルート ブリッジとして選択される可能性が高くなるように、MSTI のスイッチ プライオリティを設定できます。

（注） **spanning-tree mst priority** コマンドを使用する場合は、注意してください。通常、スイッチ プライオリティを変更するには、**spanning-tree mst root primary** および **spanning-tree mst root secondary** 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ことを推奨します。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree mst** *instance-id* **priority** *priority-value*
3. **exit**
4. **show spanning-tree mst**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree mst** *instance-id* **priority** *priority-value* **例：** `switch(config)# spanning-tree mst 5 priority 4096`	次のように、デバイス 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インスタンス範囲、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 1 ～ 4094 です。 • **priority** の範囲は、4096 単位で 0 ～ 61440 です。デフォルト値は 32768 です。値が少ない方が、デバイスがルート ブリッジとして選択される可能性が高くなります。 プライオリティ値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。これ以外の値はすべて拒否されます。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 4	**show spanning-tree mst** **例：** `switch# show spanning-tree mst`	（任意）MST コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、MSTI 5 のブリッジ プライオリティを 4096 に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst 5 priority 4096
switch(config)#
```

ポート プライオリティの設定

ループが発生すると、MST はポート プライオリティを使用して、フォワーディング ステートに置くインターフェイスを選択します。最初に選択させたいインターフェイスには低いプライオリティ値を、最後に選択させたいインターフェイスには高いプライオリティ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が同じプライオリティ値を使用している場合には、MST はインターフェイス番号が最も小さいインターフェイスをフォワーディング ステートにして、残りのインターフェイスをブロックします。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **interface** {{*type slot/port*} | {**port-channel** *number*}}
3. **spanning-tree mst** *instance-id* **port-priority** *priority*
4. **exit**
5. **show spanning-tree mst**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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** {{*type slot/port*} | {**port-channel** *number*}}
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**spanning-tree mst** *instance-id* **port-priority** *priority* **例：** `switch(config-if)# spanning-tree mst 3 port-priority 64`	次のように、ポート プライオリティを設定します。 • *instance-id* には、単一の MSTI、ハイフンで区切られた MSTI の範囲、またはカンマで区切られた一連の MSTI を指定できます。指定できる範囲は 1 ～ 4094 です。 • *priority* の範囲は 32 単位で、0 ～ 224 です。デフォルト値は 128 です。数値が小さいほど、プライオリティは高くなります。 有効なプライオリティ値は、0、32、64、96、128、160、192、224 です。その他の値はすべて拒否されます。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 5	**show spanning-tree mst** **例：** `switch# show spanning-tree mst`	（任意）MST コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、イーサネット ポート 3/1 上の MSTI 3 の MST インターフェイス ポート プライオリティを 64 に設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 3/1
switch(config-if)# spanning-tree mst 3 port-priority 64
switch(config-if)# exit
switch(config)
```

ポート コストの設定

MST ポート コストのデフォルト値は、インターフェイスのメディア速度から抽出されます。ループが発生すると、MST はコストを使用して、フォワーディング ステートに置くインターフェイスを選択します。最初に選択させたいインターフェイスには低いコスト値を、最後に選択させたい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が同じコスト値を使用している場合には、MST はインターフェイス番号が最も小さいインターフェイスをフォワーディング ステートにして、残りのインターフェイスをブロックします。

（注） MST はロング パスコスト計算方式を使用します。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **interface** {{*type slot/port*} | {**port-channel** *number*}}
3. **spanning-tree mst** *instance-id* **cost** [*cost* | *auto*]
4. **exit**
5. **show spanning-tree mst**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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** {{*type slot/port*} | {**port-channel** *number*}}
	
	例：
	`switch# config t`
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するインターフェイスを指定します。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	**spanning-tree mst** *instance-id* **cost** [*cost* | *auto*] **例：** `switch(config-if)# spanning-tree mst 4 cost 17031970`	コストを設定します。 ループが発生すると、MST はパス コストを使用して、フォワーディング ステートに置くインターフェイスを選択します。次のように、パス コストの低い方が高速で伝送されます。 • *instance-id* には、単一のインスタンス、ハイフンで区切られたインスタンス範囲、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 1 ～ 4094 です。 • *cost* の範囲は 1 ～ 200000000 です。デフォルト値は **auto** で、値はインターフェイスのメディア速度から抽出されます。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 5	**show spanning-tree mst** **例：** `switch# show spanning-tree mst`	（任意）MST コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、イーサネット 3/1 上の MSTI 4 の MST インターフェイス ポート コストを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 3/1
switch(config-if)# spanning-tree mst 4 cost 17031970
switch(config-if)# exit
switch(config)
```

hello タイムの設定

デバイス上のすべてのインスタンスに対してルート ブリッジが作成する設定メッセージの間隔を設定するには、hello タイムを変更します。

（注） **spanning-tree mst hello-time** コマンドを使用する場合は、注意してください。通常、hello タイムを変更するには、**spanning-tree mst** *instance-id* **root primary** および **spanning-tree mst** *instance-id* **root secondary** グローバル コンフィギュレーション コマンドを入力します。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree mst hello-time** *seconds*
3. **exit**
4. **show spanning-tree mst**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree mst hello-time** *seconds* **例：** `switch(config)# spanning-tree mst hello-time 1`	すべての MSTI に対して hello タイムを設定します。hello タイムは、ルート ブリッジによって作成される設定メッセージの間隔です。これらのメッセージは、デバイスが動作していることを示します。*seconds* の範囲は 1 ～ 10 です。デフォルトは 2 秒です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 4	**show spanning-tree mst** **例：** `switch# show spanning-tree mst`	（任意）MST コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、デバイスの hello タイムを 1 秒に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst hello-time 1
switch(config)#
```

転送遅延時間の設定

デバイスのすべての MSTI の転送遅延時間を 1 つのコマンドで設定できます。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree mst forward-time** *seconds*
3. **exit**
4. **show spanning-tree mst**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree mst forward-time** *seconds* **例：** `switch(config)# spanning-tree mst forward-time 10`	すべての MSTI の転送時間を設定します。転送遅延は、スパニング ツリー ブロッキングおよびラーニング ステートからフォワーディング ステートに移行するまでにポートが待機する秒数です。*seconds* の範囲は 4 ～ 30 です。デフォルトは 15 秒です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 4	**show spanning-tree mst** **例：** `switch# show spanning-tree mst`	（任意）MST コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、デバイスの転送遅延時間を 10 秒に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst forward-time 10
switch(config)#
```

最大エージング タイムの設定

デバイスのすべての MSTI の最大エージング タイマーを 1 つのコマンドで設定できます（最大エージング タイムが適用されるのは IST のみです）。

最大エージング タイマーは、デバイスがスパニング ツリー設定メッセージを受信せずに再設定を試行するまで待機する秒数です。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree mst max-age** *seconds*
3. **exit**
4. **show spanning-tree mst**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree mst max-age** *seconds* **例：** `switch(config)# spanning-tree mst max-age 40`	すべての MSTI に対して最大エージング タイムを設定します。最大エージング タイムは、デバイスがスパニング ツリー設定メッセージを受信せずに再設定を試行するまで待機する秒数です。*seconds* の範囲は 6 ～ 40 です。デフォルトは 20 秒です。

	コマンド	目的
ステップ 3	**exit** **例：** switch(config)# exit switch#	コンフィギュレーション モードを終了します。
ステップ 4	**show spanning-tree mst** **例：** switch# show spanning-tree mst	（任意）MST コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** **例：** switch(config)# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、デバイスの最大エージング タイマーを 40 秒に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst max-age 40
switch(config)#
```

最大ホップ カウントの設定

領域内の最大ホップを設定し、それをその領域内にある IST およびすべての MSTI に適用できます。MST は IST リージョナル ルートへのパス コストおよび IP Time to Live（TTL）メカニズムに似たホップ カウント メカニズムを使用します。ホップ カウントは、メッセージ有効期間情報と同じ結果（再設定の開始）となります。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **spanning-tree mst max-hops** *hop-count*
3. **exit**
4. **show spanning-tree mst**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t switch(config)#	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	**spanning-tree mst max-hops** *hop-count* **例：** switch(config)# spanning-tree mst max-hops 40	BPDU が廃棄され、ポートに維持されていた情報が期限切れになるまでの、領域内でのホップ数を指定します。*hop-count* の範囲は 1 ～ 255 です。デフォルト値は 20 ホップです。

	コマンド	目的

ステップ 3	**exit**
	
	例：
	`switch(config-mst)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show spanning-tree mst** **例：** `switch# show spanning-tree mst`	（任意）MST コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、最大ホップ数を 40 に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst max-hops 40
switch(config)#
```

リンク タイプの指定

高速接続（802.1w 標準）は、ポイントツーポイント リンク上にのみ確立されます。デフォルトでは、リンク タイプが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。つまり、全二重ポートはポイントツーポイント接続とみなされ、半二重ポートは共有接続とみなされます。

リモート デバイスの単一ポートに、ポイントツーポイントで物理的に接続されている半二重リンクがある場合、リンク タイプのデフォルト設定を上書きして高速移行をイネーブルにできます。

リンクを共有に設定すると、STP は 802.1D にフォール バックします。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree link-type** {*auto* | *point-to-point* | *shared*}
4. **exit**
5. **show spanning-tree**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定します。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	**spanning-tree link-type** {*auto* | *point-to-point* | *shared*} **例：** `switch(config-if)# spanning-tree link-type point-to-point`	リンク タイプをポイントツーポイントまたは共有に設定します。デフォルト値はデバイス接続から読み取られます。半二重リンクは共有、全二重リンクはポイントツーポイントです。リンク タイプが共有の場合、STP は 802.1D に戻ります。デフォルトの auto では、インターフェイスのデュプレックス設定に基づいてリンク タイプが設定されます。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 5	**show spanning-tree** **例：** `switch# show spanning-tree`	（任意）STP コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、リンク タイプをポイントツーポイントに設定する例を示します。

```
switch# config t
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree link-type point-to-point
switch(config-if)# exit
switch(config)#
```

プロトコルの再初期化

レガシー BPDU、または異なる領域に対応付けられた MST BPDU が受信された場合、MST ブリッジはポートが領域の境界にあることを検出できます。ただし、STP プロトコルを移行しても、レガシー デバイス（IEEE 802.1D のみが稼働するデバイス）が代表スイッチでないかぎり、レガシー デバイスがリンクから削除されたかどうかを判別することはできません。デバイス全体で、または指定されたインターフェイスでプロトコル ネゴシエーションを再初期化する（隣接デバイスとの再ネゴシエーションを強制的に行う）には、次のコマンドを入力します。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **clear spanning-tree detected-protocols** [**interface** *interface* [*interface-num* | *port-channel*]]

手順の詳細

	コマンド	目的
ステップ 1	**clear spanning-tree detected-protocol** [**interface** *interface* [*interface-num*	*port-channel*]] **例：** `switch# clear spanning-tree detected-protocol`	デバイス全体または指定されたインターフェイスで、MST を再初期化します。

次に、スロット 2 のイーサネット インターフェイスのポート 8 で、MST を再初期化する例を示します。

```
switch# clear spanning-tree detected-protocol interface ethernet 2/8
```

MST コンフィギュレーションの確認

MST コンフィギュレーション情報を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
show running-config spanning-tree [**all**]	STP 情報を表示します。
show spanning-tree mst configuration	MST 情報を表示します。
show spanning-tree mst [**detail**]	MSTI の情報を表示します。
show spanning-tree mst *instance-id* [**detail**]	指定された MSTI に関する情報を表示します。
show spanning-tree mst *instance-id* **interface** {**ethernet** *slot/port* | **port-channel** *channel-number*} [**detail**]	指定されたインターフェイスおよびインスタンスの MST 情報を表示します。
show spanning-tree summary	STP の概要を表示します。
show spanning-tree detail	STP の詳細を表示します。
show spanning-tree {**vlan** *vlan-id* | **interface** {[**ethernet** *slot/port*] | [**port-channel** *channel-number*]}} [**detail**]	VLAN またはインターフェイス単位の STP 情報を表示します。
show spanning-tree vlan *vlan-id* **bridge**	STP ブリッジの情報を表示します。

これらのコマンドの出力フィールドの詳細については、『*Cisco NX-OS Layer 2 Switching Command Reference*』を参照してください。

MST 統計情報の表示およびクリア

MST コンフィギュレーション情報を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
clear spanning-tree counters [**interface** *type/slot* | **vlan** *vlan-id*]	STP のカウンタをクリアします。
show spanning-tree {**vlan** *vlan-id* | **interface** {[**ethernet** *slot/port*] | [**port-channel** *channel-number*]}} **detail**	送受信された BPDU などの STP 情報を、インターフェイスまたは VLAN 別に表示します。

MST の設定例

次に、MST を設定する例を示します。

```
switch# configure terminal
switch(config)# spanning-tree mode mst
switch(config)# spanning-tree port type edge bpduguard default
switch(config)# spanning-tree port type edge bpdufilter default
switch(config)# spanning-tree port type network default
switch(config)# spanning-tree mst 0-64 priority 24576
switch(config)# spanning-tree mst configuration
switch(config-mst)# name cisco_region_1
switch(config-mst)# revision 2
switch(config-mst)# instance 1 vlan 1-21
switch(config-mst)# instance 2 vlan 22-42
switch(config-mst)# instance 3 vlan 43-63
switch(config-mst)# instance 4 vlan 64-84
switch(config-mst)# instance 5 vlan 85-105
switch(config-mst)# instance 6 vlan 106-126
switch(config-mst)# instance 7 vlan 127-147
switch(config-mst)# instance 8 vlan 148-168
switch(config-mst)# instance 9 vlan 169-189
switch(config-mst)# instance 10 vlan 190-210
switch(config-mst)# instance 11 vlan 211-231
switch(config-mst)# instance 12 vlan 232-252
switch(config-mst)# instance 13 vlan 253-273
switch(config-mst)# instance 14 vlan 274-294
switch(config-mst)# instance 15 vlan 295-315
switch(config-mst)# instance 16 vlan 316-336
switch(config-mst)# instance 17 vlan 337-357
switch(config-mst)# instance 18 vlan 358-378
switch(config-mst)# instance 19 vlan 379-399
switch(config-mst)# instance 20 vlan 400-420
switch(config-mst)# instance 21 vlan 421-441
switch(config-mst)# instance 22 vlan 442-462
switch(config-mst)# instance 23 vlan 463-483
switch(config-mst)# instance 24 vlan 484-504
switch(config-mst)# instance 25 vlan 505-525
switch(config-mst)# instance 26 vlan 526-546
switch(config-mst)# instance 27 vlan 547-567
switch(config-mst)# instance 28 vlan 568-588
switch(config-mst)# instance 29 vlan 589-609
switch(config-mst)# instance 30 vlan 610-630
switch(config-mst)# instance 31 vlan 631-651
switch(config-mst)# instance 32 vlan 652-672
switch(config-mst)# instance 33 vlan 673-693
switch(config-mst)# instance 34 vlan 694-714
switch(config-mst)# instance 35 vlan 715-735
switch(config-mst)# instance 36 vlan 736-756
switch(config-mst)# instance 37 vlan 757-777
switch(config-mst)# instance 38 vlan 778-798
switch(config-mst)# instance 39 vlan 799-819
switch(config-mst)# instance 40 vlan 820-840
switch(config-mst)# instance 41 vlan 841-861
switch(config-mst)# instance 42 vlan 862-882
switch(config-mst)# instance 43 vlan 883-903
switch(config-mst)# instance 44 vlan 904-924
switch(config-mst)# instance 45 vlan 925-945
switch(config-mst)# instance 46 vlan 946-966
switch(config-mst)# instance 47 vlan 967-987
switch(config-mst)# instance 48 vlan 988-1008
switch(config-mst)# instance 49 vlan 1009-1029
switch(config-mst)# instance 50 vlan 1030-1050
switch(config-mst)# instance 51 vlan 1051-1071
switch(config-mst)# instance 52 vlan 1072-1092
switch(config-mst)# instance 53 vlan 1093-1113
switch(config-mst)# instance 54 vlan 1114-1134
switch(config-mst)# instance 55 vlan 1135-1155
switch(config-mst)# instance 56 vlan 1156-1176
```

```
switch(config-mst)# instance 57 vlan 1177-1197
switch(config-mst)# instance 58 vlan 1198-1218
switch(config-mst)# instance 59 vlan 1219-1239
switch(config-mst)# instance 60 vlan 1240-1260
switch(config-mst)# instance 61 vlan 1261-1281
switch(config-mst)# instance 62 vlan 1282-1302
switch(config-mst)# instance 63 vlan 1303-1323
switch(config-mst)# instance 64 vlan 1324-1344
switch(config-mst)# exit
switch(config)# interface Ethernet3/1
switch(config-if)# switchport
switch(config-if)# no shutdown
switch(config-if)# spanning-tree port type edge
switch(config-if)# exit
switch(config)# interface Ethernet3/2
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# no shutdown
switch(config-if)# spanning-tree guard root
switch(config-if)# exit
switch(config)#
```

STP ポート タイプ、BPDU ガード、BPDU フィルタ、およびルート ガードの設定の詳細については、第 7 章「STP 拡張機能の設定」を参照してください。

デフォルト設定

表 6-1 に、MST パラメータのデフォルト設定を示します。

表 6-1　デフォルトの MST パラメータ

パラメータ	デフォルト
スパニング ツリー	イネーブル
スパニング ツリー モード	Rapid PVST+ がデフォルトでイネーブル **注意**　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 インスタンスが前のモードで停止して新規モードで開始されるため、トラフィックが中断されます。
名前	空の文字列
VLAN マッピング	すべての VLAN を CIST インスタンスにマッピング
リビジョン	0
インスタンス ID	インスタンス 0。VLAN 1 ～ 4094 はデフォルトでインスタンス 0 にマッピングされます。
MST 領域あたりの MSTI 数	65
ブリッジ プライオリティ（CIST ポート単位で設定可能）	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）	auto デフォルトのポート コストは、次のように、ポート速度から判別されます。 • 10 Mbps：2,000,000 • 100 Mbps：200,000 • 1 ギガビット イーサネット：20,000 • 10 ギガビット イーサネット：2,000
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
最大ホップ カウント	20 ホップ
リンク タイプ	auto デフォルト リンク タイプは、次のようにデュプレックスから判別されます。 • 全二重：ポイントツーポイント リンク • 半二重：共有リンク

追加情報

MST の実装に関する情報については、次のセクションを参照してください。

- 関連資料（p.6-44）
- 標準規格（p.6-44）
- MIB（p.6-44）

関連資料

関連トピック	マニュアル名
Rapid PVST+	第 5 章「Rapid PVST+ の設定」
STP 拡張機能	第 7 章「STP 拡張機能の設定」
コマンド リファレンス	『*Cisco NX-OS Layer 2 Switching Command Reference*』
DCNM レイヤ 2 スイッチングの設定	『*Cisco DCNM Layer 2 Switching Configuration Guide*』
レイヤ 2 インターフェイス	『*Cisco NX-OS Interfaces Configuration Guide*』
NX-OS の基本情報	『*Cisco NX-OS Fundamentals Configuration Guide*』
ハイ アベイラビリティ	『*Cisco NX-OS High Availability and Redundancy Guide*』
システム管理	『*Cisco NX-OS System Management Configuration Guide*』
VDC	『*Cisco NX-OS Virtual Device Context Configuration Guide*』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco NX-OS Release Notes*』 Release 4.0

標準規格

標準規格	タイトル
IEEE 802.1Q-2006（従来の名称は IEEE 802.1s）、IEEE 802.1D-2004（従来の名称は IEEE 802.1w）、IEEE 802.1D、IEEE 802.1t	—

MIB

MIB	MIB リンク
• CISCO-STP-EXTENSION-MIB • BRIDGE-MIB	次の URL から、MIB の検索およびダウンロードができます。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

CHAPTER 7

STP 拡張機能の設定

この章では、NX-OS デバイス上での Spanning Tree Protocol（STP; スパニング ツリー プロトコル）拡張機能の設定方法について説明します。

この章で説明する内容は、次のとおりです。

- STP 拡張機能の概要（p.7-2）
- STP 拡張機能のライセンス要件（p.7-9）
- STP 拡張機能の前提条件（p.7-9）
- 注意事項および制限（p.7-10）
- STP 拡張機能の設定（p.7-11）
- STP 拡張機能の設定の確認（p.7-28）
- STP 拡張機能の設定例（p.7-28）
- デフォルト設定（p.7-29）
- 追加情報（p.7-30）

(注) STP および Per VLAN Rapid Spanning Tree（Rapid PVST+）の詳細は第 5 章「Rapid PVST+ の設定」を、Multiple Spanning Tree（MST）の詳細は第 6 章「MST の設定」を参照してください。

STP 拡張機能の概要

（注） レイヤ 2 インターフェイスの作成に関する情報は、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

ループ回避を改善し、ユーザによる設定ミスを削減し、プロトコル パラメータの制御を向上するために、シスコは STP に拡張機能を追加しました。IEEE 802.1w Rapid Spanning Tree Protocol（RSTP）規格に同様の機能が統合されていることも考えられますが、ここで紹介する拡張機能を使用することを推奨します。PVST シミュレーションを除き、これらの拡張機能はすべて、Rapid PVST+ および MST の両方で使用できます。PVST シミュレーションを使用できるのは、MST だけです。

使用できる拡張機能は、スパニング ツリー エッジ ポート（従来の PortFast の機能を提供）、ブリッジ保証、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）ガード、BPDU フィルタリング、ループ ガード、ルート ガード、および PVST シミュレーションです。これらの機能のほとんどは、グローバルにも、または特定のインターフェイスだけにも適用できます。

（注） スパニング ツリーは、IEEE 802.1w および IEEE 802.1s の規格を意味します。IEEE 802.1D STP について説明している場合は、802.1D であることを明記します。

+ ここでは、次の内容について説明します。

- STP ポート タイプ（p.7-2）
- ブリッジ保証（p.7-3）
- BPDU ガード（p.7-5）
- BPDU フィルタリング（p.7-6）
- ループ ガード（p.7-6）
- ルート ガード（p.7-7）
- STP 拡張機能の適用（p.7-7）
- PVST シミュレーション（p.7-8）
- ハイ アベイラビリティ（p.7-9）
- バーチャライゼーションのサポート（p.7-9）

STP ポート タイプ

スパニング ツリーのポートは、エッジ ポート、ネットワーク ポート、または標準ポートとして設定できます。ポートは、いつの時点でも、これらのステートのいずれかになります。デフォルトのスパニング ツリー ポート タイプは、標準（normal）です。

レイヤ 2 ホストに接続するエッジ ポートは、アクセス ポートまたはトランク ポートのどちらかになります。

（注） レイヤ 2 スイッチまたはブリッジに接続しているポートをエッジ ポートとして設定すると、ブリッジング ループが発生することがあります。

ネットワーク ポートは、レイヤ 2 スイッチまたはブリッジだけに接続します。

(注)　レイヤ 2 ホストまたはエッジ デバイスに接続されたポートを、誤ってスパニング ツリー ネットワーク ポートとして設定した場合、これらのポートは自動的にブロッキング ステートに移行します。

STP エッジ ポート

STP エッジ ポートは、レイヤ 2 ホストにのみ接続します。エッジ ポート インターフェイスは、ブロッキング ステートまたはラーニング ステートを経由せずに、直接フォワーディング ステートに移行します（この直接の移行は、従来のシスコの独自機能である PortFast に設定されていました）。

レイヤ 2 ホストに接続したインターフェイスでは、STP の BPDU を受信しないようにします。

ブリッジ保証

ブリッジ保証を使用すると、ネットワーク上でブリッジング ループが発生する原因となる特定の問題を回避できます。具体的には、ブリッジ保証を使用して、単方向リンク障害または他のソフトウェア障害、およびスパニング ツリー アルゴリズムの停止後もデータ トラフィックを転送し続けているデバイスから、ネットワークを保護します。

(注)　ブリッジ保証がサポートされるのは、Rapid PVST+ および MST だけです。

ブリッジ保証はデフォルトでイネーブルであり、ディセーブルにするとグローバルに適用されます。また、ブリッジ保証をイネーブルにできるのは、ポイントツーポイント リンクのスパニング ツリー ネットワーク ポート上だけです。さらに、リンクの両端でブリッジ保証がイネーブルに設定されている必要があります。リンクの一端のデバイスでブリッジ保証がイネーブルであっても、他端のデバイスがブリッジ保証をサポートしていない、またはブリッジ保証がイネーブルではない場合、接続ポートはブロックされます。

ブリッジ保証をイネーブルにすると、代替ポートやバックアップ ポートも含めたネットワーク上で稼働しているすべてのポートに対して、ハロー タイムのたびに BPDU が送信されます。ポートが指定時間を経過したあとも BPDU を受信しない場合、そのポートはブロッキング ステートになり、ルート ポートの計算には使用されません。BPDU を受信すると、ポート上で標準 スパニング ツリーのステート移行が再開されます。

図 7-1 に、一般的な STP トポロジを示します。また、図 7-2 には、ブリッジ保証を実行していない場合、デバイスの障害発生時にネットワークで発生する可能性のある問題を示します。

図 7-1　標準的な STP トポロジのネットワーク

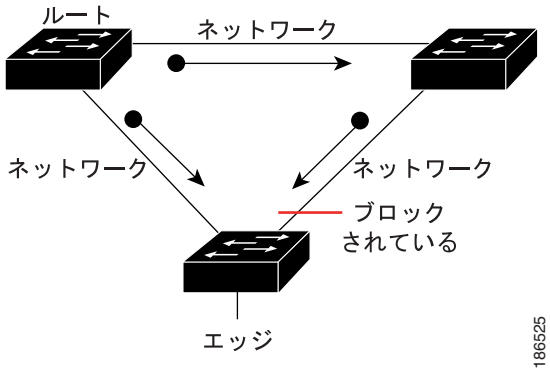


図 7-2　ブリッジ保証を実行していないネットワークの問題

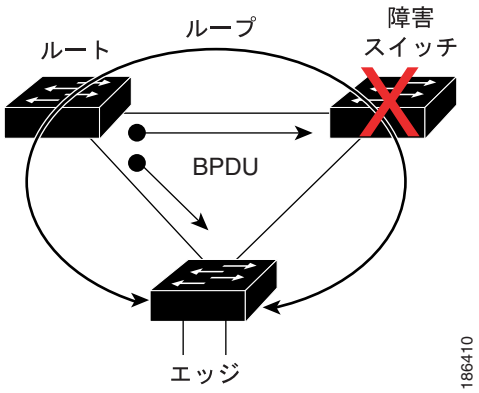


図 7-3 に、ブリッジ保証をイネーブルにしたネットワークで、すべての STP ネットワーク ポートから双方向 BPDU が発行される一般的な STP トポロジを示します。図 7-4 は、ネットワーク上でブリッジ保証をイネーブルにした場合、図 7-2 で示したネットワーク上の問題が発生しない理由を示しています。

図 7-3　ブリッジ保証を実行しているたネットワークの STP トポロジ

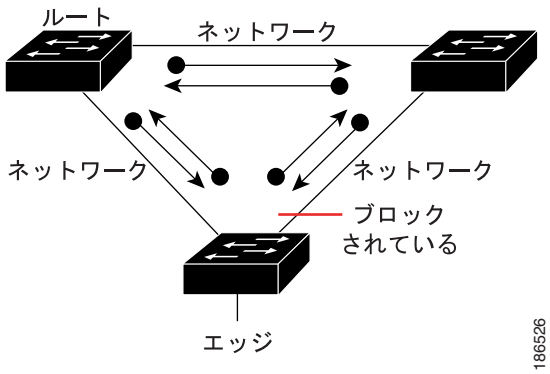
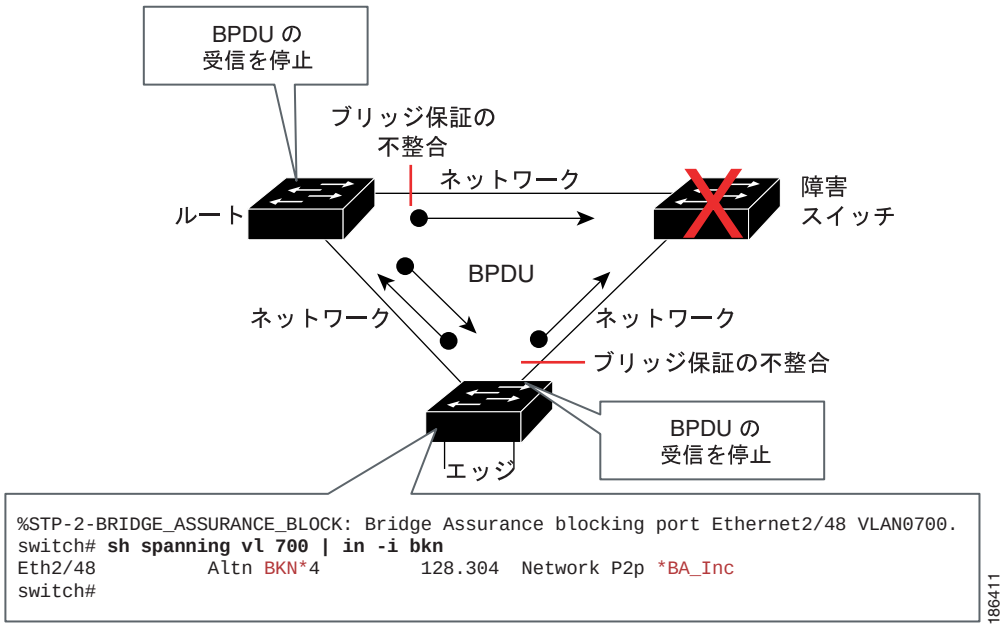


図 7-4　ブリッジ保証によるネットワーク上の問題の回避



BPDU ガード

BPDU ガードをイネーブルにすると、インターフェイスは BPDU を受信した場合にシャットダウンします。

BPDU ガードは、インターフェイス レベルで設定できます。インターフェイス レベルで BPDU ガードを設定すると、BPDU を受信したポートは、ポート タイプの設定に関係なく、すぐにシャットダウンします。

BPDU ガードをグローバルに設定すると、稼働中のスパニング ツリー エッジ ポート上でのみ有効になります。有効な設定では、レイヤ 2 LAN エッジ インターフェイスは BPDU を受信しません。レイヤ 2 LAN エッジ インターフェイスが BPDU を受信した場合、許可されていないデバイスの接続と同様に、無効な設定として通知されます。BPDU ガードをグローバルでイネーブルにすると、BPDU を受信したすべてのスパニング ツリー エッジ ポートがシャットダウンします。

BPDU ガードでは、無効な設定が通知された場合、レイヤ 2 LAN インターフェイスを手動で再起動させる必要があるので、無効な設定に対して安全に対応できます。

（注） グローバルにイネーブル化した場合、BPDU ガードは稼働中のすべてのスパニング ツリー エッジ インターフェイスに適用されます。

BPDU フィルタリング

BPDU フィルタリングを使用すると、デバイスの特定のポート上で BPDU が送信されないように、または BPDU を受信しないように設定できます。

グローバルに設定した場合、BPDU フィルタリングは稼働中のすべてのスパニング ツリー エッジ ポートに適用されます。エッジ ポートは、一般的に BPDU をドロップするホストにのみ接続すべきです。稼働中のスパニング ツリー エッジ ポートが BPDU を受信した場合、そのポートはすぐに標準スパニング ツリー ポート タイプに戻り、ステートの移行を開始します。この場合、このポート上の BPDU フィルタリングはディセーブルになり、スパニング ツリーにより、ポート上での BPDU の送信が再開されます。

また、BPDU フィルタリングは、個々のインターフェイスに対して設定できます。ポート上で BPDU フィルタリングを明示的に設定すると、そのポートは BPDU を送信しません。また、受信したすべての BPDU をドロップします。特定のインターフェイスを設定することにより、個々のポート上で、グローバルな BPDU フィルタリング設定を上書きすることができます。インターフェイスに対する BPDU フィルタリング コマンドは、インターフェイスがトランキング モードかどうかに関係なく、インターフェイス全体に適用されます。

注意　インターフェイス単位での BPDU フィルタリングの設定には、注意が必要です。ホストに接続されていないポートに BPDU フィルタリングを設定すると、そのポートは受信した BPDU を無視してフォワーディングに移行するので、ブリッジング ループが発生することがあります。

表 7-1 に、すべての BPDU フィルタリングの組み合わせを示します。

表 7-1　BPDU フィルタリングの設定

ポート単位の BPDU フィルタリング設定	BPDU フィルタリングのグローバル設定	STP エッジ ポートの設定	BPDU フィルタリング ステート
デフォルト[1]	イネーブル	イネーブル	イネーブル[2]
デフォルト	イネーブル	ディセーブル	ディセーブル
デフォルト	ディセーブル	適用なし	ディセーブル
ディセーブル	適用なし	適用なし	ディセーブル
イネーブル	適用なし	適用なし	イネーブル

1. 明示的なポート設定はありません。
2. ポートは最低 10 の BPDU を送信します。BPDU を受信すると、このポートはスパニング ツリー標準ポート ステートに戻り、BPDU フィルタリングはディセーブルになります。

ループ ガード

ループ ガードを使用すると、ポイントツーポイント リンク上の単方向リンク障害によって発生することがあるブリッジング ループを防止できます。

STP ループは、冗長トポロジのブロッキング ポートが誤ってフォワーディング ステートに移行した場合に発生します。物理的な冗長トポロジのポート（ブロッキング ポートに限らない）の 1 つで BPDU の受信が停止すると、ポートのステートが移行する原因になります。

グローバルでイネーブル化したループ ガードが有益なのは、デバイスがポイントツーポイント リンクで接続されているスイッチド ネットワークだけです。ポイントツーポイント リンクでは、代表ブリッジは不良 BPDU を送信するかリンクがダウンしない限り、存続します。ただし、共有リンク上のループ ガードはインターフェイス単位でイネーブルに設定できます。

ループ ガードを使用すると、ルート ポートまたは代替 / バックアップ ルート ポートが BPDU を受信しているかどうかを判別できます。BPDU を受信していたポートで BPDU が受信されなくなると、ループ ガードは、ポート上で BPDU の受信が再開されるまで、そのポートを不整合（ブロッキング）ステートにします。これらのポートで BPDU の受信が再開されると、ポートおよびリンクは再び動作可能として認識されます。この回復は自動的に実行されるので、プロトコルによりポートからループ不整合が排除されると、STP によりポート ステートが判別されます。

ループ ガードにより障害が特定されるので、STP は障害リンクまたは障害ブリッジのない安定したトポロジを収束できます。ループ ガードをディセーブルにすると、ループ不整合のポートはすべて、リスニング ステートに移行します（STP ポート ステートの情報については、第 5 章「Rapid PVST+ の設定」を参照してください）。

ループ ガードはポート単位でイネーブルにすることができます。ポート上でループ ガードをイネーブルにすると、そのポートが属しているすべてのアクティブ インスタンスまたは VLAN にループ ガードが自動的に適用されます。ループ ガードをディセーブルにすると、指定したポートに対してディセーブルになります。

ルート デバイス上でループ ガードをイネーブルにしても効果はありませんが、ルート デバイスが非ルート デバイスになった場合、保護が有効になります。

ルート ガード

ポート上でルート ガードをイネーブルにすると、そのポートはルート ポートになりません。受信した BPDU により、指定ポートをルート ポートとする STP コンバージェンスが実行されると、そのポートはルート不整合（ブロックされた）ステートになります。ポートが優位 BPDU の送信を停止すると、そのポートのブロックが解除されます。ポートは、STP により、フォワーディング ステートに移行します。この回復は自動的に実行されます。

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属しているすべての VLAN にルート ガードが適用されます。

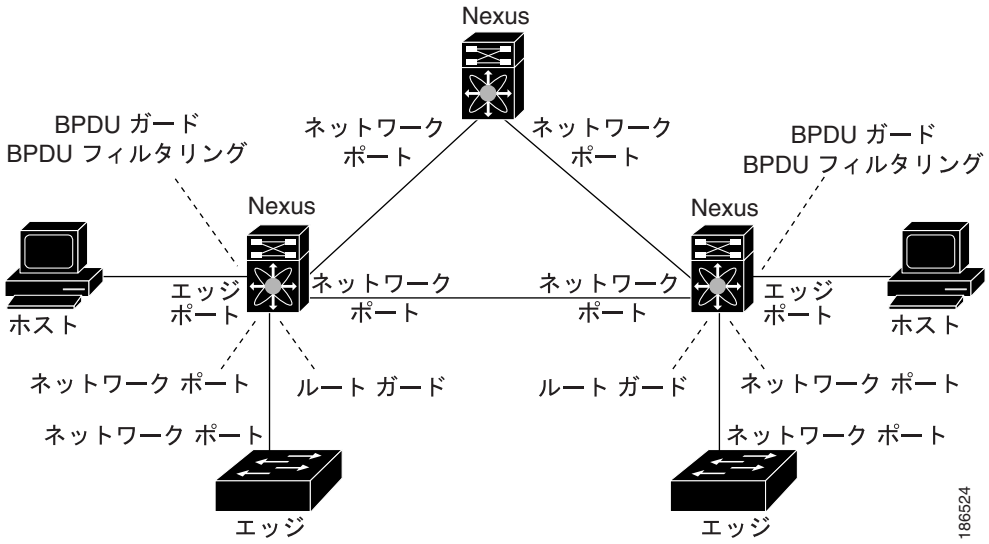
ルート ガードを使用して、ルート ブリッジをネットワークに強制的に配置できます。ルート ガードでは、ルート ガードをイネーブルにしたポートが指定ポートになります。通常、ルート ブリッジ上の複数のポートが接続されている場合を除き、ルート ブリッジのポートはすべて指定ポートです。ブリッジは、ルート ガードがイネーブルであるブリッジ ポート上で優位 BPDU を受信すると、そのポートをルート不整合 STP ステートに移行します。このように、ルート ガードによってルート ブリッジの配置を制御できます。

ルート ガードは、グローバルに設定することはできません。

STP 拡張機能の適用

図 7-5 に示すように、ネットワーク上に各種の STP 拡張機能を設定することを推奨します。ブリッジ保証は、ネットワーク全体でイネーブルになります。

図 7-5　STP 拡張機能を適正に設定したネットワーク



PVST シミュレーション

MST は、ユーザが設定しなくても、Rapid PVST+ と相互運用します。この相互運用性を提供するのが、PVST シミュレーション機能です。

（注） MST をイネーブルにすると、PVST シミュレーションがデフォルトでイネーブルになります。デフォルトでは、デバイス上のすべてのインターフェイスで MST と Rapid PVST+ が相互運用されます。

ただし、MST イネーブル ポートが Rapid PVST+ イネーブル ポートに接続される可能性を防ぐには、MST と Rapid PVST+ 間の接続を制御する必要があります。Rapid PVST+ はデフォルトの STP モードなので、多数の Rapid PVST+ 接続が発生することがあります。

Rapid PVST+ シミュレーションを、ポート単位でディセーブルにするか、デバイス全体でグローバルにディセーブルにすると、MST イネーブル ポートは、Rapid PVST+ イネーブル ポートに接続したことが検出された時点で、ブロッキング ステートに移行します。このポートは、Rapid PVST+/SSTP BPDU を受信しなくなるまで不整合ステートのままですが、そのあとは標準 STP のステート移行を再開します。

すべての STP インスタンスのルート ブリッジは、MST または Rapid PVST+ のどちらかの側に属している必要があります。すべての STP インスタンスのルート ブリッジがどちらか一方の側に属していないと、ポートは PVST シミュレーション不整合ステートになります。

（注） すべての STP インスタンスのルート ブリッジを、MST 側に配置することを推奨します。

ハイ アベイラビリティ

このソフトウェアは、STP のハイ アベイラビリティをサポートしています。ただし、統計情報とタイマーは STP の再起動時には復元されません。タイマーは最初から開始され、統計情報は 0 にリセットされます。

（注） ハイ アベイラビリティ機能の詳細については、『*Cisco NX-OS High Availability and Redundancy Configuration Guide* 』を参照してください。

バーチャライゼーションのサポート

このシステムは Virtual Device Context（VDC）をサポートしています。各 VDC で個別の STP を実行できます。1 つの VDC で Rapid VPST+ を実行し、別の VDC で MST を実行することもできます。

（注） VDC およびリソース割り当ての詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide*』を参照してください。

STP 拡張機能のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
NX-OS	STP 拡張機能には、ライセンスは不要です。ライセンス パッケージに含まれていない機能は Cisco NX-OS システム イメージにバンドルされ、追加料金なしで提供されます。NX-OS ライセンス機構の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

ただし、VDC を使用するには、Advanced Services ライセンスが必要です。

STP 拡張機能の前提条件

STP には、次の前提条件が適用されます。

- デバイスにログオンしている必要があります。
- DCNM を使用して STP パラメータを設定する前に、デバイスのコマンド ラインに NX-OS グローバル コマンドの **logging-level spanning-tree 6** を入力して、ロギング レベルを設定する必要があります。ロギング レベルの情報については、『*Cisco NX-OS System Management Configuration Guide*』を参照してください。
- STP を設定しておく必要があります。
- 必要に応じて、Advanced Services ライセンスをインストールし、特定の VDC を開始します。

注意事項および制限

STP 拡張機能の設定時は、次の注意事項および制限に従ってください。

- STP ネットワーク ポートは、スイッチだけに接続してください。
- ホスト ポートは、ネットワーク ポートではなく STP エッジ ポートとして設定する必要があります。
- STP ネットワーク ポート タイプをグローバルにイネーブルにする場合には、ホストに接続しているすべてのポートを手動で STP エッジ ポートとして設定してください。
- レイヤ 2 ホストに接続しているすべてのアクセス ポートおよびトランク ポートを、エッジ ポートとして設定する必要があります。
- ブリッジ保証は、ポイントツーポイント スパニング ツリー ネットワーク ポート上でのみ実行されます。リンクの両端に、この機能を設定しておく必要があります。
- ブリッジ保証は、ネットワーク全体でイネーブルにすることを推奨します。
- すべてのエッジ ポート上で BPDU ガードをイネーブルにすることを推奨します。
- グローバルにイネーブルしたループ ガードは、ポイントツーポイント リンク上でのみ動作します。
- インターフェイス単位でイネーブルにしたループ ガードは、共有リンクおよびポイントツーポイント リンクの両方で動作します。
- ルート ガードを適用したポートは強制的に指定ポートになりますが、ルート ポートにはなりません。ループ ガードは、ポートがルート ポートまたは代替ポートの場合にのみ有効です。ポート上でループ 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。
- ディセーブル化されたスパニング ツリー インスタンスまたは VLAN 上では、ループ ガードは無効です。
- スパニングツリーは、BPDU を送信するチャネル内で最初に動作するポートを常に選択します。このリンクが単方向になると、チャネル内の他のリンクが正常に動作していても、ループ ガードによりチャネルがブロックされます。
- ループ　ガードによってブロックされている一連のポートをグループ化してチャネルを形成すると、これらのポートのステート情報はスパニング ツリーからすべて削除され、新しいチャネルのポートは指定ロールによりフォワーディング ステートに移行できます。
- チャネルがループ ガードによりブロックされ、チャネルのメンバーが個々のリンク ステータスに戻ると、スパニング ツリーからすべてのステート情報が削除されます。チャネルを形成している 1 つ以上のリンクが単方向であっても、個々の物理ポートは指定ロールによりフォワーディング ステートに移行できます。

（注） UniDirectional Link Detection（UDLD; 単方向リンク検出）アグレッシブ モードをイネーブルにすると、リンク障害を分離できます。UDLD により障害が検出されるまではループが発生することがありますが、ループ ガードでは検出できません。UDLD の詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

- 物理ループのあるスイッチ ネットワーク上では、ループ ガードをグローバルにイネーブルにする必要があります。
- 直接の管理制御下にないネットワーク デバイスに接続しているポート上では、ルート ガードをイネーブルにする必要があります。

STP 拡張機能の設定

ここでは、次の内容について説明します。

- スパニング ツリー ポート タイプのグローバル設定（p.7-11）
- 特定のインターフェイス上でのスパニング ツリー エッジ ポートの設定（p.7-13）
- 特定のインターフェイス上でのスパニング ツリー ネットワーク ポートの設定（p.7-14）
- BPDU ガードのグローバルなイネーブル化（p.7-16）
- 特定のインターフェイス上での BPDU ガードのイネーブル化（p.7-17）
- BPDU フィルタリングのグローバルなイネーブル化（p.7-18）
- 特定のインターフェイス上での BPDU フィルタリングのイネーブル化（p.7-20）
- ループ ガードのグローバルなイネーブル化（p.7-21）
- 特定のインターフェイス上でのループ ガードまたはルート ガードのイネーブル化（p.7-23）
- PVST シミュレーションのグローバル設定（p.7-25）
- ポート単位での PVST シミュレーションの設定（p.7-26）

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

スパニング ツリー ポート タイプのグローバル設定

スパニング ツリー ポート タイプの指定は、次のように、ポートの接続先デバイスによって異なります。

- エッジ — エッジ ポートはレイヤ 2 ホストに接続し、アクセス ポートまたはトランク ポートのどちらかに設定できます。
- ネットワーク — ネットワーク ポートは、レイヤ 2 スイッチまたはブリッジだけに接続します。
- 標準 — 標準ポートは、エッジ ポートでもネットワーク ポートでもない、通常のスパニング ツリー ポートです。これらのポートは、どのデバイスにも接続できます。

ポート タイプは、グローバルまたはインターフェイス単位で設定できます。デフォルトのスパニング ツリー ポート タイプは、標準（normal）です。

始める前に

スパニング ツリー ポート タイプを設定する前に、次のことを行う必要があります。

- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。
- STP が設定されていることを確認してください。
- ポートの接続先デバイスに応じて、ポートを正しく設定していることを確認してください。

手順の要約

1. **config t**
2. **spanning-tree port type {edge | network} default**
3. **exit**
4. **show spanning-tree**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree port type edge default** **例：** `switch(config)# spanning-tree port type edge default`	レイヤ 2 ホストに接続しているすべてのアクセス ポートおよびトランク ポートを、エッジ ポートとして設定します。エッジ ポートは、リンクをアップすると、ブロッキング ステートまたはラーニング ステートを経由しないで、直接フォワーディング ステートに移行します。デフォルトのスパニング ツリー ポートは、標準ポート タイプです。
	spanning-tree port type network default **例：** `switch(config)# spanning-tree port type network default`	レイヤ 2 スイッチおよびブリッジに接続しているすべてのインターフェイスを、スパニング ツリー ネットワーク ポートとして設定します。ブリッジ保証をイネーブルにすると、ネットワーク ポート上で自動的に実行されます。デフォルトのスパニング ツリー ポートは、標準ポート タイプです。 **(注)** レイヤ 2 ホストに接続しているインターフェイスをネットワーク ポートとして設定すると、これらのポートは自動的にブロッキング ステートに移行します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show spanning-tree** **例：** `switch# show spanning-tree`	（オプション）設定した STP ポート タイプを含む STP 設定を表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、レイヤ 2 ホストに接続しているすべてのアクセス ポートとトランク ポートを、スパニング ツリー エッジ ポートとして設定する例を示します。

```
switch# config t
switch(config)# spanning-tree port type edge default
switch(config)# exit
switch#
```

次に、レイヤ 2 スイッチまたはブリッジに接続しているすべてのポートを、スパニング ツリー ネットワーク ポートとして設定する例を示します。

```
switch# config t
switch(config)# spanning-tree port type network default
switch(config)#
```

特定のインターフェイス上でのスパニング ツリー エッジ ポートの設定

スパニング ツリー エッジ ポートは、特定のインターフェイス上に設定できます。スパニング ツリー エッジ ポートとして設定したインターフェイスは、リンクをアップすると、ブロッキング ステートまたはラーニング ステートを経由しないで、直接フォワーディング ステートに移行します。

このコマンドには、4 つのステートがあります。

- **spanning-tree port type edge** — アクセス ポート上でエッジの動作を明示的にイネーブルにします。
- **spanning-tree port type edge trunk** — トランク ポート上でエッジの動作を明示的にイネーブルにします。

（注） **spanning-tree port type edge trunk** コマンドを入力すると、アクセス モードであっても、ポートはエッジ ポートとして設定されます。

- **spanning-tree port type normal** — ポートを標準スパニング ツリー ポートとして明示的に設定します。フォワーディング ステートへの直接移行はイネーブルになりません。
- **no spanning-tree port type** — グローバル コンフィギュレーション モードで **spanning-tree port type edge default** コマンドがを定義した場合、エッジの動作をイネーブルにします。エッジ ポートをグローバルに設定しない場合、**no spanning-tree port type** コマンドは **spanning-tree port type normal** コマンドと同じです。

始める前に

スパニング ツリー ポート タイプを設定する前に、次のことを行う必要があります。

- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。
- STP が設定されていることを確認してください。
- インターフェイスがレイヤ 2 ホストに接続していることを確認してください。

手順の要約

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree port type edge** [**trunk**]
4. **exit**
5. **show spanning-tree**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	`config t`
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

	コマンド	目的

ステップ 2	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**spanning-tree port type edge** **例：** `switch(config-if)# spanning-tree port type edge`	指定したアクセス インターフェイスをスパニング ツリー エッジ ポートとして設定します。エッジ ポートは、リンクをアップすると、ブロッキング ステートまたはラーニング ステートを経由しないで、すぐにフォワーディング ステートに移行します。デフォルトのスパニング ツリー ポートは、標準ポート タイプです。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**show spanning-tree** **例：** `switch# show spanning-tree`	（オプション）設定した STP ポート タイプを含む STP 設定を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、イーサネット アクセス インターフェイス 1/4 をスパニング ツリー エッジ ポートとして設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree port type edge
switch(config)# exit
switch#
```

特定のインターフェイス上でのスパニング ツリー ネットワーク ポートの設定

スパニング ツリー ネットワーク ポートは、特定のインターフェイス上に設定できます。

ブリッジ保証は、スパニング ツリー ネットワーク ポート上でのみ実行されます。

このコマンドには、3 つのステートがあります。

- **spanning-tree port type network** — ポートをネットワーク ポートとして明示的に設定します。ブリッジ保証をグローバルでイネーブルにすると、スパニング ツリー ネットワーク ポート上で自動的に実行されます。
- **spanning-tree port type normal** — ポートを標準スパニング ツリー ポートとして明示的に設定します。このインターフェイス上ではブリッジ保証を実行できません。
- **no spanning-tree port type** — グローバル コンフィギュレーション モードで **spanning-tree port type network default** コマンドが定義された場合、ポートをスパニング ツリー ネットワーク ポートとして設定します。ブリッジ保証をグローバルでイネーブルにすると、このポート上で自動的に実行されます。

（注） レイヤ 2 ホストに接続しているポートをネットワーク ポートとして設定すると、自動的にブロッキング ステートに移行します。

始める前に

スパニング ツリー ポート タイプを設定する前に、次のことを行う必要があります。

- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。
- STP が設定されていることを確認してください。
- インターフェイスがレイヤ 2 スイッチまたはブリッジに接続していることを確認してください。

手順の要約

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree port type network**
4. **exit**
5. **show spanning-tree**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**spanning-tree port type network** **例：** `switch(config-if)# spanning-tree port type network`	指定したインターフェイスをスパニング ツリー ネットワーク ポートとして設定します。ブリッジ保証をイネーブルにすると、ネットワーク ポート上で自動的に実行されます。デフォルトのスパニング ツリー ポートは、標準ポート タイプです。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**show spanning-tree** **例：** `switch# show spanning-tree`	（オプション）設定した STP ポート タイプを含む STP 設定を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、イーサネット インターフェイス 1/4 をスパニング ツリー ネットワーク ポートとして設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree port type network
switch(config)# exit
switch#
```

BPDU ガードのグローバルなイネーブル化

BPDU ガードは、デフォルトでグローバルにイネーブル化できます。この設定では、BPDU を受信したエッジ ポートがシャットダウンされます。

（注） すべてのエッジ ポート上で BPDU ガードをイネーブルにすることを推奨します。

始める前に

この機能を設定する前に、次のことを行う必要があります。

- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。
- STP が設定されていることを確認してください。
- いくつかのスパニング ツリー エッジ ポートが設定されていることを確認してください。

手順の要約

1. **config t**
2. **spanning-tree port type edge bpduguard default**
3. **exit**
4. **show spanning-tree summary**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree port type edge bpduguard default** **例：** `switch(config)# spanning-tree port type edge bpduguard default`	すべてのスパニング ツリー エッジ ポート上で、デフォルトの BPDU ガードをイネーブルにします。デフォルトで、グローバル BPDU ガードはディセーブルです。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 4	**show spanning-tree summary** **例：** switch# show spanning-tree summary	（オプション）STP 情報の要約を表示します。
ステップ 5	**copy running-config startup-config** **例：** switch# copy running-config startup-config	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、すべてのスパニング ツリー エッジ ポート上で BPDU ガードをイネーブルにする例を示します。

```
switch# config t
switch(config)# spanning-tree port type edge bpduguard default
switch(config)# exit
switch#
```

特定のインターフェイス上での BPDU ガードのイネーブル化

指定したインターフェイス上で BPDU ガードをイネーブルに設定できます。BPDU ガードをイネーブルにすると、BPDU を受信した場合にポートがシャットダウンされます。

指定したインターフェイス上の BPDU ガードは、次のように設定できます。

- **spanning-tree bpduguard enable** — インターフェイス上で BPDU ガードを無条件でイネーブルにします。
- **spanning-tree bpduguard disable** — インターフェイス上で BPDU ガードを無条件でディセーブルにします。
- **no spanning-tree bpduguard** — インターフェイスが稼働中のエッジ ポートで、さらに **spanning-tree port type edge bpduguard default** コマンドが設定された場合にのみ、そのインターフェイス上で BPDU ガードをイネーブルにします。

始める前に

この機能を設定する前に、次のことを行う必要があります。

- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。
- STP が設定されていることを確認してください。

手順の要約

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree bpduguard** {**enable** | **disable**}
4. **exit**
5. **show spanning-tree summary**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**spanning-tree bpduguard** {**enable** | **disable**} **例：** `switch(config-if)# spanning-tree bpduguard enable`	指定したスパニング ツリー エッジ インターフェイスの BPDU ガードをイネーブルまたはディセーブルにします。デフォルトでは、インターフェイス上の BPDU ガードはディセーブルです。
	no spanning-tree bpduguard **例：** `switch(config-if)# no spanning-tree bpduguard`	**spanning-tree port type edge bpduguard default** コマンドの入力により、インターフェイスに設定されたデフォルトのグローバル BPDU ガード 設定に戻します。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 5	**show spanning-tree summary** **例：** `switch# show spanning-tree summary`	（オプション）STP 情報の要約を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、イーサネット エッジ ポート 1/4 で、BPDU ガードを明示的にイネーブルにする例を示します。

```
switch# config t
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpduguard enable
switch(config-if)# exit
switch(config)#
```

BPDU フィルタリングのグローバルなイネーブル化

スパニング ツリー エッジ ポート上で、BPDU フィルタリングをデフォルトでグローバルにイネーブル化できます。

BPDU フィルタリングがイネーブルであるエッジ ポートは、BPDU を受信するとエッジ ポートとしての稼働ステータスが失われ、通常の STP ステート移行を再開します。ただし、エッジ ポートとしてのポート設定は維持されます。

注意　このコマンドは、慎重に使用してください。このコマンドを誤って使用すると、ブリッジング ループの原因になります。

始める前に

この機能を設定する前に、次のことを行う必要があります。

- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。
- STP が設定されていることを確認してください。
- いくつかのスパニング ツリー エッジ ポートが設定されていることを確認してください。

（注） グローバルにイネーブル化した BPDU フィルタリングは、エッジ ポートとして稼働中のポートに*のみ*適用されます。ポートは、リンクアップ時にいくつかの BPDU を送信してから、発信 BPDU をフィルタリングします。エッジ ポート上で BPDU が受信されると、稼働 エッジ ポートとしてのステータスがすぐに失われ、BPDU フィルタリングはディセーブルになります。

手順の要約

1. **config t**
2. **spanning-tree port type edge bpdufilter default**
3. **exit**
4. **show spanning-tree summary**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree port type edge bpdufilter default** **例：** `switch(config)# spanning-tree port type edge bpdufilter default`	すべての稼働中のスパニング ツリー エッジ ポート上で、デフォルトの BPDU フィルタリングをイネーブルにします。デフォルトでは、グローバル BPDU フィルタリングはディセーブルです。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show spanning-tree summary** **例：** `switch# show spanning-tree summary`	（オプション）STP 情報の要約を表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、すべての稼働中のスパニング ツリー エッジ ポート上で BPDU フィルタリングをイネーブルにする例を示します。

```
switch# config t
switch(config)# spanning-tree port type edge bpdufilter default
switch(config)# exit
switch#
```

特定のインターフェイス上での BPDU フィルタリングのイネーブル化

指定したインターフェイスに BPDU フィルタリングを適用できます。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、そのインターフェイス上では BPDU は送信されず、受信したすべての BPDU がドロップされます。この BPDU フィルタリング機能は、トランキング モードかどうかに関係なく、インターフェイス全体に適用されます。

注意　特定のインターフェイスへの **spanning-tree bpdufilter enable** コマンドの入力は、慎重に行ってください。ホストに接続していないポートに BPDU フィルタリングを設定すると、そのポートは受信した BPDU をすべて無視してフォワーディングに移行するので、ブリッジング ループが発生することがあります。

このコマンドの入力により、指定したインターフェイスのポート設定を上書きすることができます。

このコマンドには、3 つのステートがあります。

- **spanning-tree bpdufilter enable** — インターフェイス上で BPDU フィルタリングを無条件でイネーブルにします。
- **spanning-tree bpdufilter disable** — インターフェイス上で BPDU フィルタリングを無条件でディセーブルにします。
- **no spanning-tree bpdufilter** — インターフェイスが稼働中のエッジ ポートで、さらに **spanning-tree port type edge bpdufilter default** コマンドが設定された場合にのみ、インターフェイスの BPDU フィルタリングをイネーブルにします。

始める前に

この機能を設定する前に、次のことを行う必要があります。

- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。
- STP が設定されていることを確認してください。

（注）　ポート上で BPDU フィルタリングをローカルでイネーブルにすると、そのポートでは BPDU が送受信されなくなります。

手順の要約

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree bpdufilter** {**enable** | **disable**}
4. **exit**

5. **show spanning-tree summary**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**spanning-tree bpdufilter** {**enable** | **disable**} **例：** `switch(config-if)# spanning-tree bpdufilter enable`	指定したスパニング ツリー エッジ インターフェイスの BPDU フィルタリングをイネーブルまたはディセーブルにします。デフォルトでは、BPDU フィルタリングはディセーブルです。
	no spanning-tree bpdufilter **例：** `switch(config-if)# spanning-tree bpdufilter enable`	インターフェイスが稼働中のスパニング ツリー エッジ ポートで、さらに **spanning-tree port type edge bpdufilter default** コマンドが入力された場合、インターフェイスの BPDU フィルタリングをイネーブルにします。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 5	**show spanning-tree summary** **例：** `switch# show spanning-tree summary`	（オプション）STP 情報の要約を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、イーサネット エッジ ポート 1/4 で、BPDU フィルタリングを明示的にイネーブルにする例を示します。

```
switch# config t
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpdufilter enable
switch(config-if)# exit
switch(config)#
```

ループ ガードのグローバルなイネーブル化

すべてのポイントツーポイント スパニング ツリー 標準ポートおよびネットワーク ポート上で、ループ ガードをデフォルトでグローバルにイネーブル化できます。ループ ガードは、エッジ ポート上では実行されません。

ループ ガードは、ブリッジ ネットワークに追加のセキュリティ機能を提供します。ループ ガードは、単方向リンク障害が発生した場合、代替ポートまたはルート ポートが指定ポートにならないように阻止します。

（注） インターフェイスを指定してループ ガードを適用すると、グローバルなループ ガード設定が上書きされます。

始める前に

この機能を設定する前に、次のことを行う必要があります。

- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。
- STP が設定されていることを確認してください。
- スパニング ツリーの標準ポートまたはいくつかのネットワーク ポートが設定されていることを確認してください。

手順の要約

1. **config t**
2. **spanning-tree loopguard default**
3. **exit**
4. **show spanning-tree summary**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**spanning-tree loopguard default** **例：** `switch(config)# spanning-tree loopguard default`	すべてのスパニング ツリー標準ポートおよびネットワーク ポート上で、デフォルトのループ ガードをイネーブルにします。デフォルトで、グローバル ループ ガードはディセーブルです。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show spanning-tree summary** **例：** `switch# show spanning-tree summary`	（オプション）STP 情報の要約を表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch# copy running-config startup-config`	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、すべてのスパニング ツリー標準ポートおよびネットワーク ポート上で、ループ ガードをイネーブルにする例を示します。

```
switch# config t
switch(config)# spanning-tree loopguard default
switch(config)# exit
switch#
```

特定のインターフェイス上でのループ ガードまたはルート ガードのイネーブル化

（注） ループ ガードは、スパニング ツリー標準ポートまたはネットワーク ポート上で実行できます。ルート ガードは、すべてのスパニング ツリー ポート（標準、エッジ、またはネットワーク）で実行できます。

指定したインターフェイス上で、ループ ガードまたはルート ガードのどちらかをイネーブルに設定できます。

ループ ガードは、共有リンクまたはポイントツーポイント リンク上のインターフェイス単位でイネーブルに設定できます。

ポート上でルート ガードをイネーブルにすることは、そのポートをルート ポートにできないことを意味します。ループ ガードは、単方向リンクの障害発生時に、代替ポートまたはルート ポートが指定ポートになるのを防止します。

インターフェイス上でイネーブルにしたループ ガードおよびルート ガードは、そのインターフェイスが属すすべての VLAN に適用されます。

（注） インターフェイスを指定してループ ガードを適用すると、グローバルなループ ガード設定が上書きされます。

始める前に

この機能を設定する前に、次のことを行う必要があります。

- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。
- STP が設定されていることを確認してください。
- ループ ガードを設定する対象が、スパニング ツリー標準ポートまたはネットワーク ポートであることを確認してください。

手順の要約

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree guard** {**loop** | **root** | **none**}
4. **exit**
5. **show spanning-tree summary**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t switch(config)#	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** *type slot/port* **例：** switch(config)# interface ethernet 1/4 switch(config-if)#	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree guard** {**loop** | **root** | **none**} **例：** switch(config-if)# spanning-tree guard loop	指定したインターフェイス上でループ ガードまたはルート ガードをイネーブルまたはディセーブルにします。デフォルトでは、ルート ガードはディセーブルです。指定したポートのループ ガードもディセーブルです。 **（注）** ループ ガードが実行されるのは、スパニング ツリーの標準インターフェイスおよびネットワーク インターフェイス上だけです。 この例では、指定したインターフェイス上でループ ガードをイネーブルにしています。
ステップ 4	**exit** **例：** switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 5	**interface** *type slot/port* **例：** switch(config)# interface ethernet 1/10 switch(config-if)#	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 6	**spanning-tree guard** {**loop** | **root** | **none**} **例：** switch(config-if)# spanning-tree guard root	指定したインターフェイス上でループ ガードまたはルート ガードをイネーブルまたはディセーブルにします。デフォルトでは、ルート ガードはディセーブルです。指定したポートのループ ガードもディセーブルです。 この例では、別のインターフェイス上でルート ガードをイネーブルにしています。
ステップ 7	**exit** **例：** switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 8	**show spanning-tree summary** **例：** switch# show spanning-tree summary	（オプション）STP 情報の要約を表示します。
ステップ 9	**copy running-config startup-config** **例：** switch(config)# copy running-config startup-config	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、イーサネット ポート 1/4 上でルート ガードをイネーブルにする例を示します。

```
switch# config t
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree guard root
switch(config-if)# end
switch(config)#
```

PVST シミュレーションのグローバル設定

（注） PVST シミュレーションは、デフォルトでイネーブルです。デフォルトでは、デバイス上のすべてのインターフェイスで MST と Rapid PVST+ が相互運用されます。

MST は、Rapid PVST+ と相互運用します。ただし、デフォルトの STP モードで、MST を実行していないデバイスに接続する可能性を防ぐには、この自動機能をディセーブルに設定できます。PVST シミュレーションをディセーブルにすると、Rapid PVST+ イネーブル ポートに接続したことが検出された時点で、MST イネーブル ポートはブロッキング ステートに移行します。このポートは、BPDU を受信しなくなるまでは不整合ステートのままですが、そのあとは標準 STP のステート移行を再開します。

この自動機能は、グローバルまたはポート単位でブロックできます。グローバル コマンドを入力し、インターフェイス コマンド モードでデバイス全体の PVST シミュレーション設定を変更できます。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **no spanning-tree mst simulate pvst global**
3. **exit**
4. **show spanning-tree detail**
5. **copy running-config startup-config**

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**no spanning-tree mst simulate pvst global** **例：** `switch(config)# no spanning-tree mst simulate pvst global`	スイッチ上のすべてのインターフェイスで、Rapid PVST+ モードを実行している接続先デバイスとの自動的な相互運用をディセーブルにします。この機能はデフォルトではイネーブルです。デフォルトでは、デバイス上のすべてのインターフェイスが、Rapid PVST+ と MST の間で運用されます。

	コマンド	目的
ステップ 3	**exit** **例：** switch(config)# exit switch#	コンフィギュレーション モードを終了します。
ステップ 4	**show spanning-tree detail** **例：** switch# show spanning-tree detail	（オプション）STP 情報の詳細を表示します。
ステップ 5	**copy running-config startup-config** **例：** switch(config)# copy running-config startup-config	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、Rapid PVST+ を実行している接続先デバイスとの自動的な相互運用を回避する例を示します。

```
switch# config t
switch(config)# no spanning-tree mst simulate pvst global
switch(config)#
```

ポート単位での PVST シミュレーションの設定

（注） PVST シミュレーションは、デフォルトでイネーブルです。デフォルトでは、デバイス上のすべてのインターフェイスで MST と Rapid PVST+ が相互運用されます。

PVST シミュレーションを設定できるのは、デバイス上で MST を実行している場合だけです（Rapid PVST+ がデフォルトの STP モードです）。MST は、Rapid PVST+ と相互運用します。ただし、デフォルトの STP モードで、MST を実行していないデバイスに接続する可能性を防ぐには、この自動機能をディセーブルに設定できます。PVST シミュレーションをディセーブルにすると、Rapid PVST+ イネーブル ポートに接続したことが検出された時点で、MST イネーブル ポートはブロッキング ステートに移行します。このポートは、Rapid PVST+ BPDU を受信しなくなるまで不整合ステートのままですが、そのあとは標準 STP のステート移行を再開します。

この自動機能は、グローバルまたはポート単位でブロックできます。

始める前に

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。

手順の要約

1. **config t**
2. **interface** {{*type slot/port*} | {**port-channel** *number*}}
3. **spanning-tree mst simulate pvst disable**
4. **exit**
5. **show spanning-tree detail**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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** {{*type slot/port*} | {**port-channel** *number*}}
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**spanning-tree mst simulate pvst disable** **例：** `switch(config-if)# spanning-tree mst simulate pvst`	指定したインターフェイスで、Rapid PVST+ モードを実行している接続先デバイスとの自動的な相互運用をディセーブルにします。 デフォルトでは、デバイス上のすべてのインターフェイスで Rapid PVST+ と MST が相互運用されます。
	spanning-tree mst simulate pvst **例：** `switch(config-if)# spanning-tree mst simulate pvst`	指定したインターフェイスで、MST と Rapid PVST+ のシームレスな相互運用を再びイネーブルにします。
	no spanning-tree mst simulate pvst **例：** `switch(config-if)# no spanning-tree mst simulate pvst`	インターフェイスに、**spanning-tree mst simulate pvst global** コマンドで設定したデバイス全体での MST と Rapid PVST+ の相互運用を適用します。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 5	**show spanning-tree detail** **例：** `switch# show spanning-tree detail`	（オプション）STP 情報の詳細を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（オプション）実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、指定したインターフェイスで、MST を実行していない接続先デバイスとの自動的な相互運用を回避する例を示します。

```
switch(config-if)# spanning-tree mst simulate pvst
switch(config-if)#
```

STP 拡張機能の設定の確認

STP 拡張機能の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config spanning-tree [**all**]	STP の情報を表示します。
show spanning-tree summary	STP 情報の要約を表示します。
show spanning-tree mst *instance-id* **interface** {**ethernet** *slot/port* | **port-channel** *channel-number*} [**detail**]	指定したインターフェイスおよびインスタンスの MST 情報を表示します。

これらのコマンドの出力フィールドの詳細については、『*Cisco NX-OS Layer 2 Switching Command Reference*』を参照してください。

STP 拡張機能の設定例

次に、STP 拡張機能を設定する例を示します。

```
switch# configure terminal
switch(config)# spanning-tree port type network default
switch(config)# spanning-tree port type edge bpduguard default
switch(config)# spanning-tree port type edge bpdufilter default
switch(config)# interface Ethernet1/1
switch(config-if)# spanning-tree port type edge
switch(config-if)# exit
switch(config)# interface Ethernet1/2
switch(config-if)# spanning-tree port type edge
switch(config-if)# exit
switch(config)#
```

デフォルト設定

表 7-2 に、STP 拡張機能のデフォルト設定を示します。

表 7-2　STP 拡張機能パラメータのデフォルト設定

パラメータ	デフォルト
ポート タイプ	標準
ブリッジ保証	イネーブル（STP ネットワーク ポートのみ）
グローバル BPDU ガード	ディセーブル
インターフェイス単位の BPDU ガード	ディセーブル
グローバル BPDU フィルタリング	ディセーブル
インターフェイス単位の BPDU フィルタリング	ディセーブル
グローバル ループ ガード	ディセーブル
インターフェイス単位のループ ガード	ディセーブル
インターフェイス単位のルート ガード	ディセーブル
PVST シミュレーション	イネーブル **（注）** デバイスで MST と Rapid PVST+ の相互運用をディセーブルにする手順は、「PVST シミュレーション」（p.7-8）を参照してください。

追加情報

STP 拡張機能の実装に関する追加情報は、次のセクションを参照してください。

- 関連資料（p.7-30）
- 標準規格（p.7-30）
- MIB（p.7-30）

関連資料

関連トピック	マニュアル名
Rapid PVST+	第 5 章「Rapid PVST+ の設定」
MST	第 6 章「MST の設定」
コマンド リファレンス	『*Cisco NX-OS Layer 2 Switching Command Reference*』
DCNM レイヤ 2 スイッチング コンフィギュレーション	『*Cisco DCNM Layer 2 Switching Configuration Guide*』
レイヤ 2 インターフェイス	『*Cisco NX-OS Interfaces Configuration Guide*』
NX-OS の基本情報	『*Cisco NX-OS Security Configuration Guide*』
ハイ アベイラビリティ	『*Cisco NX-OS High Availability and Redundancy Guide*』
システム管理	『*Cisco NX-OS System Management Configuration Guide*』
VDC	『*Cisco NX-OS Virtual Device Context Configuration Guide*』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco NX-OS Release Notes*』 Release 4.0

標準規格

標準規格	タイトル
IEEE 802.1Q-2006（従来の IEEE 802.1s）、IEEE 802.1D-2004（従来の IEEE 802.1w）、IEEE 802.1D、IEEE 802.1t	—

MIB

MIB	MIB リンク
• CISCO_STP_EXTENSION MIB • BRIDGE MIB	次の URL から、MIB の検索およびダウンロードができます。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

APPENDIX **A**

Cisco NX-OS Release 4.0 レイヤ 2 スイッチング機能の設定の上限

NX-OS でサポートされている機能には、設定の上限があります。表 A-1 に、NX-OS Release 4.0 が稼働するレイヤ 2 デバイスの設定の上限を示します。

表 A-1　Cisco NX-OS Release 4.0 のレイヤ 2 設定の上限

機能	上限
MAC アドレス	131,060
MAC エージング タイム値	14
VLAN	VDC ごとに 4000
	75,000 個の VLAN ポート
Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）	65 個の MST Instance（MSTI; MST インスタンス）（インスタンス 0 を含む）
	VDC ごとに 4000 個の Rapid PVST+
	モジュールごとに 6500 個の Rapid PVST+ 論理ポート
	システムごとに 16,000 個の Rapid PVST+ 論理ポート
	モジュールごとに 12,000 個の MST 論理ポート
	システムごとに 75,000 個の MST 論理ポート

INDEX

B

BPDU
- M レコード 6-4
- MST 6-4
- MST 領域 6-5
- Rapid PVST+ 5-6, 5-9
- TC 時間タイマー 5-8
- エッジ ポート 7-3
- 交換の結果 5-6
- 説明 5-6
- バージョン 5-10, 6-7, 6-10
- ブリッジ保証 7-3
- ポート チャネル 7-10
- ホップ カウント 6-8
- 優位 7-7

BPDU ガード
- インターフェイス単位のイネーブル化 7-17
- グローバルなイネーブル化 7-16
- 説明 7-5
- デフォルト設定 7-29
- プライベート VLAN ポート 4-9

BPDU フィルタリング
- インターフェイス単位のイネーブル化 7-20
- エッジ ポート 7-6
- グローバル 7-6
- グローバルなイネーブル化 7-18
- 説明 7-6
- デフォルト設定 7-29
- ポート単位 7-6

Bridge Protocol Data Unit、BPDU を参照

C

CIST
- 説明 6-5

CIST リージョナル ルート 6-6

Common And Internal Spanning Tree、CIST を参照

Common Spanning Tree、CST を参照

CST
- 説明 6-5

H

hello タイム
- MST の設定 6-33
- VLAN 単位の RPVST+ の設定 5-32
- 説明 5-11

I

IEEE 802.1D
- 用語 5-2

IEEE 802.1s
- 用語 5-2

IEEE 802.1w
- 用語 5-2

Internal Spanning Tree、IST を参照

IST
- BPDU 6-4
- MST 6-3
- 説明 6-5

M

MAC アドレス
- エージング タイム 2-3
- 制限 2-4
- 注意事項 2-4
- テーブルの説明 2-3

MAC アドレス テーブル
- 確認 2-8
- クリア 2-7
- スタティック アドレス 2-3, 2-5
- ダイナミックな構築 2-3

MAC アドレス リダクション
- MST 6-3

Rapid PVST+ 5-5
MIB
MST 6-44
Rapid PVST+ 5-40
STP 拡張機能 7-30
VLAN 4-24
プライベート VLAN 4-24
MST
BPDU 6-4, 6-7, 6-8
CIST リージョナル ルート 6-6
IEEE 802.1D との相互運用性 6-10
IEEE 802.1w 6-3
MST コンフィギュレーション モード 6-16
Rapid PVST+ との相互運用 7-8
VDC 6-11, 6-15
VLAN/MST マッピング 6-3, 6-4, 6-23
イネーブル化 6-15
インスタンス 6-3
確認 6-40
境界ポート 6-8
コンフィギュレーション情報 6-3
最大エージング タイム 6-8
最大ホップ カウント 6-8
制約事項 6-13
セカンダリ ルート 6-27
設定
スイッチ プライオリティ 6-29
設定例 6-41
説明 6-2 - 6-10
先行標準 MSTP との相互運用性 6-10
他の機能との相互運用性 6-13
注意事項 6-13
デフォルト設定 6-43
デフォルト値の設定 6-22
統計情報 6-40
トラブルシューティング 6-26
名前 6-4
プライベート VLAN 6-24
プロトコル移行 6-10
プロトコルの再初期化 6-38
ポート プライオリティ 6-30
ライセンス 6-12
リビジョン番号 6-3, 6-4
リビジョン番号の設定 6-19
領域の指定 6-20
領域名の設定 6-16, 6-18
ルート ブリッジ 7-8
ルート ブリッジの設定 6-26
MST インスタンス
数 6-3
MST 領域
サポートされているスパニング ツリー インスタンス 6-3
説明 6-3
Multiple Spanning Tree Protocol、MST を参照

P

PortFast
エッジ ポート 7-3
PVST シミュレーション
インターフェイス単位の設定 7-26
グローバル設定 7-25
説明 7-8
デフォルト設定 7-29
ルート ブリッジ 7-8

R

Rapid per VLAN Spanning Tree +、Rapid PVST+ を参照
Rapid PVST+
BPDU 5-9
IEEE 802.1D との相互運用性 5-2, 5-9, 5-18
IEEE 802.1Q との相互運用性 5-2, 5-17
IEEE 802.1s との相互運用性 5-18
MST との相互運用 7-8
MST との相互運用性 5-18
VDC 5-19
VLAN 単位 5-2
VLAN 単位のイネーブル化 5-23
VLAN プライオリティ 5-28
イネーブル化 5-21
確認 5-37
期限切れ 5-8
高速コンバージェンス 5-8
指定ポート 5-8
制約事項 5-20
セカンダリ ルート 5-26
設定例 5-37
説明 5-8 - 5-18
他の機能との相互作用 5-20
注意事項 5-20

デフォルト設定 5-38
統計情報 5-37
トポロジ変更 5-9
トラブルシューティング 5-25
プロトコル タイマー 5-11
プロトコルの再初期化 5-36
ポートの移行 5-11
ライセンス 5-20
ルート スイッチ 5-8
ルート ブリッジの設定 5-24
RSTP
BPDU 5-15
アクティブ トポロジ 5-12
高速コンバージェンス 5-8

S

STP
BPDU 5-3
MAC アドレス リダクション 5-5
MST 6-3
PortFast 5-8, 7-2
VLAN 単位 5-2
異議メカニズム 5-16, 6-9
エッジ ポート 5-8, 7-2
説明 5-3 - 5-7
デフォルト モード 5-2, 6-15
トポロジ 5-3, 5-7, 7-7
トラブルシューティング 5-24, 7-7
ネットワーク ポート 7-3
バーチャライゼーション 5-2, 5-19, 6-11
パス コスト 5-6
複数のインスタンス 5-19, 6-11
プライベート VLAN 4-9
ブリッジング ループ 5-3
プロトコル移行 5-18
ポート ステート 5-12
ポート ロール 5-11
用語 5-2
ルート ブリッジ 5-6
ルート ポート 5-6
STP 拡張機能
確認 7-28
制限 7-10
設定例 7-28
説明 7-2 - 7-8
注意事項 7-10
デフォルト設定 7-29
バーチャライゼーション 7-9
ベスト プラクティス 7-7
ライセンス 7-9
STP ポート タイプ
説明 7-2
デフォルト設定 7-29
スパニング ツリー プロトコル STP を参照
SVI
VLAN インターフェイス 3-3

U

UDLD
MST 6-9
Rapid PVST+ 5-16
ループ ガード 7-10
Unidirectional Link Detection、UDLD を参照

V

VDC
MAC アドレス テーブル 2-3
MST 6-11
Rapid PVST+ 5-19
STP 拡張機能 7-9
VLAN 3-6
障害分離 1-5
バーチャライゼーション 1-5
プライベート VLAN 4-8
ユーザ ロール 1-5
ライセンス 2-4
リソース 1-5
レイヤ 2 スイッチング機能 1-5
Virtual Device ContextVDC を参照
VLAN
Rapid PVST+ 5-2
SVI 3-3
拡張システム ID 3-4
削除 3-5, 3-8
作成 3-8, 3-9
制約事項 3-7
設定の確認 3-12
説明 3-2 - 3-6
注意事項 3-7

デフォルト設定　3-13
バーチャライゼーション　3-6
変更　3-9
ポートの割り当て　3-5
予約範囲　3-4
ライセンス　3-7
VLAN インターフェイス
VLAN 間の通信　3-3
イネーブル化　4-5
トラブルシューティング　4-7
プライベート VLAN　4-7, 4-17
VLAN コンフィギュレーション サブモード
コマンドの実行　3-5
使用　3-9
VLAN ステート
設定　3-11
VLAN 統計情報
クリア　3-13
表示　3-13
VLAN トラフィック
配信　3-2
ルーティング　3-3
VLAN の作成
デフォルトのステート　3-5
VLAN の設定
例　3-13
VLAN の範囲
説明　3-4
VLAN の変更
許可されるパラメータ　3-5
VLAN 番号
許可される番号　3-4
再使用　3-6
範囲　3-7
予約範囲　3-4
VLAN プライオリティ
Rapid PVST+　5-17
設定　5-28
VLAN 名
設定　3-11
VTP
モード　3-2

あ

アクセス ポート
作成　3-5

い

インスタンス
MST　6-3

え

エッジ ポート
PortFast　7-3
Rapid PVST+　5-8
インターフェイス単位の設定　7-13
グローバル設定　7-11
説明　7-3

か

拡張システム ID
VLAN　3-4
確認
MAC アドレス テーブル　2-8
MST　6-40
Rapid PVST+　5-37
STP 拡張機能　7-28
VLAN　3-12
プライベート VLAN　4-22
仮想 LAN
VLAN を参照
関連資料　xiv

き

境界ポート
STP　6-8

こ

コミュニティ VLAN
説明　4-4
プライベート VLAN　4-4

コミュニティ ポート
プライベート VLAN 4-4

さ

サービス リクエスト
リクエスト xv
最大エージング タイム
VLAN 単位の RPVST+ の設定 5-34
説明 5-11

し

指定ポート
BPDU 5-9
Rapid PVST+ 5-8
説明 5-11
上限
説明（表） A-1
資料
追加資料 xiv

す

スイッチ プライオリティ
MST 6-29
スタティック MAC アドレス
追加 2-3, 2-5
例 2-8

せ

制限
STP 拡張機能 7-10
プライベート VLAN 4-9
制約事項
MST 6-13
Rapid PVST+ 5-20
セカンダリ VLAN 4-3
VLAN インターフェイスへのマッピング 4-17
コミュニティ 4-3
独立 4-3
プライマリ VLAN との関連付け 4-4, 4-6, 4-15
設定の上限
説明（表） A-1

た

代替ポート
説明 5-11
ダイナミック MAC アドレス
クリア 2-7
追加 2-3
代表スイッチ
説明 5-11
代表ブリッジ
説明 5-6
タイマー
STP 5-11

ち

注意事項
MAC アドレス 2-4
MST 6-13
Rapid PVST+ 5-20
STP 拡張機能 7-10
VLAN 3-7
プライベート VLAN 4-9, 4-12
直径
説明 5-25

て

提案合意ハンドシェイク
BPDU 5-9
Rapid PVST+ 5-10
デフォルト設定
MST 6-43
Rapid PVST+ 5-38
STP 5-2
STP 拡張機能 7-29
VLAN 3-13
プライベート VLAN 4-23
レイヤ 2 スイッチング 2-9
転送遅延時間
MST の設定 6-34
VLAN 単位の RPVST+ の設定 5-33
説明 5-11

と

統計情報
  MST 6-40
  Rapid PVST+ 5-37
  VLAN 3-13
  プライベート VLAN 4-22
独立 VLAN
  セカンダリ プライベート VLAN 4-3
  定義 4-4
  プライマリ VLAN 4-4
独立ポート
  プライベート VLAN 4-4
トランク ポート
  エッジ ポートとして設定 7-13
  作成 3-5

ね

ネットワーク ポート
  インターフェイス単位の設定 7-14
  グローバル設定 7-11
  説明 7-3
  ブリッジ保証 7-3

は

バーチャライゼーション
  STP 5-2, 5-19, 6-11
  STP 拡張機能 7-9
  VDC 1-5
  VLAN 3-6
  プライベート VLAN 4-8
パス コスト
  説明 5-6
パスコスト方式
  MST 6-10, 6-31
  Rapid PVST+ 5-16
  設定 5-30
バックアップ ポート
  説明 5-11

ふ

フォワーディング ポート ステート
  説明 5-13
プライベート VLAN 4-4
  MST マッピング 6-24
  STP 4-9
  SVI 4-7
  VLAN インターフェイス 4-2, 4-5, 4-7, 4-17
  アソシエーション 4-15, 4-19, 4-20, 4-23
    動作可能 4-6
    変更 4-6
  イネーブル化 4-2, 4-13
  確認 4-22
  コミュニティ VLAN 4-3, 4-4, 4-14
  制限 4-9
  セカンダリ VLAN 4-3
  設定 4-14
    セカンダリ VLAN 入力トラフィックのルーティング 4-17
  設定時の注意事項 4-10
  設定例 4-23
  説明 4-2 - 4-7
  他の機能との相互作用 4-9
  端末へのアクセス 4-7
  注意事項 4-9, 4-12
  通信 4-2, 4-7
  ディセーブル化 4-2
  デフォルト設定 4-23
  統計情報 4-22
  独立 VLAN 4-3, 4-4, 4-14
  トラフィックの配信 4-17
  トラブルシューティング 4-2
  バーチャライゼーション 4-8
  複数デバイスにまたがる 4-7
  プライベート VLAN 外との通信 4-5
  プライベート VLAN のアソシエーション 4-6
  プライマリ VLAN 4-3, 4-14
  ブロードキャスト ドメイン 4-2
  ブロードキャスト トラフィック 4-6
  ポート
    コミュニティ 4-4
    設定時の注意事項 4-10
    独立 4-4
    無差別 4-4
  マッピング 4-7, 4-17, 4-23
  ライセンス 4-8
  利点 4-3
  ルーティング 4-2

プライベート VLAN ポート
BPDU ガード 4-9
コミュニティ ポート 4-4, 4-19
制限 4-10
独立ポート 4-4, 4-19
トラフィックの配信 4-5
トランク ポート 4-4
ブロードキャスト トラフィック 4-6
無差別ポート 4-4, 4-20
PVLAN プライベート VLAN を参照
プライマリ VLAN
セカンダリ VLAN との関連付け 4-4, 4-6, 4-15
トラフィックの配信 4-5
プライベート VLAN 4-3, 4-4
無差別ポート 4-5
ブリッジ ID
拡張システム ID 5-4
ブリッジ保証
サポートされるプロトコルとリンク タイプ 7-3
説明 7-3 - 7-5
デフォルト設定 7-29
ネットワーク ポート 7-3
ブリッジング ループ
STP 5-3
ループ ガード 7-6
ブロードキャスト トラフィック
VLAN 3-2
プライベート VLAN 4-6
ブロッキング ポート ステート
説明 5-12
プロトコルの再初期化
MST 6-38
Rapid PVST+ 5-36

ほ

ポート
エッジ ポート 7-11
ネットワーク ポート 7-11
標準ポート 7-11
レイヤ 2 4-2, 4-4, 4-10, 5-8, 7-2
ポート コスト
値 5-16, 6-10
設定 5-30, 6-31
ポート ステート
STP 5-12
ポート チャネル
BPDU 7-10
STP 7-10
ポート プライオリティ
MST の設定 6-30
Rapid PVST+ 5-17
Rapid PVST+ 用の設定 5-29
ポート ロール
STP 5-11
ホスト ポート 4-4
エッジ ポート 5-8, 7-3
設定 4-19
プライベート VLAN 4-4, 4-6, 4-19

ま

マッピング
プライベート VLAN 4-7
マルチキャスト トラフィック
VLAN 3-2

む

無差別ポート 4-4
コミュニティ VLAN 4-5
設定 4-20
独立 VLAN 4-5
プライマリ VLAN 4-5
プライマリ VLAN 内の数 4-5

ら

ラーニング ポート ステート
説明 5-13
ライセンス
MST 6-12
Rapid PVST+ 5-20
STP 拡張機能 7-9
VDC 2-4
VLAN 3-7
プライベート VLAN 4-8
レイヤ 2 スイッチング 2-4

り

デフォルト値　2-9

リンク タイプ
　Rapid PVST+　5-8
　設定　5-35, 6-37
　ポイントツーポイント　5-8
リンク障害
　単一方向の検出　5-16, 6-9

る

ルート ガード
　イネーブル化　7-23
　説明　7-7
　デフォルト設定　7-29
ルート ブリッジ
　MST　7-8
　MST の設定　6-26
　PVST シミュレーション　7-8
　Rapid PVST+ 用の設定　5-24
　選定　5-6
　複数のバックアップ　5-26
　ルート ガード　7-7
ルート ポート
　BPDU　5-9
　説明　5-6, 5-11
ループ ガード
　インターフェイス単位のイネーブル化　7-23
　グローバルなイネーブル化　7-21
　説明　7-6
　デフォルト設定　7-29
　リンク タイプ　7-7

れ

例
　MST　6-41
　Rapid PVST+　5-37
　STP 拡張機能　7-28
　VLAN の設定　3-13
　スタティック MAC アドレス　2-8
　プライベート VLAN　4-23
レイヤ 2 スイッチング
　VDC　2-3
　イーサネット スイッチング　2-2
　説明　2-2 - 2-3