



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

August 21, 2008

**【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, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; 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, MeetingPlace Chime Sound, 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. (0807R)

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 DCNM 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 © 2009, シスコシステムズ合同会社 .
All rights reserved.



CONTENTS

追加および変更された情報 xi

はじめに xiii

対象読者 xiii

マニュアルの構成 xiv

表記法 xiv

関連資料 xv

マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン
xvi

シスコのテクニカル サポート xvi

Service Request ツールの使用 xvi

その他の情報の入手方法 xvii

CHAPTER 1

概要 1-1

VLAN 1-2

プライベート VLAN 1-2

スパンニング 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

VLAN の設定 2-1

VLAN について 2-2

VLAN の概要 2-2

VLAN の範囲 2-4

VLAN の作成、削除、および変更 2-5

ハイ アベイラビリティ 2-6

バーチャライゼーションのサポート 2-6

VLAN のライセンス要件 2-7

VLAN 設定の前提条件 2-7

注意事項および制約事項 2-7

VLAN の設定	2-8
VLAN の作成および削除	2-8
VLAN の基本設定の変更	2-10
統計情報の表示	2-11
VLAN 設定のフィールドの説明	2-11
Device ビュー : デバイス : グローバル設定 : Global Settings セクション	2-11
Device ビュー : VLAN : VLAN の詳細 : VLAN Settings セクション	2-12
Device ビュー : VLAN : VLAN の詳細 : Advanced Settings セクション	2-16
Device ビュー : VLAN : 標準 VLAN の VLAN ポート : Access Ports セクション	2-16
Device ビュー : VLAN : 標準 VLAN の VLAN ポート : Trunk Ports セクション	2-16
Device ビュー : VLAN : プライマリ VLAN のプライマリ VLAN ポート : Promiscuous Ports セクション	2-17
Device ビュー : VLAN : セカンダリ VLAN の Secondary VLAN Ports タブ : PVLAN Host Ports セクション	2-17
Network ビュー : デバイス : VLAN の詳細 : VLAN Settings セクション	2-18
Network ビュー : デバイス : VLAN の詳細 : Advanced Settings セクション	2-19
Network ビュー : デバイス : VLAN ポート : Access Ports セクション	2-19
Network ビュー : デバイス : VLAN ポート : Trunk Ports セクション	2-19
Network ビュー : デバイス : プライマリ VLAN ポート : Promiscuous Ports セクション	2-20
Network ビュー : デバイス : セカンダリ VLAN ポート : PVLAN Host Ports セクション	2-20
追加情報	2-21
関連資料	2-21
標準規格	2-21
MIB	2-21

CHAPTER 3

プライベート VLAN の設定 3-1

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

プライベート VLAN ポートの分離	3-7
プライベート VLAN および VLAN インターフェイス	3-7
複数のデバイスにまたがるプライベート VLAN	3-7
ハイ アベイラビリティ	3-8
バーチャライゼーションのサポート	3-8
プライベート VLAN のライセンス要件	3-8
プライベート VLAN の前提条件	3-8
注意事項および制約事項	3-9
セカンダリ VLAN およびプライマリ VLAN の設定	3-9
プライベート VLAN ポートの設定	3-10
他の機能に関連する制限	3-10
プライベート VLAN の設定	3-12
プライベート VLAN の設定時の注意事項	3-12
プライベート VLAN のイネーブル化	3-13
プライベート VLAN としての VLAN の設定	3-14
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	3-15
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	3-16
プライベート VLAN ホスト ポートとプライベート VLAN 無差別ポートの設定	3-18
プライベート VLAN の統計情報の表示	3-19
フィールドの説明	3-19
追加情報	3-20
関連資料	3-20
標準規格	3-20
MIB	3-20

CHAPTER 4

Rapid PVST+ の設定	4-1
Rapid PVST+ について	4-2
STP	4-3
概要	4-3
トポロジの作成方法	4-4
ブリッジ ID	4-4
BPDU	4-6
ルート ブリッジの選定	4-7
スパンニング ツリー トポロジの作成	4-7
Rapid PVST+	4-8
概要	4-8
Rapid PVST+ BPDU	4-9

提案合意ハンドシェイク	4-10
プロトコル タイマー	4-11
ポート ロール	4-12
ポート ステート	4-13
ポート ロールの同期化	4-15
単一方向リンク障害の検出	4-16
ポート コスト	4-17
ポート プライオリティ	4-17
Rapid PVST+ および IEEE 802.1Q トランク	4-18
Rapid PVST+ とレガシー 802.1D STP の相互運用性	4-18
Rapid PVST+ と 802.1s MST の相互運用性	4-18
ハイ アベイラビリティ	4-19
バーチャライゼーションのサポート	4-19
Rapid PVST+ のライセンス要件	4-20
Rapid PVST+ を設定するための前提条件	4-20
注意事項および制約事項	4-21
Rapid PVST+ の設定	4-22
Rapid PVST+ のイネーブル化	4-23
デバイスのすべての STP パラメータをデフォルト値に設定	4-24
Rapid PVST+ の VLAN 単位でのディセーブル化またはイネーブル化	4-25
プライマリおよびセカンダリ ルートとスイッチ プライオリティの設定	4-26
Rapid PVST+ ポート プライオリティの設定	4-28
Rapid PVST+ パスコスト方式およびポート コストの設定	4-28
インターフェイス別にすべての Rapid PVST+ パラメータをデフォルト値に設定	4-30
VLAN の Rapid PVST+ hello タイムの設定	4-32
VLAN の Rapid PVST+ 転送遅延時間の設定	4-33
VLAN の Rapid PVST+ 最大エージング タイムの設定	4-33
リンク タイプの指定	4-34
統計情報の表示	4-35
Rapid PVST+ のフィールドの説明	4-35
Device ビュー : VLAN : Details : VLAN Setting セクション	4-35
Device ビュー : VLAN : Details : Port Setting セクション	4-36
Network ビュー : デバイス : Details : VLAN Setting セクション	4-36
Network ビュー : デバイス : Details : Port Setting セクション	4-37
追加情報	4-38
関連資料	4-38
標準規格	4-38

MIB 4-38

CHAPTER 5

MST の設定 5-1

MST について	5-3
MST の概要	5-3
MST 領域	5-4
MST BPDU	5-5
MST コンフィギュレーション情報	5-5
IST、CIST、および CST	5-6
IST、CIST、および CST の概要	5-6
MST 領域内のスパンニング ツリー動作	5-6
MST 領域間のスパンニング ツリー動作	5-7
MST 用語	5-8
ホップ カウント	5-8
境界ポート	5-9
単一方向リンク障害の検出	5-9
ポート コストおよびポート プライオリティ	5-10
IEEE 802.1D との相互運用性	5-11
ハイ アベイラビリティ	5-11
バーチャライゼーションのサポート	5-12
MST のライセンス要件	5-13
MST の前提条件	5-13
注意事項および制約事項	5-14
MST の設定	5-15
MST のイネーブル化	5-15
MST 名およびリビジョンの指定	5-17
MST のデフォルト値への設定	5-17
MST インスタンスの追加およびインスタンスと VLAN のマッピング	5-18
MST インスタンスの削除	5-20
VLAN と MSTI のマッピングおよびマッピング解除	5-21
プライマリおよびセカンダリ ルートとスイッチ プライオリティの設定	5-22
ポート プライオリティおよび MST ポートのコストの設定	5-23
ポートごとのデフォルト MST 値の設定	5-24
hello タイム、転送遅延時間、最大エージング タイム、最大ホップ カウントの設定	5-25
リンク タイプの指定	5-26
統計情報の表示	5-26
MST のフィールドの説明	5-27

Device ビュー : インスタンス : Details : MST Settings セクション	5-27
Device ビュー : インスタンス : Details : Access Ports セクション	5-28
Device ビュー : インスタンス : Details : Trunk Ports セクション	5-29
Network ビュー : デバイス : Details : MST Settings セクション	5-30
Network ビュー : デバイス : Details : Access Ports セクション	5-30
Network ビュー : デバイス : Details : Trunk Ports セクション	5-31
追加情報	5-32
関連資料	5-32
標準規格	5-32
MIB	5-32

CHAPTER 6

STP 拡張機能の設定 6-1

STP 拡張機能の概要	6-2
STP ポート タイプ	6-3
STP エッジ ポート	6-3
ブリッジ保証	6-3
BPDU ガード	6-6
BPDU フィルタリング	6-6
ループ ガード	6-7
ルート ガード	6-8
STP 拡張機能の適用	6-8
PVST シミュレーション	6-9
ハイ アベイラビリティ	6-9
バーチャライゼーションのサポート	6-9
STP 拡張機能のライセンス要件	6-10
STP 拡張機能の前提条件	6-10
注意事項および制約事項	6-11
STP 拡張機能の設定	6-12
STP 拡張機能のデフォルト値の設定	6-12
STP 拡張機能のグローバル設定	6-13
PVST シミュレーションのグローバル設定	6-14
STP 拡張機能のインターフェイス単位での設定	6-15
STP 拡張機能の設定フィールドの説明	6-16
デバイス : 設定 : Global Settings セクション	6-16
デバイス : 設定 : Port Setting セクション	6-17
追加情報	6-18
関連資料	6-18
標準規格	6-18
MIB	6-18

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



追加および変更された情報

この章では、『Cisco DCNM Layer 2 Switching コンフィギュレーション ガイド Release 4.0』で追加および変更された各情報について、リリース固有の内容を説明します。このマニュアルの最新版については、シスコの次の Web サイトにアクセスしてください。

http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/security/configuration/guide/sec_nx-os_config.html

Cisco NX-OS Release 4.0 の追加情報については、シスコの次の Web サイトにアクセスして『Cisco DCNM Release Notes』を参照してください。

http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/release/notes/401_nx-os_release_note.html

表 1 に、『Cisco DCNM Layer 2 Switching コンフィギュレーション ガイド Release 4.0』で追加および変更された機能についての概要と、その参照先を示します。

表 1 リリースで追加および変更された情報 4.0

機能	説明	変更されたリリース	参照先
SVI が VLAN ネットワーク インターフェイスに変更されました。	SVI が、すべての画面で VLAN ネットワーク インターフェイスという用語に変更されました。機能に変更はありません。	4.0(3)	マニュアルでのすべての表現



はじめに

この章では、『Cisco DCNM Layer 2 Switching コンフィギュレーション ガイド』の対象読者、構成、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。

この章で説明する内容は、次のとおりです。

- [対象読者 \(p.xiii\)](#)
- [マニュアルの構成 \(p.xiv\)](#)
- [表記法 \(p.xiv\)](#)
- [関連資料 \(p.xv\)](#)
- [マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン \(p.xvi\)](#)

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「VLAN の設定」	VLAN 設定の詳細について説明します。
第 3 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 4 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 5 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 6 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

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 DCNM のマニュアルの詳細は、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

Cisco DCNM の一連の資料には、次のマニュアルが含まれています。

リリース ノート

『Cisco DCNM Release Notes, Release 4.0』

DCNM コンフィギュレーション ガイド

『Cisco DCNM Getting Started with Virtual Device Contexts, Release 4.0』

『Cisco DCNM Fundamentals Configuration Guide, Release 4.0』

『Cisco DCNM Interfaces Configuration Guide, Release 4.0』

『Cisco DCNM Layer 2 Switching Configuration Guide, Release 4.0』

『Cisco DCNM Web Services API Guide, Release 4.0』

『Cisco DCNM Security Configuration Guide, Release 4.0』

『Cisco DCNM Unicast Routing Configuration Guide, Release 4.0』

『Cisco DCNM Virtual Device Context Configuration Guide, Release 4.0』

マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、テクニカル サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨エイリアスや一般的なシスコのマニュアルについては、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も示されています。

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

シスコのテクニカル サポート

次の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。

<http://www.cisco.com/en/US/support/index.html>

以下を含むさまざまな作業にこの Web サイトが役立ちます。

- テクニカル サポートを受ける
- ソフトウェアをダウンロードする
- セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける
- ツールおよびリソースへアクセスする
 - Product Alert の受信登録
 - Field Notice の受信登録
 - Bug Toolkit を使用した既知の問題の検索
- Networking Professionals (NetPro) コミュニティで、技術関連のディスカッションに参加する
- トレーニング リソースへアクセスする
- TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する

Japan テクニカル サポート Web サイトでは、Technical Support Web サイト (<http://www.cisco.com/techsupport>) の、利用頻度の高いドキュメントを日本語で提供しています。

Japan テクニカル サポート 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>

Service Request ツールの使用

Service Request ツールには、次の URL からアクセスできます。

<http://www.cisco.com/techsupport/servicerequest>

日本語版の Service Request ツールは次の URL からアクセスできます。

<http://www.cisco.com/jp/go/tac/sr/>

シスコの世界各国の連絡先一覧は、次の URL で参照できます。

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

その他の情報の入手方法

シスコの製品、サービス、テクノロジー、ネットワークング ソリューションに関する情報について、さまざまな資料をオンラインで入手できます。

- シスコの E メール ニュースレターなどの配信申し込みについては、Cisco Subscription Center にアクセスしてください。

<http://www.cisco.com/offer/subscribe>

- 日本語の月刊 Email ニュースレター「Cisco Customer Bridge」については、下記にアクセスください。

http://www.cisco.com/web/JP/news/cisco_news_letter/ccb/

- シスコ製品に関する変更やアップデートの情報を受信するには、Product Alert Tool にアクセスし、プロファイルを作成して情報の配信を希望する製品を選択してください。Product Alert Tool には、次の URL からアクセスできます。

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

- 『Cisco Product Quick Reference Guide』はリファレンス ツールで、パートナーを通じて販売されている多くのシスコ製品に関する製品概要、主な機能、製品番号、および簡単な技術仕様が記載されています。『Cisco Product Quick Reference Guide』を発注するには、次の URL にアクセスしてください。

<http://www.cisco.com/go/guide>

- ネットワークの運用面の信頼性を向上させることのできる最新の専門的サービス、高度なサービス、リモート サービスに関する情報については、Cisco Services Web サイトを参照してください。Cisco Services Web サイトには、次の URL からアクセスできます。

<http://www.cisco.com/go/services>

- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、マニュアル、ロゴ入り商品を提供しています。Cisco Marketplace には、次の URL からアクセスできます。

<http://www.cisco.com/go/marketplace/>

- DVD に収録されたシスコの技術マニュアル (Cisco Product Documentation DVD) は、Product Documentation Store で発注できます。Product Documentation Store には、次の URL からアクセスできます。

<http://www.cisco.com/go/marketplace/docstore>

- 日本語マニュアルの DVD は、マニュアルセンターから発注できます。マニュアルセンターには下記よりアクセスください。

http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/manual_center/index.shtml

- Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を発行しています。Cisco Press には、次の URL からアクセスできます。

<http://www.ciscopress.com>

- 日本語のシスコプレスの情報は以下にアクセスください。

<http://www.seshop.com/se/ciscopress/default.asp>

- 『Internet Protocol Journal』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『Internet Protocol Journal』には、次の URL からアクセスできます。

<http://www.cisco.com/ipj>

- 『What's New in Cisco Product Documentation』は、シスコ製品の最新マニュアル リリースに関する情報を提供するオンライン資料です。毎月更新されるこの資料は、製品カテゴリ別にまとめられているため、目的の製品マニュアルを見つけることができます。

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

- シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

http://www.cisco.com/public/countries_languages.shtml



概要

Cisco NX-OS デバイスは、本マニュアル『Cisco DCNM Layer 2 Switching コンフィギュレーション ガイド』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 DCNM 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。

- [VLAN \(p.1-2\)](#)
- [プライベート VLAN \(p.1-2\)](#)
- [スパンニング 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 \(p.1-6\)](#)

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せん。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。

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。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) 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 2 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 3 章「プライベート VLAN の設定」](#)を参照してください。

スパンニングツリー

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。スパンニングツリーは、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 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、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 を単一のスパン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、独立したスパン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ン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+ 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。

Rapid PVST+ の設定および実行の詳細については、[第 4 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、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。

Cisco NX-OS Release 4.0(2)以降のリリースでは、コマンドラインインターフェイス（CLI）を使用して、標準ではなく先行標準のMSTメッセージを送信するように特定のインターフェイスを設定できます。

MSTの設定および実行の詳細については、[第5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状態に移行します。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フォワーディング状態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6章「STP拡張機能の設定」](#)を参照してください。

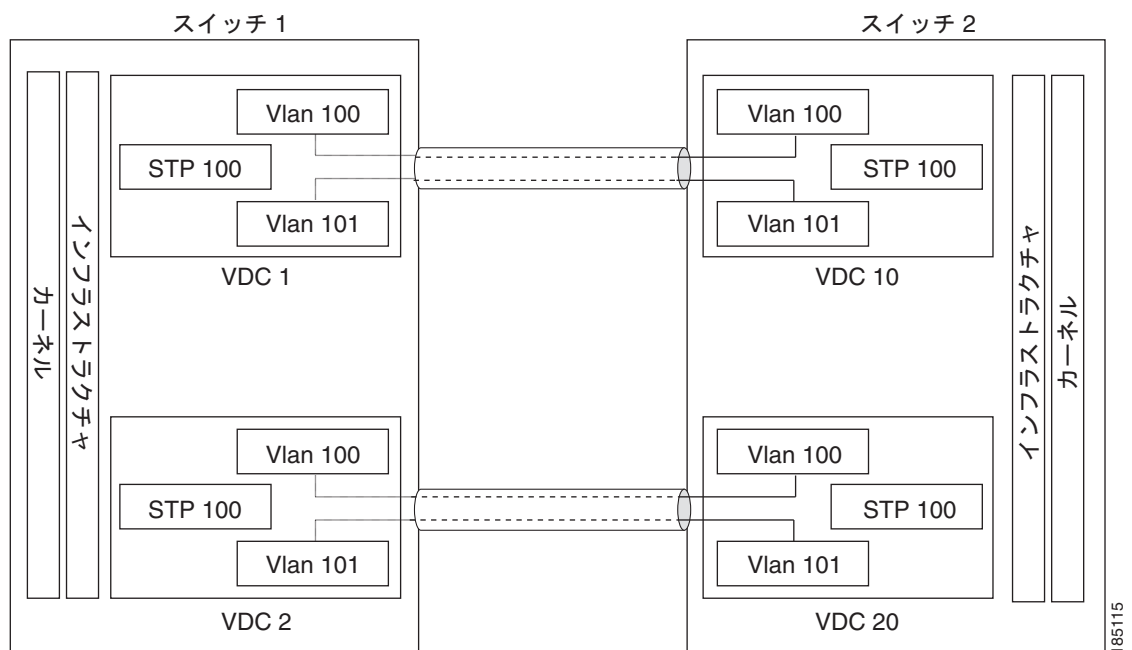
バーチャライゼーションとレイヤ2スイッチング

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 DCNM 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 Configuration Guide](#)』
- 『[Cisco DCNM Interfaces Configuration Guide](#)』
- 『[Cisco DCNM Security Configuration Guide](#)』
- 『[Cisco DCNM Virtual Device Context Configuration Guide](#)』
- 『[Cisco DCNM Licensing Guide](#)』
- 『[Cisco NX-OS High Availability and Redundancy Guide](#)』
- 『[Cisco NX-OS System Management Configuration Guide](#)』



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。

Data Center Network Manager（DCNM）機能の詳細については、『*Cisco DCNM Fundamentals Configuration Guide*』を参照してください。

この章の内容は、次のとおりです。

- [VLAN について \(p.2-2\)](#)
- [VLAN のライセンス要件 \(p.2-7\)](#)
- [VLAN 設定の前提条件 \(p.2-7\)](#)
- [注意事項および制約事項 \(p.2-7\)](#)
- [VLAN の設定 \(p.2-8\)](#)
- [統計情報の表示 \(p.2-11\)](#)
- [VLAN 設定のフィールドの説明 \(p.2-11\)](#)
- [追加情報 \(p.2-21\)](#)



(注) プライベート VLAN の情報については、[第 3 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せん。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 \(p.2-2\)](#)
- [VLAN の範囲 \(p.2-4\)](#)
- [VLAN の作成、削除、および変更 \(p.2-5\)](#)
- [ハイ アベイラビリティ \(p.2-6\)](#)
- [バーチャライゼーションのサポート \(p.2-6\)](#)

VLAN の概要



(注)

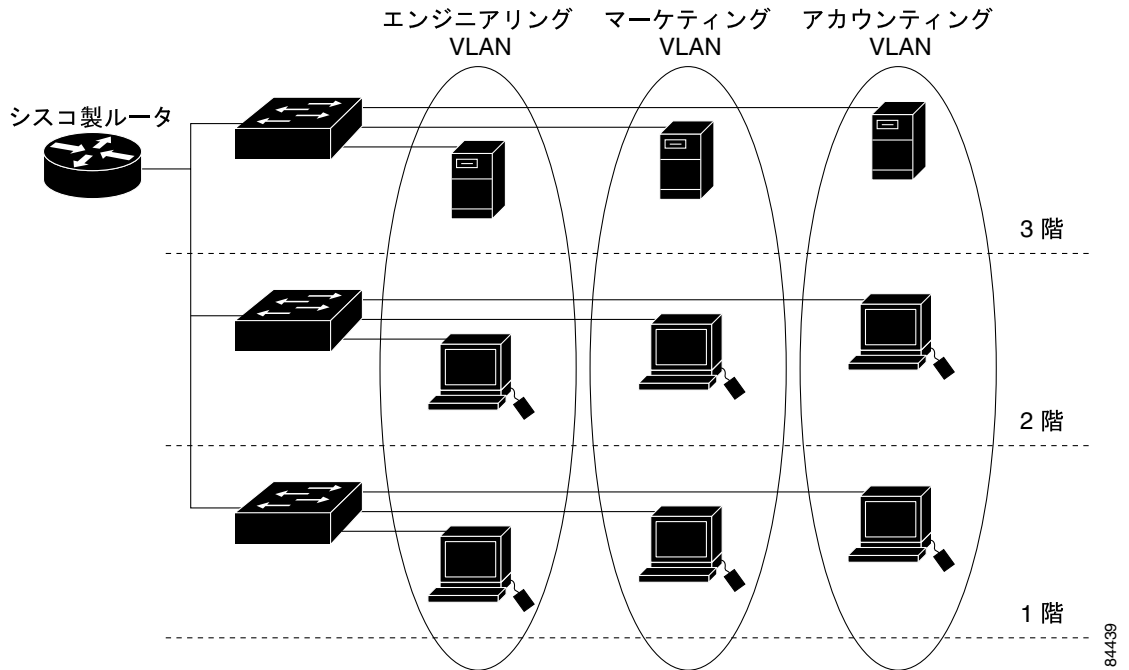
VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) モードは、オフです。他のデバイス上で VTP がオンの場合に VTP ドメインを分割する VTP Protocol Data Unit (PDU; プロトコル データ ユニット) は、すべてのデバイスのインターフェイスで廃棄されます。

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せん。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 2-1 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 2-1 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 サブネットワーク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。

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) 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。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)

VLAN ネットワーク 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 DCNM Interfaces Configuration Guide』を参照してください。この機能は、VLAN ネットワーク 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 2-1 に VLAN の範囲を示します。

表 2-1 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。 <ul style="list-style-type: none"> • 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せん。

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、アクティブ状態から一時停止状態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、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 DCNM 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ため、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 アドレスとエイジング 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 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 DCNM 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。

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ルールに関連付けることができます。VLAN をル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、ルールに 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 - 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、ル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ル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
DCNM	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 DCNM にバンドルされ、無料で提供されます。DCNM ライセンス機構の詳細については、『 <i>Cisco DCNM Licensing Guide</i> 』を参照してください。
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、『 <i>Cisco NX-OS Licensing Guide</i> 』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。
- 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。
- 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 \(p.2-8\)](#)
- [VLAN の基本設定の変更 \(p.2-10\)](#)



(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 DCNM 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。

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。



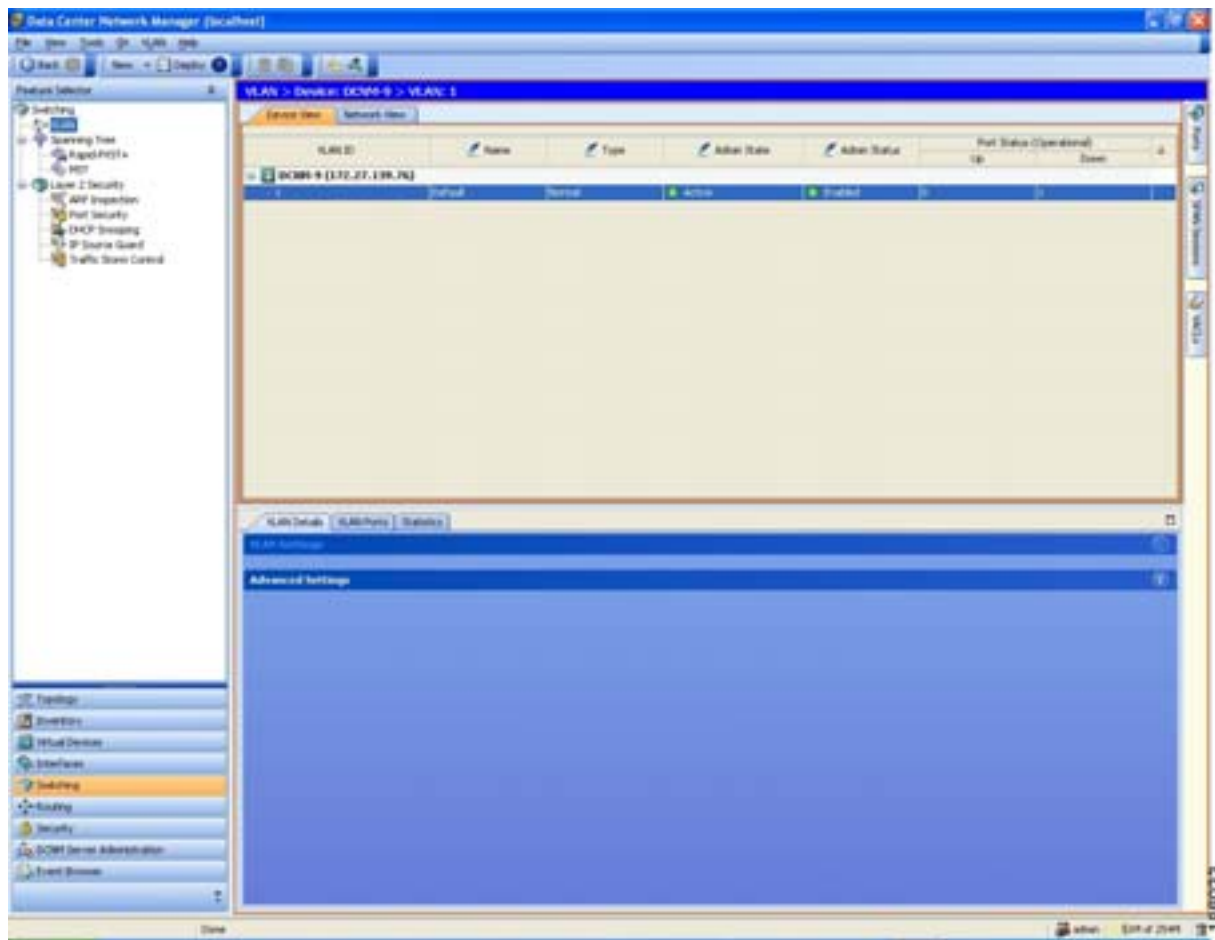
(注)

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、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。

VLAN を作成するには、VLAN ペインを使用します ([図 2-2](#) を参照)。

図 2-2 VLAN 設定の詳細



手順の詳細

VLAN を作成または削除するには、次の手順を実行します。

- ステップ 1** Feature Selector ペインから、**Switching > VLAN** を選択して VLAN ペインを開きます。
- ステップ 2** Summary ペインで **Device View** タブをクリックします。
- ステップ 3** Summary ペインで、VLAN を作成するデバイスをクリックします。
- ステップ 4** ツールバーで **New** をクリックします。
- ステップ 5** ドロップダウン リストから、**Normal VLAN** を選択します。
- ステップ 6** VLAN ID カラムで、作成する VLAN の ID を入力します。
VLAN は、デフォルト設定の状態ですぐに作成されます。
- ステップ 7** (任意) VLAN の名前を変更するには、Name カラムをクリックし、設定する名前を入力します。

ステップ 8 (任意) Summary ペインで削除する VLAN をクリックしてから、メニューバーから **VLAN > Delete** を選択します。

これらの VLAN を削除してよいかどうかの確認メッセージが表示されます。Yes をクリックすると、これらの VLAN はデバイスからすぐに削除されます。

ステップ 9 (任意) デバイスに変更を適用するには、メニューバーから **File > Deploy** を選択します。

VLAN の基本設定の変更

VLAN ペインを使用して、VLAN の基本設定を変更できます (図 2-2 を参照)。

手順の詳細

VLAN の基本設定を変更するには、次の手順を実行します。

ステップ 1 Feature Selector ペインから、**Switching > VLAN** を選択して VLAN ペインを開きます。

ステップ 2 Summary ペインで **Device View** タブをクリックします。

ステップ 3 設定を変更するデバイスをクリックします。

Summary ペインで選択したデバイスが強調表示され、Details ペインにタブが表示されます。

ステップ 4 そのデバイスを展開表示します。

デバイスに設定された VLAN が一覧表示されます。

ステップ 5 設定を変更するデバイスを選択します。

ステップ 6 Details ペインで **VLAN Details** タブをクリックします。

ステップ 7 **VLAN Settings** タブをクリックします。



(注) Media 行のグレー表示された値を Ethernet から変更しないでください。サポートされるメディアは Ethernet のみです。

ステップ 8 VLAN Name フィールドに名前を入力します。

ステップ 9 ドロップダウン リストから、設定する VLAN のタイプ、管理ステート、および管理ステータスを選択します。

ステップ 10 デバイスに変更を適用するには、メニューバーから **File > Deploy** を選択します。

統計情報の表示

次のウィンドウが Statistics タブに表示されます。

- VLAN Traffic Statistics レイヤ 2 のユニキャスト、マルチキャスト、およびブロードキャストトラフィック、レイヤ 3 のユニキャストおよびマルチキャストトラフィックなどの VLAN トラフィックについての情報が表示されます。

VLAN 設定のフィールドの説明

ここでは、VLAN ペインで表示されるフィールドについて説明します。内容は次のとおりです。

- Device ビュー：デバイス：グローバル設定：Global Settings セクション (p.2-11)
- Device ビュー：VLAN：VLAN の詳細：VLAN Settings セクション (p.2-12)
- Device ビュー：VLAN：VLAN の詳細：Advanced Settings セクション (p.2-16)
- Device ビュー：VLAN：標準 VLAN の VLAN ポート：Access Ports セクション (p.2-16)
- Device ビュー：VLAN：標準 VLAN の VLAN ポート：Trunk Ports セクション (p.2-16)
- Device ビュー：VLAN：プライマリ VLAN のプライマリ VLAN ポート：Promiscuous Ports セクション (p.2-17)
- Device ビュー：VLAN：セカンダリ VLAN の Secondary VLAN Ports タブ：PVLAN Host Ports セクション (p.2-17)
- Network ビュー：デバイス：VLAN の詳細：VLAN Settings セクション (p.2-18)
- Network ビュー：デバイス：VLAN の詳細：Advanced Settings セクション (p.2-19)
- Network ビュー：デバイス：VLAN ポート：Access Ports セクション (p.2-19)
- Network ビュー：デバイス：VLAN ポート：Trunk Ports セクション (p.2-19)

Device ビュー：デバイス：グローバル設定：Global Settings セクション

表 2-2 Device ビュー：デバイス：グローバル設定：Global Settings セクション

フィールド	説明
Dot1Q Native Tag	デバイスのすべてのトランク ポートで維持されるネイティブ VLAN のパケットのタグングデフォルトはディセーブルです。

Device ビュー : VLAN : VLAN の詳細 : VLAN Settings セクション

表 2-3 Device ビュー : VLAN : VLAN の詳細 : VLAN Settings セクション : 標準 VLAN

フィールド	説明
VLAN ID	表示のみ。VLAN ID です。デフォルトでは、VLAN の後ろに VLAN の番号が付きます (VLANXXXX)。
Device	表示のみ。この VLAN のデバイスのホスト名または IP アドレスです。
VLAN Name	VLAN の名前。デフォルト名は、VLAN の後ろに VLAN の番号が付きます (VLANXXXX)。
VLAN Type	標準 VLAN として設定されるタイプ。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Normal • Primary • Community • Isolated
Media	このフィールドはサポートされていません。
Admin State	管理ステート。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Active • Suspended デフォルトは Active です。
Admin Status	管理ステータス。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Enabled • Disabled デフォルトは Enabled です。
VLAN ネットワーク インターフェイス設定	
Description	VLAN ネットワーク インターフェイスの説明。任意の印刷可能な文字列です。
IP Address	VLAN ネットワーク インターフェイスの IP アドレス。ドット付き 10 進表記の有効な IP アドレスです (A:B:C:D)。
Netmask	VLAN ネットワーク インターフェイスのネットワーク マスク (ドット付き 10 進表記)。
Admin State	VLAN ネットワーク インターフェイスの管理ステート。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Down • Up デフォルトは Up です。
Oper Status	表示のみ。VLAN ネットワーク インターフェイスの動作ステータス。

表 2-4 Device ビュー : VLAN : VLAN の詳細 : VLAN 設定 : プライマリ VLAN

フィールド	説明
VLAN ID	表示のみ。VLAN ID です。デフォルトでは、VLAN の後ろに VLAN の番号が付きます (VLANXXXX)。
Device	表示のみ。この VLAN のデバイスのホスト名または IP アドレスです。
VLAN Name	VLAN の名前。デフォルト名は、VLAN の後ろに VLAN の番号が付きます (VLANXXXX)。
VLAN Type	プライマリ VLAN として設定される VLAN のタイプ。プライベート VLAN は、ルータからプライベート VLAN ホストポートへのダウンストリームトラフィックを伝送します。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Normal • Primary • Community • Isolated
Media	このフィールドはサポートされていません。
Admin State	管理ステート。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Active • Suspended デフォルトは Active です。
Admin Status	管理ステータス。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Enabled • Disabled デフォルトは Enabled です。
Oper Status	表示のみ。VLAN の動作ステータス。

セカンダリ VLAN



(注) 各プライマリ VLAN に複数のセカンダリ VLAN を関連付けることができます。


VLAN Id	表示のみ。デバイスに設定された独立およびコミュニティ VLAN。
Type	表示のみ。セカンダリ VLAN のタイプ。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Community • Isolated

VLAN ネットワーク インターフェイス設定

Description	VLAN ネットワーク インターフェイスの説明。任意の印刷可能な文字列です。
IP Address	VLAN ネットワーク インターフェイスの IP アドレス。ドット付き 10 進表記の有効な IP アドレスです (A:B:C:D)。
Netmask	VLAN ネットワーク インターフェイスのネットワーク マスク (ドット付き 10 進表記)。
Admin State	VLAN ネットワーク インターフェイスの管理ステート。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Down • Up デフォルトは Up です。

■ VLAN 設定のフィールドの説明

表 2-5 Device ビュー : VLAN : VLAN の詳細 : VLAN 設定 : コミュニティ VLAN

フィールド	説明
VLAN ID	表示のみ。VLAN ID です。デフォルトでは、VLAN の後ろに VLAN の番号が付きます (VLANXXXX)。
Device	表示のみ。この VLAN のデバイスの ホスト名または IP アドレスです。
VLAN Name	VLAN の名前。デフォルト名は、VLAN の後ろに VLAN の番号が付きます (VLANXXXX)。
VLAN Type	コミュニティ VLAN として設定される VLAN。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Normal • Primary • Community • Isolated
Primary VLAN ID	表示のみ。このコミュニティ VLAN が関連付けられているプライマリ VLAN が表示されます。  (注) プライマリ VLAN を関連付けていない場合、Not Configured と表示されます。
Media	このフィールドはサポートされていません。
Admin State	有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Active • Suspended デフォルトは Active です。
Admin Status	有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Enabled • Disabled デフォルトは Enabled です。


VLAN ネットワーク インターフェイス設定



(注) コミュニティ VLAN をプライマリ VLAN に関連付けている場合、この VLAN ネットワーク インターフェイスはサポートされません。プライベート VLAN については、プライマリ VLAN 上の VLAN ネットワーク インターフェイスのみ動作します。

Description	VLAN ネットワーク インターフェイスの説明。任意の印刷可能な文字列です。
IP Address	VLAN ネットワーク インターフェイスの IP アドレス。ドット付き 10 進表記の有効な IP アドレスです (A:B:C:D)。
Netmask	VLAN ネットワーク インターフェイスのネットワーク マスク (ドット付き 10 進表記)。
Admin State	VLAN ネットワーク インターフェイスの管理ステート。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Down • Up デフォルトは Up です。
Oper Status	表示のみ。VLAN ネットワーク インターフェイスの動作ステータス。

表 2-6 Device ビュー : VLAN : VLAN の詳細 : VLAN 設定 : 独立 VLAN

フィールド	説明
VLAN ID	表示のみ。VLAN ID です。デフォルトでは、VLAN の後ろに VLAN の番号が付きます (VLANXXXX)。
Device	表示のみ。この VLAN のデバイスのホスト名または IP アドレスです。
VLAN Name	VLAN の名前。最大文字列数は XXX です。デフォルト名は、VLAN の後ろに VLAN の数値が付きます (VLANXXXX)。
VLAN Type	独立 VLAN として設定される VLAN のタイプ。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Normal • Primary • Community • Isolated
Primary VLAN ID	表示のみ。このコミュニティ VLAN が関連付けられているプライマリ VLAN が表示されます。  (注) プライマリ VLAN を関連付けていない場合、Not Configured と表示されます。
Media	このフィールドはサポートされていません。
Admin State	管理ステート。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Active • Suspended デフォルトは Active です。
Admin Status	管理ステータス。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Enabled • Disabled デフォルトは Enabled です。
Oper Status	VLAN の動作ステータス。

VLAN ネットワーク インターフェイス設定



(注) 独立 VLAN がプライマリ VLAN に関連付けられている場合、この VLAN ネットワーク インターフェイスはサポートされません。プライベート VLAN については、プライマリ VLAN 上の VLAN ネットワーク インターフェイスのみ動作します。

Description	VLAN ネットワーク インターフェイスの説明。任意の印刷可能な文字列です。
IP Address	VLAN ネットワーク インターフェイスの IP アドレス。ドット付き 10 進表記の有効な IP アドレスです (A:B:C:D)。
Netmask	VLAN ネットワーク インターフェイスのネットワーク マスク (ドット付き 10 進表記)。
Admin State	VLAN ネットワーク インターフェイスの管理ステート。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Down • Up デフォルトは Up です。

Device ビュー : VLAN : VLAN の詳細 : Advanced Settings セクション

表 2-7 Device ビュー : VLAN : VLAN の詳細 : Advanced Settings セクション

フィールド	説明
SPAN 設定	
RSPAN VLAN	リモート SPAN (RSPAN) VLAN の有無についてのステータス
SPAN の始点の設定	
Session ID	表示のみ。インターフェイス結合時の SPAN セッション ID
Type	表示のみ。セッションのタイプ
Direction:Ingress	入力パケットのモニタ
Direction:Egress	出力パケットのモニタ
セキュリティ設定	
DAI	表示のみ。Dynamic ARP Inspection (DAI; ダイナミック ARP インスペクション) がイネーブルかディセーブルかについてのステータス
DHCP Snooping	表示のみ。DHCP スヌーピングがイネーブルかディセーブルかについてのステータス
VACL	VLAN で入力トラフィックをフィルタする VLAN アクセス マップ

Device ビュー : VLAN : 標準 VLAN の VLAN ポート : Access Ports セクション

表 2-8 Device ビュー : VLAN : 標準 VLAN の VLAN ポート : Access Ports セクション

フィールド	説明
Interface Name	表示のみ。アクセス インターフェイスの名前。このインターフェイスは、物理ポートまたはポート チャネルのいずれでも可能です。
Description	表示のみ。インターフェイスに設定される説明。デフォルトはブランクです。
Port Status	表示のみ。ポートのステータス。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Admin down • Up • Down

Device ビュー : VLAN : 標準 VLAN の VLAN ポート : Trunk Ports セクション

表 2-9 Device ビュー : VLAN : 標準 VLAN の VLAN ポート : Trunk Ports セクション

フィールド	説明
Interface Name	表示のみ。トランク インターフェイスの名前。物理ポートまたはポート チャネルのいずれでも可能です。
Description	表示のみ。インターフェイスに設定される説明。デフォルトはブランクです。
Port Status	表示のみ。ポートのステータス。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Admin down • Up • Down

Device ビュー : VLAN : プライマリ VLAN のプライマリ VLAN ポート : Promiscuous Ports セクション

表 2-10 Device ビュー : VLAN : プライマリ VLAN の VLAN ポート : Promiscuous Ports セクション

フィールド	説明
Interface Name	表示のみ。インターフェイスの名前。このインターフェイスは、物理ポートまたはポート チャネルのいずれでも可能です。
Description	表示のみ。インターフェイスに設定される説明。デフォルトはブランクです。
Secondary VLANs	プライマリ VLAN の無差別ポートに関連付けられたセカンダリ VLAN
Port Status	表示のみ。ポートのステータス。有効な値は、次のとおりです。 <ul style="list-style-type: none"> Admin down Up Down

Device ビュー : VLAN : セカンダリ VLAN の Secondary VLAN Ports タブ : PVLAN Host Ports セクション

表 2-11 Device ビュー : VLAN : セカンダリ VLAN の VLAN ポート : PVLAN Host Ports セクション

フィールド	説明
Interface Name	表示のみ。インターフェイスの名前。このインターフェイスは、物理ポートまたはポート チャネルのいずれでも可能です。
Description	表示のみ。インターフェイスに設定される説明。デフォルトはブランクです。
Port Status	ポートが関連付けられているセカンダリ VLAN。 表示のみ。ポートのステータス。有効な値は、次のとおりです。 <ul style="list-style-type: none"> Admin down Up Down

■ VLAN 設定のフィールドの説明

Network ビュー : デバイス : VLAN の詳細 : VLAN Settings セクション

表 2-12 Network ビュー : デバイス : VLAN の詳細 : VLAN 設定 : 標準 VLAN

フィールド	説明
VLAN ID	表示のみ。VLAN ID です。デフォルトでは、VLAN の後ろに VLAN の番号が付きます (VLANXXXX)。
Device	表示のみ。この VLAN のデバイスの ホスト名または IP アドレスです。
VLAN Name	VLAN の名前。最大文字列数は XXX です。デフォルト名は、VLAN の後ろに VLAN の数値が付きます (VLANXXXX)。
VLAN Type	標準 VLAN として設定される VLAN のタイプ。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Normal • Primary • Community • Isolated
Media	このフィールドはサポートされていません。
Admin State	管理ステート。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Active • Suspended デフォルトは Active です。
Admin Status	管理ステータス。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Enabled • Disabled デフォルトは Enabled です。
VLAN ネットワーク インターフェイス設定	
Description	VLAN ネットワーク インターフェイスの説明。任意の印刷可能な文字列です。
IP Address	VLAN ネットワーク インターフェイスの IP アドレス。ドット付き 10 進表記の有効な IP アドレスです (A:B:C:D)。
Netmask	VLAN ネットワーク インターフェイスのネットワーク マスク (ドット付き 10 進表記)。
Admin State	VLAN ネットワーク インターフェイスの管理ステート。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Down • Up デフォルトは Up です。
Oper Status	表示のみ。VLAN ネットワーク インターフェイスの動作ステータス。

Network ビュー : デバイス : VLAN の詳細 : Advanced Settings セクション

表 2-13 Network ビュー : デバイス : VLAN の詳細 : Advanced Settings セクション

フィールド	説明
SPAN 設定	
RSPAN VLAN	リモート SPAN (RSPAN) VLAN の有無についてのステータス
SPAN の始点の設定	
Session ID	表示のみ。インターフェイス結合時の SPAN セッション ID
Type	表示のみ。セッションのタイプ
Direction:Ingress	入力パケットのモニタ
Direction:Egress	出力パケットのモニタ
セキュリティ設定	
DAI	表示のみ。Dynamic ARP Inspection (DAI; ダイナミック ARP インスペクション) がイネーブルかディセーブルかについてのステータス
DHCP Snooping	表示のみ。DHCP スヌーピングがイネーブルかディセーブルかについてのステータス
VACL	VLAN で入力トラフィックをフィルタする VLAN アクセス マップ

Network ビュー : デバイス : VLAN ポート : Access Ports セクション

表 2-14 Network ビュー : デバイス : 標準 VLAN の VLAN ポート : Access Ports セクション

フィールド	説明
Interface Name	表示のみ。アクセス インターフェイスの名前。このインターフェイスは、物理ポートまたはポート チャネルのいずれでも可能です。
Description	表示のみ。インターフェイスに設定される説明。デフォルトはブランクです。
Port Status	表示のみ。ポートのステータス。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Admin down • Up • Down

Network ビュー : デバイス : VLAN ポート : Trunk Ports セクション

表 2-15 Network ビュー : VLAN : 標準 VLAN の VLAN ポート : Trunk Ports セクション

フィールド	説明
Interface Name	表示のみ。トランク インターフェイスの名前。このインターフェイスは、物理ポートまたはポート チャネルのいずれでも可能です。
Description	表示のみ。インターフェイスに設定される説明。デフォルトはブランクです。
Port Status	表示のみ。ポートのステータス。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Admin down • Up • Down

Network ビュー : デバイス : プライマリ VLAN ポート : Promiscuous Ports セクション

表 2-16 Network ビュー : デバイス : プライマリ VLAN ポート : Promiscuous Ports セクション

フィールド	説明
Interface Name	表示のみ。インターフェイスの名前。このインターフェイスは、物理ポートまたはポート チャネルのいずれでも可能です。
Description	表示のみ。インターフェイスに設定される説明。デフォルトはブランクです。
Secondary VLANs	プライマリ VLAN の無差別ポートに関連付けられたセカンダリ VLAN
Port Status	表示のみ。ポートのステータス。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Admin down • Up • Down

Network ビュー : デバイス : セカンダリ VLAN ポート : PVLAN Host Ports セクション

表 2-17 Network ビュー : デバイス : セカンダリ VLAN ポート : PVLAN Host Ports セクション

フィールド	説明
Interface Name	表示のみ。インターフェイスの名前。このインターフェイスは、物理ポートまたはポート チャネルのいずれでも可能です。
Description	表示のみ。インターフェイスに設定される説明。デフォルトはブランクです。
Port Status	ポートが関連付けられているセカンダリ VLAN。 表示のみ。ポートのステータス。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Admin down • Up • Down

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.2-21)
- [標準規格](#) (p.2-21)
- [MIB](#) (p.2-21)

関連資料

関連トピック	マニュアル名
プライベート VLAN	第 3 章「プライベート VLAN の設定」
Rapid PVST+	第 4 章「Rapid PVST+ の設定」
MST	第 5 章「MST の設定」
STP 拡張機能	第 6 章「STP 拡張機能の設定」
NX-OS レイヤ 2 スイッチングの設定	『Cisco NX-OS Layer 2 Switching Configuration Guide』
インターフェイス、VLAN ネットワーク インターフェイス、IP アドレス指定、ポート チャネル	『Cisco DCNM Interfaces Configuration Guide』
DCNM fundamentals	『Cisco DCNM Security 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 DCNM Virtual Device Context Configuration Guide』
ライセンス	『Cisco DCNM Licensing Guide』
リリース ノート	『Cisco DCNM 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
<ul style="list-style-type: none"> • CISCO-VLAN-MEMBERSHIP-MIB : vmMembershipTable-MIB vmMembershipSummaryTable-MIB 	<p>次の URL から、MIB の検索およびダウンロードができます。</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>



プライベート VLAN の設定

Data Center Network Manager (DCNM) 機能の詳細については、『*Cisco DCNM Fundamentals Configuration Guide*』を参照してください。

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 \(p.3-2\)](#)
- [プライベート VLAN のライセンス要件 \(p.3-8\)](#)
- [プライベート VLAN の前提条件 \(p.3-8\)](#)
- [注意事項および制約事項 \(p.3-9\)](#)
- [プライベート VLAN の設定 \(p.3-12\)](#)
- [プライベート VLAN の統計情報の表示 \(p.3-19\)](#)
- [フィールドの説明 \(p.3-19\)](#)
- [追加情報 \(p.3-20\)](#)



(注)

VLAN ネットワーク 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 DCNM 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.3-9] 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無差別ポートとのみ通信します。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のみ通信し、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.3-10] 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 ネットワーク インターフェイスを割り当てることにより、ルーティングを提供できます。VLAN ネットワーク インターフェイスは、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 VLAN ネットワーク インターフェイス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 VLAN ネットワーク インターフェイスは、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 \(p.3-3\)](#)
- [ハイ アベイラビリティ \(p.3-8\)](#)
- [パーチャライゼーションのサポート \(p.3-8\)](#)

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。

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

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くてもできますが、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 に属するホストポートです。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 に属するホストポートです。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

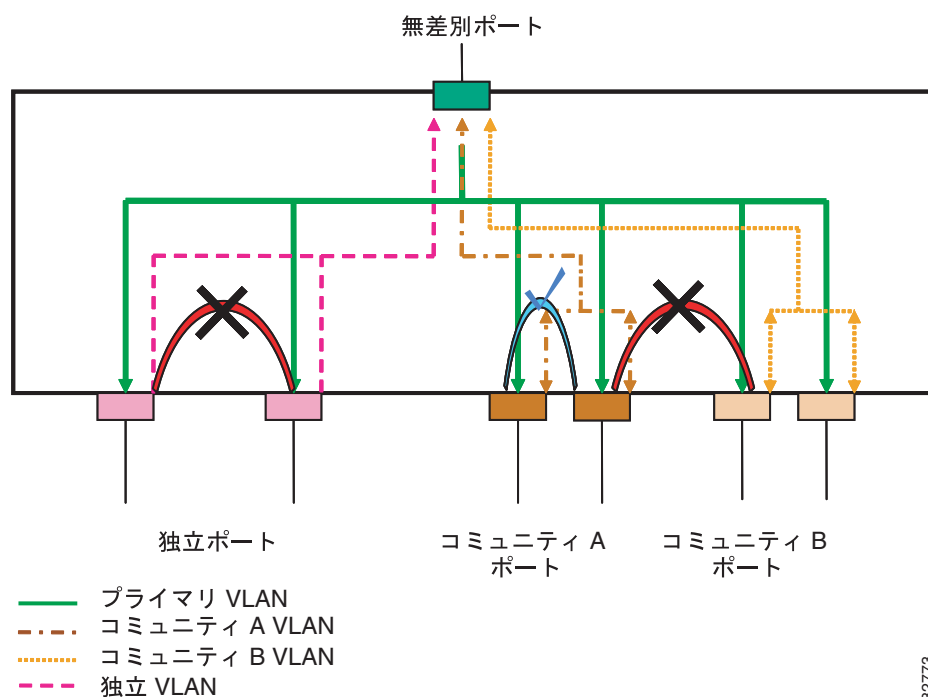
プライマリ VLAN にはレイヤ 3 ゲートウェイがあるので、プライベート VLAN の外部と通信するには、セカンダリ VLAN をプライマリ VLAN に関連付けます。プライマリ VLAN および 2 種類のセカンダリ VLAN (独立 VLAN およびコミュニティ VLAN) には、次の特性があります。

- **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 3-1 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 3-1 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 ゲートウェイを設定するには、VLAN ネットワーク 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 ネットワーク インターフェイスと IP アドレス指定の詳細については、『Cisco DCNM 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。

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。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。

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 ネットワーク 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 ネットワーク インターフェイス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 ネットワーク インターフェイスが設定された VLAN をセカンダリ VLAN として設定しようとする、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 ネットワーク インターフェイスを作成してイネーブルにしようとする、その VLAN インターフェイスはディセーブルのまま、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 VLAN ネットワーク インターフェイスに 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 DCNM 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。

■ プライベート VLAN のライセンス要件

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 DCNM 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
DCNM	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 DCNM にバンドルされ、無料で提供されます。DCNM ライセンス機構の詳細については、『Cisco DCNM Licensing Guide』を参照してください。
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、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。

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。

注意事項および制約事項

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 \(p.3-9\)](#)
- [プライベート VLAN ポートの設定 \(p.3-10\)](#)
- [他の機能に関連する制限 \(p.3-10\)](#)

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。
- 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 6 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 VLAN ネットワーク インターフェイスにセカンダリ VLAN をマッピングしてから、プライマリ VLAN の VLAN ネットワーク インターフェイス上に VACL を設定します。
- プライマリ VLAN の VLAN ネットワーク インターフェイスに適用した 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 VLAN ネットワーク インターフェイスにセカンダリ VLAN をマッピングせず、プライマリ VLAN とセカンダリ VLAN に異なる VACL を設定すると、問題が生じる場合があります。
- 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 に伝播されません。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 VLAN ネットワーク インターフェイス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 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。
- ポートチャンネル 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 チャン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 DCNM Security Configuration Guide』を参照してください。

プライベート VLAN の設定

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 \(p.3-12\)](#)
- [プライベート VLAN のイネーブル化 \(p.3-13\)](#)
- [プライベート VLAN としての VLAN の設定 \(p.3-14\)](#)
- [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 \(p.3-15\)](#)
- [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 \(p.3-16\)](#)
- [プライベート VLAN ホストポートとプライベート VLAN 無差別ポートの設定 \(p.3-18\)](#)



(注) VLAN ネットワーク インターフェイスへの IP アドレス指定の詳細については、『*Cisco DCNM Interfaces Configuration Guide*』を参照してください。

プライベート VLAN の設定時の注意事項

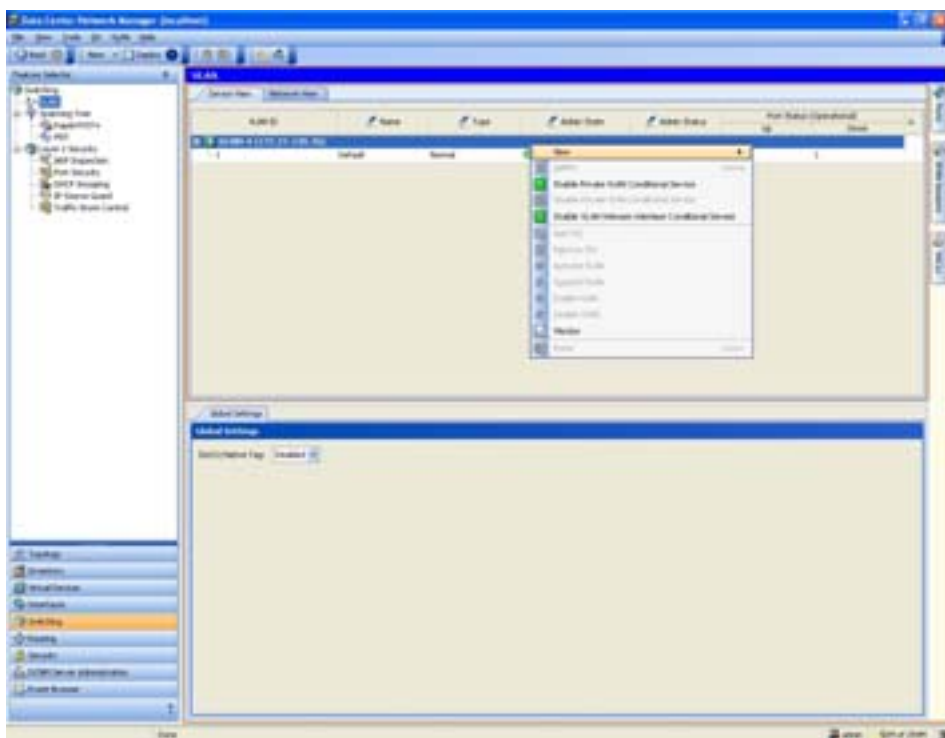
- デバイスにプライベート VLAN 機能を適用するには、プライベート VLAN をイネーブルにしておく必要があります。VLAN インターフェイス機能をイネーブルにしてから、この機能をデバイスに適用してください。
- セカンダリ VLAN を設定する前に、セカンダリ VLAN として設定するすべての VLAN の VLAN ネットワーク インターフェイスをシャットダウンします。
- プライベート VLAN 機能の設定を開始する前に、「[注意事項および制約事項](#)」(p.3-9)を参照してください。

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。

VLAN ペインを使用してデバイス上でプライベート VLAN をイネーブルにします(図 3-2 を参照)。

図 3-2 プライベート VLAN の設定



手順の詳細

デバイス上でプライベート VLAN 機能をイネーブルにするには、次の手順を実行します。

- ステップ 1** Feature Selector ペインから、**Switching > VLAN** を選択して VLAN ペインを開きます。
- ステップ 2** Summary ペインで **Device View** タブをクリックします。
- ステップ 3** Summary ペインで、VLAN を作成するデバイスをクリックします。
- ステップ 4** デバイス上で右クリックし、ドロップダウン リストから **Enable Private VLAN Conditional Services** を選択します。
- ステップ 5** (任意) デバイスに変更を適用するには、メニュー バーから **File > Deploy** を選択します。

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 のネットワーク インターフェイス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 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。



(注) プライベート VLAN がイネーブルであることを確認してください。

VLAN ペインを使用してプライベート VLAN を作成し、関連付けます (図 3-2 を参照)。

手順の詳細

プライベート VLAN を作成するには、次の手順を実行します。

-
- ステップ 1** Feature Selector ペインから、**Switching > VLAN** を選択して VLAN ペインを開きます。
 - ステップ 2** Summary ペインで **Device View** タブをクリックします。
 - ステップ 3** Summary ペインで、VLAN を作成するデバイスをクリックします。
 - ステップ 4** メニューで **New** をクリックします。
 - ステップ 5** ドロップダウン リストから、**Primary VLAN**、**Community VLAN**、または **Isolated VLAN** を選択します。
 - ステップ 6** VLAN ID カラムで、追加する VLAN の ID を入力します。

VLAN は、デフォルト設定の状態ですぐに作成されます。
 - ステップ 7** (任意) VLAN の名前を変更するには、Name カラムをクリックし、設定する名前を入力します。
 - ステップ 8** (任意) 特定の VLAN を削除するには、メニュー バーから **VLAN > Delete** を選択します。

これらの VLAN を削除してよいかどうかの確認メッセージが表示されます。Yes をクリックすると、これらの VLAN はデバイスからすぐに削除されます。
 - ステップ 9** (任意) デバイスに変更を適用するには、メニュー バーから **File > Deploy** を選択します。
-

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

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。

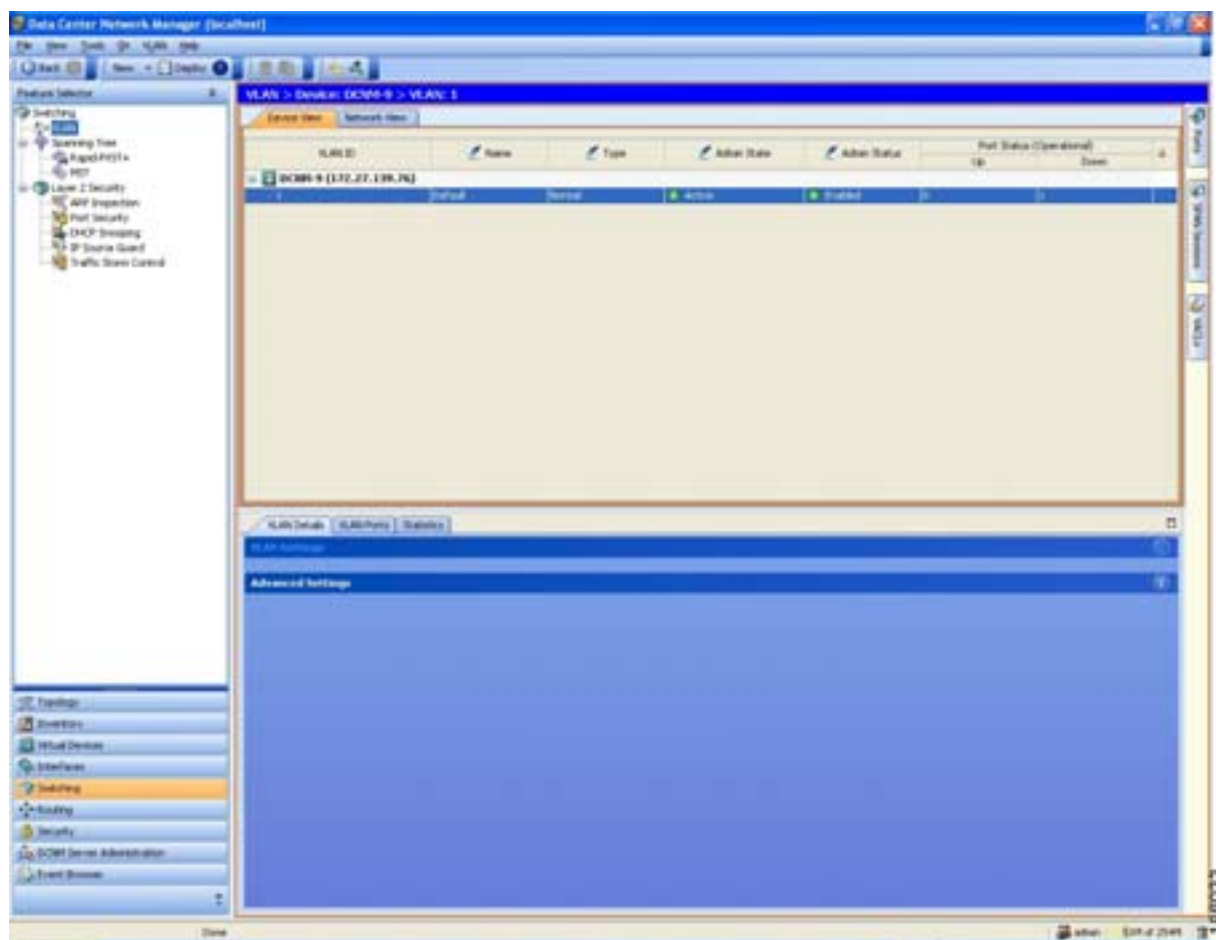
特定の VLAN をプライベート VLAN モードに再変換すると、元のアソシエーションが復元されません。

セカンダリ VLAN をプライマリ VLAN に関連付けます。コミュニティ VLAN および独立 VLAN は、セカンダリ VLAN です。各セカンダリ VLAN は、プライマリ VLAN に関連付ける必要があります。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。既存のアソシエーションを変更するには、まず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設定します。

VLAN ペインを使用してプライベート VLAN を関連付けます (図 3-3 を参照)。

図 3-3 セカンダリ VLAN とプライベート VLAN の関連付け



手順の詳細



(注) セカンダリ VLAN を作成してから、セカンダリ VLAN とプライマリ VLAN を関連付けます。

セカンダリ VLAN とプライマリ VLAN を関連付けるには、次の手順を実行します。

-
- ステップ 1** Feature Selector ペインから、**Switching > VLAN** を選択して VLAN ペインを開きます。
 - ステップ 2** Summary ペインで **Device View** タブをクリックします。
 - ステップ 3** Summary ペインで、VLAN を関連付けるデバイスをクリックします。
 - ステップ 4** Summary ペインで、**プライマリ VLAN** をクリックします。

Details ペインにタブが表示されます。
 - ステップ 5** **VLAN Details** タブをクリックします。
 - ステップ 6** **VLAN Settings** セクションをクリックします。
 - ステップ 7** **Secondary VLANs** エリアで右クリックし、このプライマリ VLAN と関連付けるセカンダリ VLAN を入力します。

Secondary VLANs エリアに、関連付けられた各セカンダリ VLAN の VLAN タイプおよび VLAN ID が表示されます。
 - ステップ 8** (任意) プライマリ VLAN にセカンダリ VLAN を追加で関連付けるには、ステップ 4 ~ 7 を繰り返します。
 - ステップ 9** (任意) プライマリ VLAN からセカンダリ VLAN を削除するには、**Secondary VLANs** エリアをクリックし、プライマリ VLAN との関連付けを削除したい VLAN を選択します。マウスを右クリックし、**Delete Secondary VLAN.** をクリックします。
 - ステップ 10** (任意) デバイスに変更を適用するには、メニューバーから **File > Deploy** を選択します。
-

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

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 ネットワーク インターフェイスにマッピングします。



(注) VLAN ネットワーク インターフェイスを設定する前に、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 ネットワーク 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 ネットワーク インターフェイスだけです。

VLAN ペインで、プライマリ VLAN の VLAN ネットワーク インターフェイスを追加し、VLAN ネットワーク インターフェイスをセカンダリ VLAN に関連付けます (図 3-3 を参照)。

手順の詳細



(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 のネットワーク インターフェイスをシャットダウンする必要があります。

プライマリ VLAN の VLAN ネットワーク インターフェイスを設定し、セカンダリ VLAN に関連付けるには、次の手順を実行します。

ステップ 1 Feature Selector ペインから、**Switching >VLAN** を選択して VLAN ペインを開きます。

ステップ 2 Summary ペインで **Device View** タブをクリックします。

ステップ 3 Summary ペインで、**プライマリ VLAN** をクリックします。

ステップ 4 メニュー バーから **VLAN > Add VLAN Network Interface** を選択します。

VLAN Details タブの VLAN Settings セクションにウィンドウが表示されます。ここで、VLAN ネットワーク インターフェイスを設定できます。

ステップ 5 Description フィールドに、VLAN ネットワーク インターフェイスの説明を入力します。

ステップ 6 IP Address フィールドに、VLAN ネットワーク インターフェイスの IP アドレスを入力します。

ステップ 7 Netmask フィールドに、VLAN ネットワーク インターフェイスのネットマスクを入力します。

ステップ 8 Admin State フィールドで、ドロップダウン リストから Up または Down を選択します。

ステップ 9 (任意) VLAN Network Interface エリアで、Secondary VLANs フィールドのドロップダウン リストをクリックし、プライマリ VLAN の VLAN ネットワーク インターフェイスに追加で関連付けるセカンダリ VLAN を選択します。

ステップ 10 (任意) デバイスに変更を適用するには、メニュー バーから **File > Deploy** を選択します。

プライベート VLAN ホストポートとプライベート VLAN 無差別ポートの設定

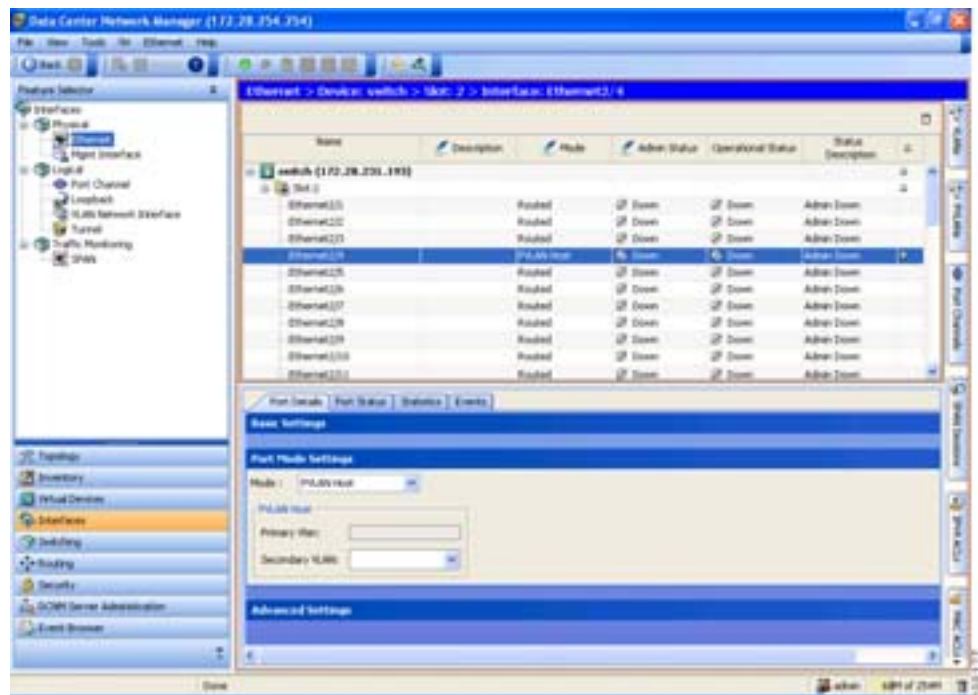
プライベート VLAN ホストポートとプライベート VLAN 無差別ポートを設定できます。プライベート VLAN では、ホストポートはセカンダリ VLAN (コミュニティ VLAN または独立 VLAN のどちらか) に含まれます。レイヤ 2 インターフェイスをプライベート VLAN の無差別ポートとして設定し、その無差別ポートをプライマリ VLAN およびセカンダリ VLAN に関連付けることができます。



(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。

Ethernet ペインを使用してプライベート VLAN ポートを設定します (図 3-4 を参照)。

図 3-4 プライベート VLAN ホストの設定



手順の詳細

ホストおよび無差別のプライベート VLAN ポートを作成するには、次の手順を実行します。

- ステップ 1** Feature Selector ペインから、**Interfaces > Physical > Ethernet** を選択して Ethernet ペインを開きます。
- ステップ 2** Contents ペインの Summary ペインから、デバイスをダブルクリックし、インターフェイスを表示します。
- ステップ 3** スロットをダブルクリックし、インターフェイスを一覧表示します。

ステップ 4 インターフェイスをクリックします。

Summary ペインで選択したインターフェイスが強調表示され、Details ペインにタブが表示されません。

ステップ 5 Details ペインで **Port Details** タブをクリックします。

ステップ 6 **Port Mode Settings** セクションをクリックします。

ステップ 7 ドロップダウン リストから、**PVLAN Host** または **PVLAN Promiscuous** を選択し、アクセスポートとしてポートを設定します。

ステップ 8 セカンダリ VLAN ドロップダウン リストをクリックし、このインターフェイス用に設定したいセカンダリ VLAN を選択します。

Secondary VLAN ウィンドウに、設定されたセカンダリ VLAN と、各セカンダリ VLAN が関連付けられているプライマリ VLAN が表示されます。セカンダリ VLAN を選択すると、Primary VLAN フィールドが自動的に生成されます。

ステップ 9 (任意) デバイスに変更を適用するには、メニューバーから **File > Deploy** を選択します。

プライベート VLAN の統計情報の表示

次のウィンドウが Statistics タブに表示されます。

- **VLAN Traffic Statistics** レイヤ 2 のユニキャスト、マルチキャスト、ブロードキャストトラフィック、およびレイヤ 3 のユニキャスト、マルチキャストトラフィックなどのプライベート VLAN トラフィックについての情報が表示されます。

フィールドの説明

プライベート VLAN ポートの設定に使用するフィールドの詳細については、『*Cisco DCNM Interfaces Configuration Guide*』を参照してください。

プライベート VLAN の設定に使用するフィールドの詳細については、[第 2 章「VLAN の設定」](#)を参照してください。

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.3-20)
- 標準規格 (p.3-20)
- MIB (p.3-20)

関連資料

関連トピック	マニュアル名
すべての VLAN	第 2 章「VLAN の設定」
STP 拡張機能	第 6 章「STP 拡張機能の設定」
NX-OS レイヤ 2 スイッチングの設定	『Cisco NX-OS Layer 2 Switching Configuration Guide』
VLAN インターフェイス、IP アドレス指定	『Cisco DCNM Interfaces Configuration Guide』
スタティック MAC アドレス、セキュリティ	『Cisco DCNM Security Configuration Guide』
DCNM fundamentals	『Cisco DCNM 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 DCNM Virtual Device Context Configuration Guide』
ライセンス	『Cisco DCNM Licensing Guide』
リリース ノート	『Cisco DCNM 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
<ul style="list-style-type: none"> • CISCO-PRIVATE-VLAN-MIB 	<p>次の URL から、MIB の検索およびダウンロードができます。</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>



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。

Data Center Network Manager の機能の詳細については、『Cisco DCNM Fundamentals 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。

- [Rapid PVST+ について \(p.4-2\)](#)
- [Rapid PVST+ のライセンス要件 \(p.4-20\)](#)
- [Rapid PVST+ を設定するための前提条件 \(p.4-20\)](#)
- [注意事項および制約事項 \(p.4-21\)](#)
- [Rapid PVST+ の設定 \(p.4-22\)](#)
- [統計情報の表示 \(p.4-35\)](#)
- [Rapid PVST+ のフィールドの説明 \(p.4-35\)](#)
- [追加情報 \(p.4-38\)](#)



(注)

Multiple Spanning Tree (MST) の詳細については、[第 5 章「MST の設定」](#)、STP 拡張の詳細については、[第 6 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) Spanning Tree Protocol (STP; スパニング ツリー プロトコル) パラメータの設定に DCNM を使用する前に、使用しているデバイスのコマンドラインに NX-OS グローバル コマンドを入力してログレベルを設定する必要があります。

```
--logging-level spanning-tree 6
--logging logfile messages 6
--logging event link-status default
```

ログレベルについては、『Cisco NX-OS System Management Configuration Guide』を参照してください。



(注) レイヤ 2 インターフェイスの作成方法については、『Cisco DCNM 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。

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.4-18] 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.4-18] 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.4-3)
- [Rapid PVST+](#) (p.4-8)
- [Rapid PVST+ および IEEE 802.1Q トランク](#) (p.4-18)
- [Rapid PVST+ とレガシー 802.1D STP の相互運用性](#) (p.4-18)
- [Rapid PVST+ と 802.1s MST の相互運用性](#) (p.4-18)
- [ハイ アベイラビリティ](#) (p.4-19)
- [バーチャライゼーションのサポート](#) (p.4-19)



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

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 フレームを定期的を送受信します。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状態にします。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ーワーディング状態になり、どちらのポートがブロッキング状態になるかは、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 \(p.4-4\)](#)
- [拡張システム ID \(p.4-5\)](#)
- [STP MAC アドレスの割り当て \(p.4-5\)](#)

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.4-32) 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 ビットの拡張システム ID フィールドは、ブリッジ ID の一部です (図 4-1 を参照)。

図 4-1 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 4-1 を参照)。

表 4-1 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、スパンニング 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ンニング 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

■ Rapid PVST+ について

- 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)

同じスパンニング 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、スパンニング 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。
- スパンニング 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.4-9)」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。

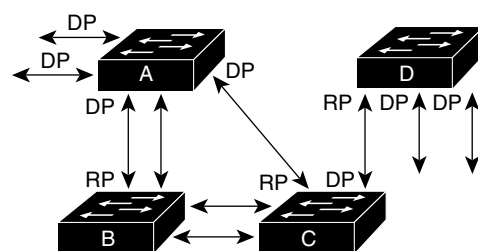
STP ルートブリッジは、レイヤ 2 ネットワークにおける各スパンニングツリートポロジの論理上の中心です。レイヤ 2 ネットワーク内のどの場所からも、ルートブリッジに到達するために必要とされないパスは、すべて STP ブロッキングモードになります。

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。

スパンニングツリートポロジの作成

図 4-2 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 4-2 スパンニングツリートポロジ



RP = ルートポート
DP = 指定ポート

187026

スパン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.4-8)
- Rapid PVST+ BPDU (p.4-9)
- 提案合意ハンドシェイク (p.4-10)
- プロトコル タイマー (p.4-11)
- ポート ロール (p.4-12)
- ポート ステート (p.4-13)
- ポート ロールの同期化 (p.4-15)
- 単一方向リンク障害の検出 (p.4-16)
- ポート コスト (p.4-17)
- ポート プライオリティ (p.4-17)

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、または最大エイジング 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、または最大エイジング 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ーワーディング 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。



(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 6 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.4-18) 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.4-15] を参照)。

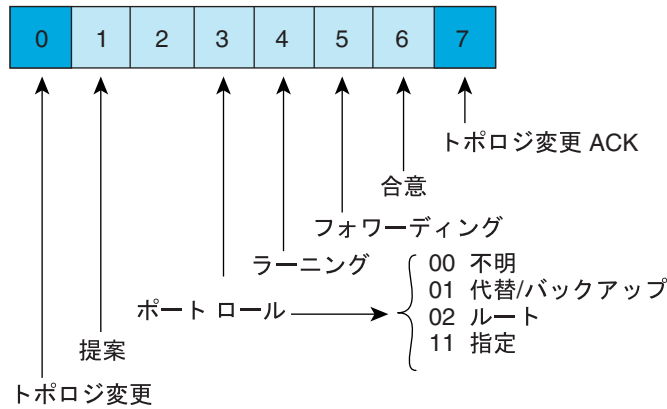
Rapid PVST+ BPDU

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 4-3 に、Rapid PVST+ での BPDU フラグの使用方法を示します。

図 4-3 BPDU 内の Rapid PVST+ フラグ バイト

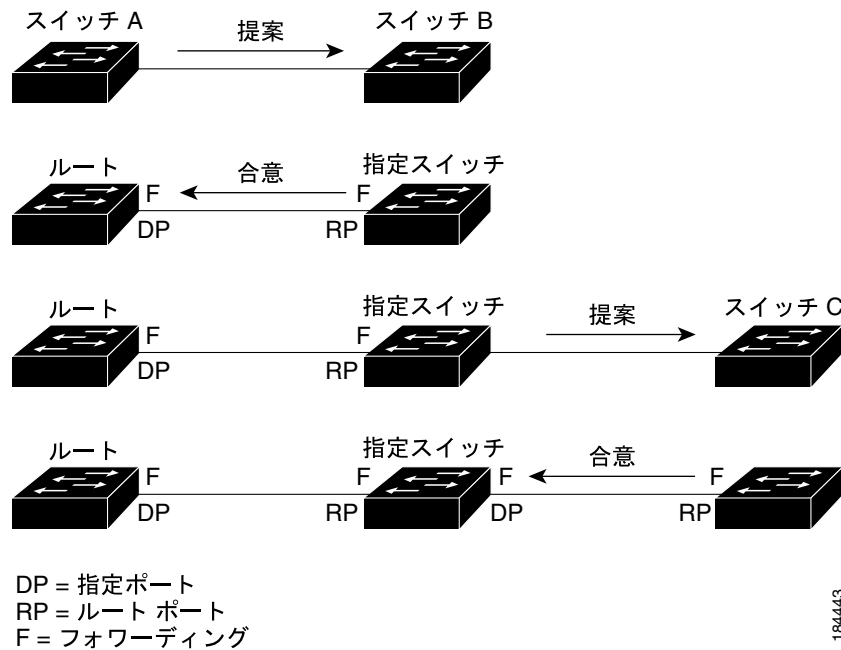


もう 1 つの重要な変更点は、Rapid PVST+ BPDU がタイプ 2、バージョン 2 であるため、デバイスが接続先のレガシー（802.1D）ブリッジを検出できることです。802.1D の BPDU はタイプ 0、バージョン 0 です。

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 4.4 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 4-4 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 4-4 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.4-13] 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 4-2 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 4-2 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。
最大エイジングタイマー	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

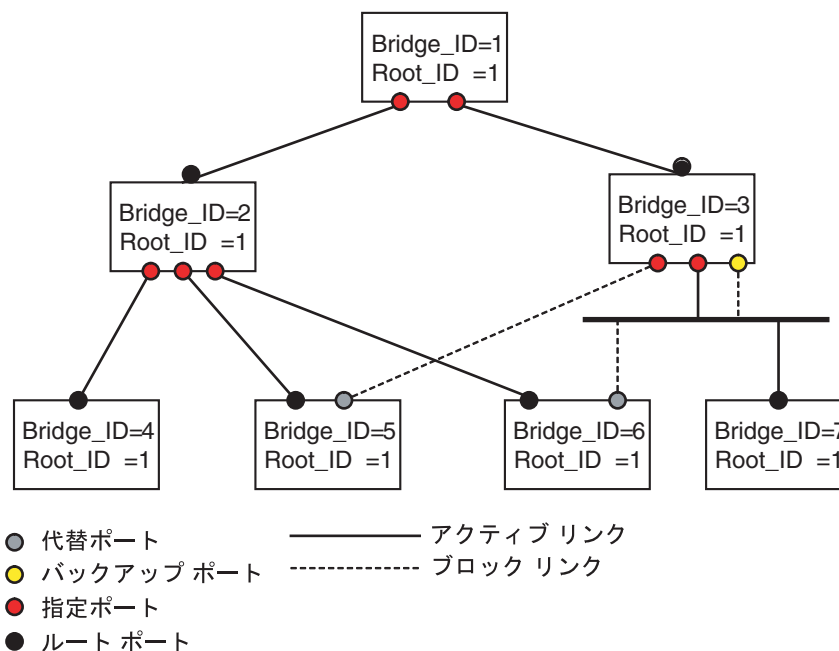
Rapid PVST+ では、ポート ロールを割り当ててアクティブ トポロジを学習することで、スパニング ツリーの高速コンバージェンスを実現します。「ルートブリッジの選定」(p.4-7) で説明しているように、Rapid PVST+ は、802.1D STP を利用して、最も高いスイッチ プライオリティ (最小プライオリティ値) を持つデバイスをルートブリッジとして選択します。Rapid PVST+ は、次に示すポート ロールの 1 つを各ポートに割り当てます。

- 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 4-5 を参照)。

図 4-5 ポート ロールを示すトポロジ例



182775

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 \(p.4-13\)](#)
- [ブロッキング ステート \(p.4-14\)](#)
- [ラーニング ステート \(p.4-14\)](#)
- [フォワーディング ステート \(p.4-14\)](#)
- [ディセーブル ステート \(p.4-14\)](#)
- [ポート ステートの概要 \(p.4-15\)](#)

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 ポートがスパンニング 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 4-3 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 4-3 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。

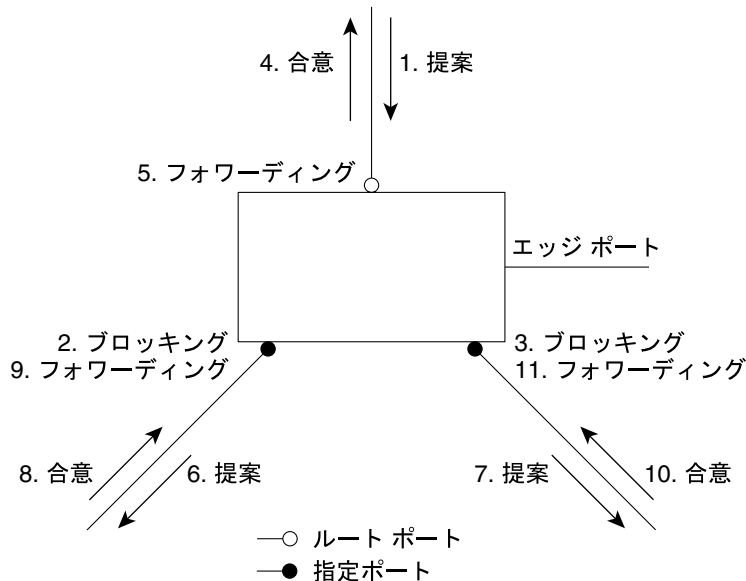
他のポートがすべて同期化されると、デバイスはルートポートで受信した上位のルート情報と同期化されます。次のいずれかの場合は、デバイスの個別のポートが同期されます。

- 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 4-6 に、このイベントシーケンスを示します。

図 4-6 高速コンバージェンス時のイベントシーケンス



184442

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.4-16)
- 不良 BPDU 情報の処理 (p.4-16)

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状態になるとすぐに、新しいルートポートがフォワーディング状態に移行します。

ポートで上位の情報を受信されたために、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状態に設定され、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状態に移行します。

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

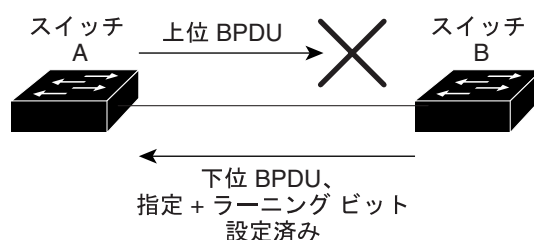
ソフトウェアは、受信した BPDU のポート ロールと状態の一貫性をチェックし、Unidirectional Link Detection (UDLD; 単一方向リンク検出) 機能を使用して、ブリッジングループが発生する可能性のある単一方向リンク障害を検出します。この機能は、異議メカニズムに基づいています。

UDLD の詳細については、『Cisco DCNM Interface 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、状態は廃棄状態に戻ります。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 4-7 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状態が含まれます。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 4-7 単一方向リンク障害の検出



184440



(注) ブリッジ保証機能の詳細については、第6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 4-4 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 4-4 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、フォワーディング状態に移行するために 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。

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 6 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。

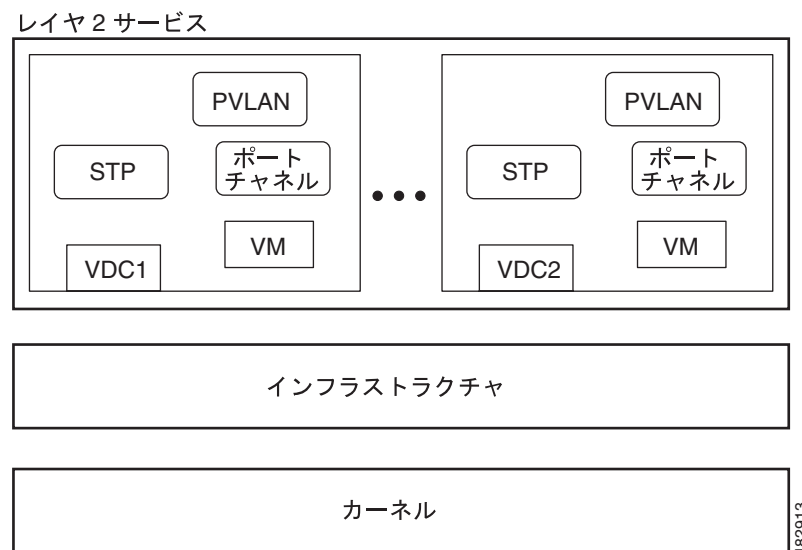
バーチャライゼーションのサポート



(注) VDC およびリソースの割り当ての詳細については、『Cisco DCNM 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 4-8 を参照)。

図 4-8 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 に渡って 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
DCNM	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 DCNM に組み込まれており、無料で提供されます。DCNM ライセンス スキームの詳細については、『 <i>Cisco DCNM Licensing Guide</i> 』を参照してください。
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 ライセンス機構の詳細については、『 <i>Cisco NX-OS Licensing Guide</i> 』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している必要があります。
- STP パラメータの設定に DCNM を使用する前に、使用している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グレベルを設定する必要があります。ロ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。

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。

- 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 6 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、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、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 802.1w 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。



(注)

デバイスで Rapid PVST+ を実行している場合、MST のプリプロビジョニングを行うことができます。メインメニューで、**Tools > Global Preferences > Pre Provisioning** を選択し、この機能の有効化と表示を行う画面にアクセスしたり、画面を非表示にしたりできます。プリプロビジョニングについては、『Cisco DCNM Fundamentals 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。

- [Rapid PVST+ のイネーブル化 \(p.4-23\)](#)
- [デバイスのすべての STP パラメータをデフォルト値に設定 \(p.4-24\)](#)
- [Rapid PVST+ の VLAN 単位でのディセーブル化またはイネーブル化 \(p.4-25\)](#)
- [プライマリおよびセカンダリルートとスイッチプライオリティの設定 \(p.4-26\)](#)
- [Rapid PVST+ ポートプライオリティの設定 \(p.4-28\)](#)
- [Rapid PVST+ パスコスト方式およびポートコストの設定 \(p.4-28\)](#)
- [インターフェイス別にすべての Rapid PVST+ パラメータをデフォルト値に設定 \(p.4-30\)](#)
- [VLAN の Rapid PVST+ hello タイムの設定 \(p.4-32\)](#)
- [VLAN の Rapid PVST+ 転送遅延時間の設定 \(p.4-33\)](#)
- [VLAN の Rapid PVST+ 最大エージングタイムの設定 \(p.4-33\)](#)
- [リンクタイプの指定 \(p.4-34\)](#)

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.4-25) を参照してください。

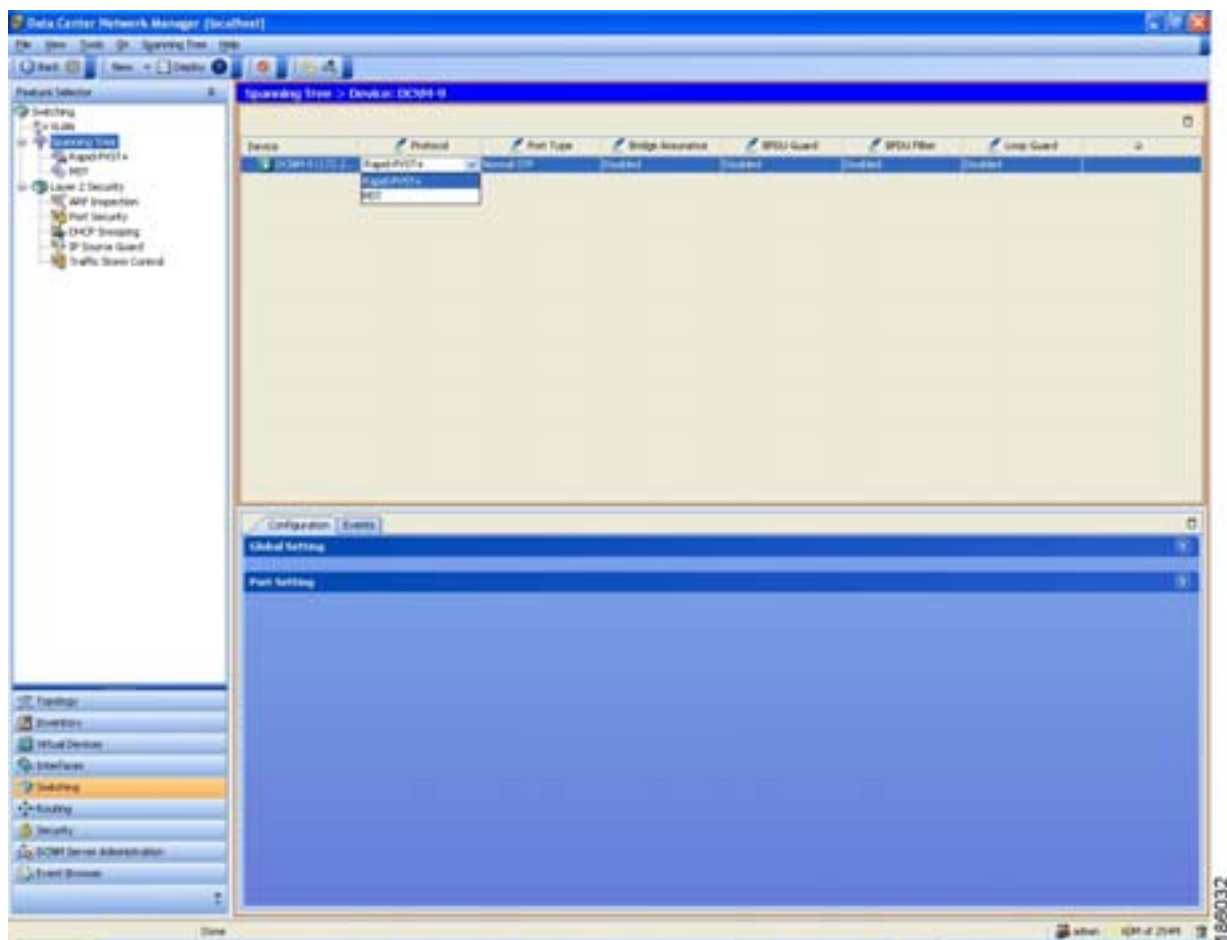
デフォルトの STP モードは Rapid PVST+ です。同じ VDC 上で MST と Rapid PVST+ を同時に実行することはできません。



(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。

Spanning Tree ペインを使用して Rapid PVST+ をイネーブルにします (図 4-9 を参照)。

図 4-9 Rapid PVST+ のイネーブル化



手順の詳細



(注) デフォルトの STP モードは Rapid PVST+ です。Rapid PVST+ はデフォルトでイネーブルです。以前にデバイスのモードを MST に変更し、デバイスの STP モードを Rapid PVST+ に戻す場合にこの手順を使用します。

デバイスで Rapid PVST+ をイネーブルにするには、次の手順を実行します。

-
- ステップ 1** Feature Selector ペインで、**Switching > Spanning Tree** を選択して、Spanning Tree ペインを表示します。
- ステップ 2** Summary ペインで、Rapid PVST+ をイネーブルにするデバイスをクリックします。
- Rapid PVST+ はすべての VLAN でデフォルトでイネーブルです。
- ステップ 3** Protocol フィールドで、ドロップダウン リストをクリックして **Rapid-PVST+** を選択します。
- ステップ 4** (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。
-

デバイスのすべての STP パラメータをデフォルト値に設定

デバイスのすべての STP パラメータをデフォルト値に設定できます。これによって STP モードは Rapid PVST+ になります。

Spanning Tree ペインを使用してデバイスのすべての STP パラメータをデフォルト値に設定します (図 4-9 を参照)。

手順の詳細

デバイスのすべての STP パラメータをデフォルト値に設定するには、次の手順を実行します。

-
- ステップ 1** Feature Selector ペインで、**Switching > Spanning Tree** を選択して、Spanning Tree ペインを表示します。
- ステップ 2** Summary ペインで、STP のデフォルト値に設定するデバイスをクリックします。
- デフォルトの STP モードは Rapid PVST+ です。
- ステップ 3** メニューバーで **Spanning Tree > Set to default** を選択します。
- ステップ 4** (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。
-

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

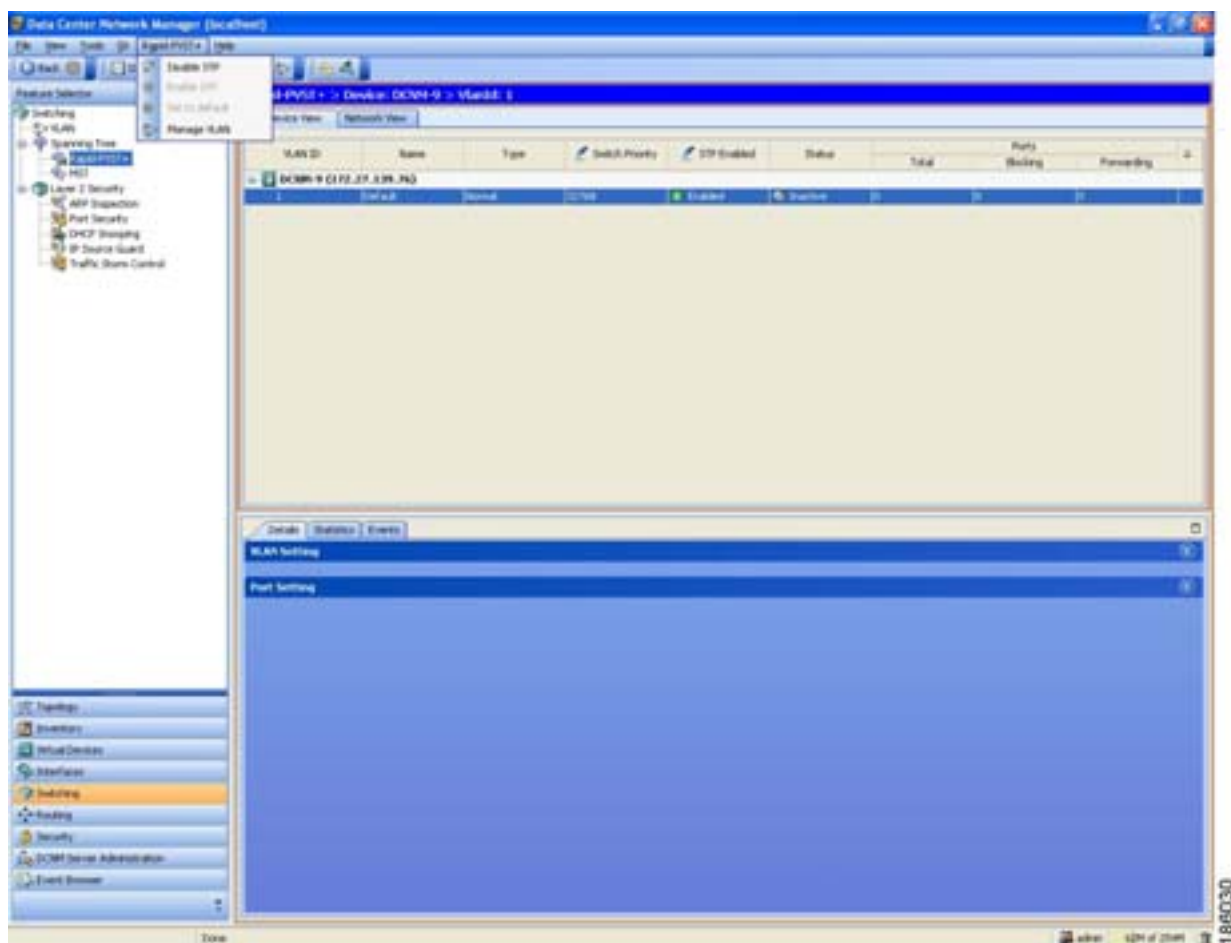
Rapid PVST+ は VLAN 単位でイネーブルまたはディセーブルにできます。



(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。

Rapid-PVST+ ペインを使用して VLAN 別に Rapid PVST+ をイネーブルまたはディセーブルにします (図 4-10 を参照)。

図 4-10 Rapid PVST+ の設定



手順の詳細

VLAN 別に Rapid PVST+ をイネーブルまたはディセーブルにするには、次の手順を実行します。

ステップ 1 Feature Selector ペインで、**Switching > Spanning Tree > Rapid-PVST+** を選択して、Rapid-PVST+ ペインを表示します。

ステップ 2 Summary ペインで、**Device View** タブをクリックします。

ステップ 3 Summary ペインで、イネーブルまたはディセーブルにする VLAN をクリックします。

Rapid PVST+ はすべての VLAN でデフォルトでイネーブルです。

ステップ 4 メニューバーで **Rapid-PVST+ > Enable STP** を選択します。



(注) **Rapid-PVST+ > Manage VLAN** を選択すると、VLAN ペインに戻ります。

ステップ 5 (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。



(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。

プライマリおよびセカンダリ ルートとスイッチ プライオリティの設定

ソフトウェアは、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。

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、プライマリおよびセカンダリ ルートまたは指定された VLAN のスイッチ プライオリティを設定できます。



(注) 特定のスイッチ プライオリティ値を設定するよりも、プライマリおよびセカンダリ ルートを指定することを推奨します。

複数のバックアップ ルート ブリッジを設定する場合は、複数のデバイスをセカンダリ ルートとして指定する必要があります。プライマリ ルート ブリッジを設定するときに使用したのと同じネットワーク直径および hello タイムをセカンダリ ルートに使用してください。

Rapid-PVST+ ペインを使用してデバイスを VLAN のプライマリ ルート ブリッジに設定します (図 4-10 を参照)。

手順の詳細

Rapid PVST+ が有効な VLAN で、デバイスがプライマリまたはセカンダリ ルート ブリッジになるよう設定する、あるいはスイッチ プライオリティを設定するには、次の手順を実行します。

-
- ステップ 1** Feature Selector ペインで、**Switching > Spanning Tree > Rapid-PVST+** を選択して、Rapid-PVST+ ペインを表示します。
 - ステップ 2** Summary ペインで、**Device View** タブをクリックします。
 - ステップ 3** Summary ペインで、デバイスをプライマリ ルートに設定する VLAN をクリックします。

Details ペインにタブが表示されます。
 - ステップ 4** Details タブをクリックします。
 - ステップ 5** VLAN Setting セクションをクリックします。

VLAN Setting セクションの Switch Priority エリアでは、デバイスを特定の VLAN のプライマリまたはセカンダリ ルートに設定したり、スイッチ プライオリティを設定したりできます。
 - ステップ 6** (任意) Root フィールドでドロップダウン リストをクリックし、**primary** をクリックしてデバイスを VLAN のプライマリ ルートに設定します。
 - ステップ 7** (任意) Root フィールドでドロップダウン リストをクリックし、**secondary** をクリックしてデバイスを VLAN のセカンダリ ルートに設定します。
 - ステップ 8** (任意) Switch Priority エリアの Switch Priority フィールドでドロップダウン リストをクリックし、デバイスを VLAN のルート スイッチとして設定するための値を選択します。

デフォルト値は 32768 です。
 - ステップ 9** (任意) Diameter フィールドでドロップダウン リストをクリックし、直径に設定する値を選択します。

直径のデフォルト値は 7 です。
 - ステップ 10** (任意) Hello Time フィールドでドロップダウン リストをクリックし、hello メッセージの間に設定する秒数を選択します。

hello タイムのデフォルトは 2 秒です。
 - ステップ 11** (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。
-

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状態にして、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。

Rapid-PVST+ ペインを使用して Rapid PVST+ のポートプライオリティ値を割り当てます(図 4-10 を参照)。

手順の詳細

個々のポートに Rapid PVST+ ポートプライオリティを割り当てるには、次の手順を実行します。

-
- ステップ 1** Feature Selector ペインで、**Switching > Spanning Tree > Rapid-PVST+** を選択して、Rapid-PVST+ ペインを表示します。
 - ステップ 2** Summary ペインで、**Device View** タブをクリックします。
 - ステップ 3** Summary ペインで、ポートプライオリティを設定する VLAN をクリックします。
Details ペインにタブが表示されます。
 - ステップ 4** Details タブをクリックします。
 - ステップ 5** Port Setting セクションをクリックします。
 - ステップ 6** プライオリティを設定するポートをクリックします。
 - ステップ 7** Priority フィールドでドロップダウンリストをクリックし、ポートの Rapid PVST+ プライオリティとして設定する値を選択します。
デフォルト値は 128 です。
 - ステップ 8** (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。
-

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。

Spanning Tree ペインを使用して Rapid PVST+ のパスコスト方式号を設定します (図 4-9 を参照)。

Rapid-PVST+ ペインを使用してポートの Rapid PVST+ コストを設定します (図 4-10 を参照)。

手順の詳細

Rapid PVST+ のパスコスト方式およびポート コストを設定するには、次の手順を実行します。

ステップ 1 Feature Selector ペインで、**Switching > Spanning Tree** を選択して、Spanning Tree ペインを表示します。

ステップ 2 Summary ペインで、設定するデバイスをクリックします。

Details ペインにタブが表示されます。

ステップ 3 Configuration タブをクリックします。

ステップ 4 Global Setting セクションをクリックします。

ステップ 5 Path Cost フィールドで、パスコスト方式としてロングまたはショートを選択します。

デフォルト パスコスト方式はショートです。

ステップ 6 メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。

ステップ 7 Feature Selector ペインで、**Switching > Spanning Tree > Rapid-PVST+** を選択して、Rapid-PVST+ ペインを表示します。

ステップ 8 Summary ペインで、**Device View** タブをクリックします。

ステップ 9 Summary ペインで、ポート プライオリティを設定する VLAN をクリックします。

Details ペインにタブが表示されます。

ステップ 10 Details タブをクリックします。

ステップ 11 Port Setting セクションをクリックします。

ステップ 12 コストを設定するポートをクリックします。

ステップ 13 Cost フィールドで、**auto** をクリックしてポートのコストをディセーブルにします。

デフォルト値は 128 です。

■ Rapid PVST+ の設定

ステップ 14 値を入力してポートのコストを設定します。

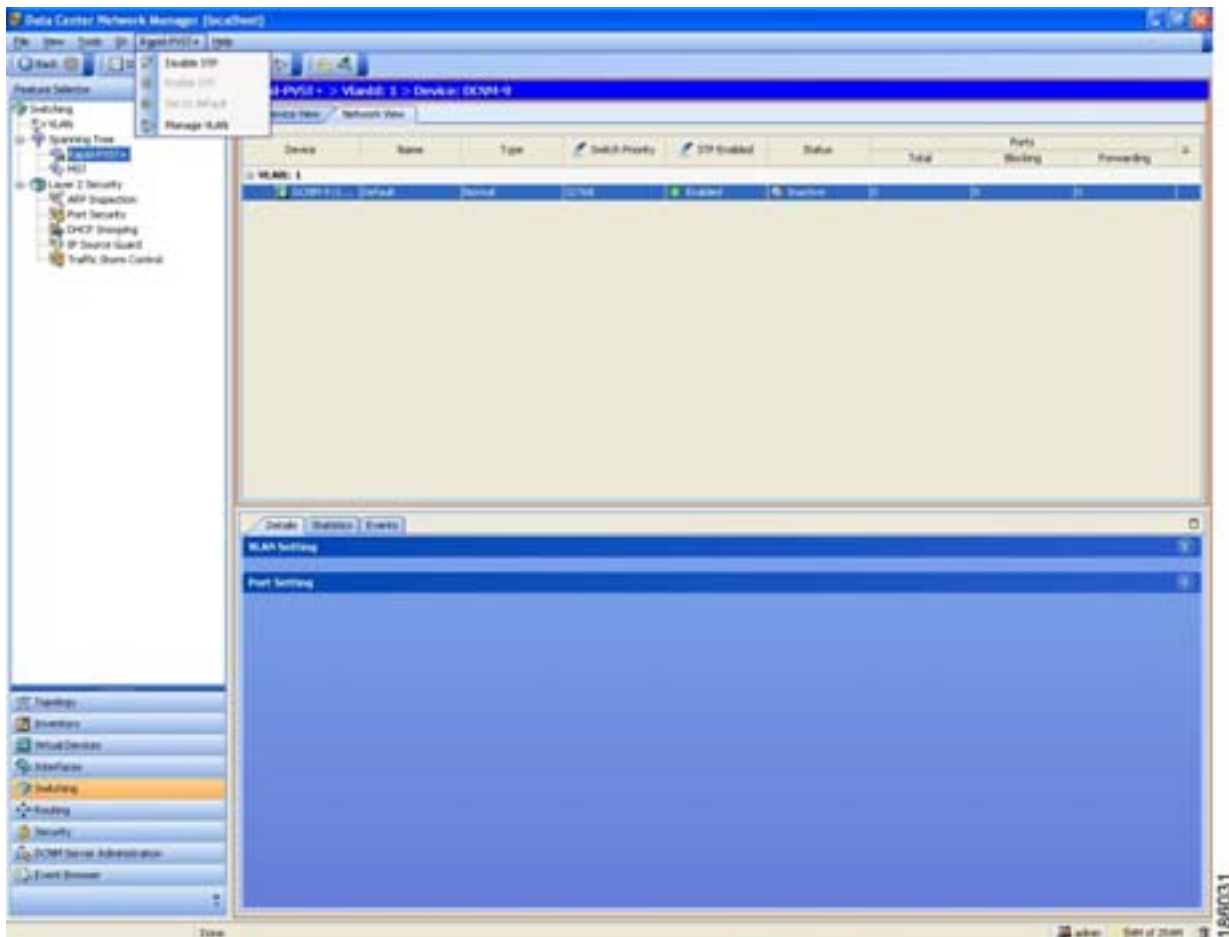
デフォルト方式であるショートパスコスト方式で有効な値は 1 ~ 65535 です。ロングパスコスト方式で有効な値は 1 ~ 200000000 です。デフォルトのポートコストはポートの帯域幅によって決定されます。

ステップ 15 (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。

インターフェイス別にすべての Rapid PVST+ パラメータをデフォルト値に設定

Rapid-PVST+ ペインを使用して、デバイスで特定の VLAN の特定のインターフェイスに設定されたすべての STP パラメータをデフォルトの Rapid PVST+ 値にリセットします (図 4-11 を参照)。

図 4-11 Rapid PVST+ 値の設定



手順の詳細

デバイスで特定の VLAN のインターフェイスに設定されたすべての STP パラメータをデフォルト値に設定するには、次の手順を実行します。

-
- ステップ 1** Feature Selector ペインで、**Switching > Spanning Tree > Rapid-PVST+** を選択して、Rapid-PVST+ ペインを表示します。
 - ステップ 2** Summary ペインで、**Network View** タブをクリックします。
 - ステップ 3** Summary ペインで、設定するデバイスをクリックします。

VLAN が含まれるデバイスが表示されます。
 - ステップ 4** デバイスをクリックします。

Summary ペインでデバイスが強調表示され、Details ペインにタブが表示されます。
 - ステップ 5** Details ペインで、**Details** タブをクリックします。
 - ステップ 6** Details タブで、**Port Setting** セクションをクリックします。

選択したデバイスの VLAN のインターフェイスが表示されます。
 - ステップ 7** インターフェイスをクリックします。

選択したインターフェイスが強調表示されます。
 - ステップ 8** メニューバーで **Rapid PVST+ > Set to default** を選択します。
 - ステップ 9** (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。
-

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。スパンニング 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。

Rapid-PVST+ ペインを使用して VLAN の hello タイムを設定します ([図 4-10](#) を参照)。

手順の詳細

Rapid PVST+ が有効な VLAN の hello タイムを設定するには、次の手順を実行します。

- ステップ 1** Feature Selector ペインで、**Switching > Spanning Tree > Rapid-PVST+** を選択して、Rapid-PVST+ ペインを表示します。
- ステップ 2** Summary ペインで、**Device View** タブをクリックします。
- ステップ 3** Summary ペインで、hello タイムを設定する VLAN をクリックします。

Details ペインにタブが表示されます。
- ステップ 4** Details タブをクリックします。
- ステップ 5** VLAN Settings セクションをクリックします。
- ステップ 6** Hello Time フィールドでドロップダウン リストをクリックし、hello メッセージの間に設定する秒数を選択します。

hello タイムのデフォルトは 2 秒です。
- ステップ 7** (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。

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。

Rapid-PVST+ ペインを使用して VLAN の転送遅延時間を設定します (図 4-10 を参照)。

手順の詳細

Rapid PVST+ が有効な VLAN の転送遅延時間を設定するには、次の手順を実行します。

-
- ステップ 1** Feature Selector ペインで、**Switching > Spanning Tree > Rapid-PVST+** を選択して、Rapid-PVST+ ペインを表示します。
 - ステップ 2** Summary ペインで、**Device View** タブをクリックします。
 - ステップ 3** Summary ペインで、hello タイムを設定する VLAN をクリックします。
Details ペインにタブが表示されます。
 - ステップ 4** Details タブをクリックします。
 - ステップ 5** VLAN Setting セクションをクリックします。
 - ステップ 6** Forward Delay Time フィールドで、転送遅延値に設定する秒数を入力します。
転送遅延時間のデフォルトは 15 秒です。
 - ステップ 7** (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。
-

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。

Rapid-PVST+ ペインを使用して VLAN の最大エージング タイムを設定します (図 4-10 を参照)。

手順の詳細

Rapid PVST+ が有効な VLAN の最大エージング タイムを設定するには、次の手順を実行します。

-
- ステップ 1** Feature Selector ペインで、**Switching > Spanning Tree > Rapid-PVST+** を選択して、Rapid-PVST+ ペインを表示します。
 - ステップ 2** Summary ペインで、**Device View** タブをクリックします。
 - ステップ 3** Summary ペインで、hello タイムを設定する VLAN をクリックします。
Details ペインにタブが表示されます。
 - ステップ 4** Details タブをクリックします。

ステップ 5 VLAN Setting セクションをクリックします。

ステップ 6 Max Age Time フィールドで、BPDU が期限切れになるまでに必要な秒数を入力します。

最大エージング タイムのデフォルトは 20 秒です。

ステップ 7 (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。

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 リンク上にものみ確立されます。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。

Spanning Tree ペインを使用してリンク タイプを設定します (図 4-9 を参照)。

手順の詳細

リンク タイプを設定するには、次の手順を実行します。

ステップ 1 Feature Selector ペインで、**Switching > Spanning Tree** を選択して、Spanning Tree ペインを表示します。

ステップ 2 Summary ペインで、デバイスをクリックします。

ステップ 3 Details ペインで、**Configuration** タブをクリックします。

ステップ 4 Details ペインで、**Port Setting** セクションをクリックします。

Port Setting セクションが展開します。

ステップ 5 Port Setting セクションで設定するインターフェイスをクリックします。

ステップ 6 Link Type カラムで、ドロップダウン リストをクリックしてリンク タイプを選択します。

Link Type のデフォルトは Auto です。

ステップ 7 (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。

統計情報の表示

Statistics タブに次のウィンドウが表示されます。

- Spanning Tree Statistics 送受信した BPDU を含む Rapid PVST+ の情報を表示します。

Rapid PVST+ のフィールドの説明

これらのフィールドの説明は、Rapid PVST+ の設定に使用されます。ここでは、次の内容について説明します。

- Device ビュー : VLAN : Details : VLAN Setting セクション (p.4-35)
- Device ビュー : VLAN : Details : Port Setting セクション (p.4-36)
- Network ビュー : デバイス : Details : VLAN Setting セクション (p.4-36)
- Network ビュー : デバイス : Details : Port Setting セクション (p.4-37)

Device ビュー : VLAN : Details : VLAN Setting セクション

表 4-5 Device ビュー : VLAN : Details : VLAN Setting セクション

フィールド	説明
VLAN	表示のみ。VLAN を一意に識別する番号
Device	表示のみ。デバイス名
Name	表示のみ。VLAN 名。デフォルトの名前は VLANXXXXX です。
Type	表示のみ。VLAN のタイプ。有効な値は以下のとおりです。 <ul style="list-style-type: none"> Normal Primary Secondary
Status	表示のみ。VLAN の STP の動作ステータス
Root Bridge MAC Address	表示のみ。ルートブリッジの MAC アドレス
Hello Time	デバイスでの hello メッセージのブロードキャスト間隔。デフォルト値は、2 秒です。
Forward Delay Time	ポートが転送を開始する前にラーニングステートでいる期間。デフォルト値は、15 秒です。
Max Age Time	プロトコル情報がポートに保管される期間。デフォルト値は、20 秒です。
STP	VLAN で STP がイネーブル/ディセーブルかのステータス。デフォルト値は Enabled です。
Switch Priority	
Switch Priority	ブリッジのプライオリティ。デフォルト値は 32768 です。
Root	Rapid PVST+ のプライマリまたはセカンダリルート。デフォルトは、ブランクです。
Diameter	レイヤ 2 ネットワークにおいて任意の 2 つのエンドステーション間で許可される最大ホップ数。デフォルトは、ブランクです。
Hello Time	hello メッセージのブロードキャスト間隔。デフォルトは、ブランクです。
Port Status	
Total Ports	表示のみ。VLAN に含まれるポート数
Blocking Ports	表示のみ。VLAN に含まれるポートで STP ブロッキングステートのポート数
Forwarding Ports	表示のみ。VLAN に含まれるポートで STP フォワーディングステートのポート数

Device ビュー : VLAN : Details : Port Setting セクション

表 4-6 Device ビュー : VLAN : Details : Port Setting セクション

フィールド	説明
Name	表示のみ。ポート名
Mode	表示のみ。ポートモード
Configuration	
Priority	STP ポート プライオリティ。デフォルト値は 128 です。
Cost	<ul style="list-style-type: none"> Auto インターフェイスのメディア速度から得た STP ポート コスト Value 手動で設定したポート コスト。有効値は 1 ~ 200000000 です。
Status	
Role	表示のみ。Rapid PVST+ ポート ロール。有効な値は以下のとおりです。 <ul style="list-style-type: none"> Root port Designated port Alternate port Backup port Disabled
State	表示のみ。Rapid PVST+ ポート ステート。有効な値は以下のとおりです。 <ul style="list-style-type: none"> Blocking Learning Forwarding Disabled
Priority	表示のみ。STP ポート プライオリティ。デフォルト値は 128 です。
Cost	表示のみ。STP ポート コスト。コスト値はインターフェイスのメディア スピードから取得します。有効値は 1 ~ 200000000 です。
Link Type	表示のみ。リンク タイプ。デフォルトは自動です。

Network ビュー : デバイス : Details : VLAN Setting セクション

表 4-7 Network ビュー : デバイス : Details : VLAN Setting セクション

フィールド	説明
VLAN	表示のみ。VLAN を一意に識別する番号
Device	表示のみ。デバイス名
Name	表示のみ。VLAN 名。デフォルトの名前は VLANXXXX です。
Type	表示のみ。VLAN のタイプ。有効な値は以下のとおりです。 <ul style="list-style-type: none"> Normal Primary Secondary
Status	表示のみ。VLAN の STP の動作ステータス
Root Bridge MAC Address	表示のみ。ルートブリッジの MAC アドレス
Hello Time	デバイスでの hello メッセージのプロードキャスト間隔。デフォルト値は、2 秒です。
Forward Delay Time	ポートが転送を開始する前にラーニングステートでいる期間。デフォルト値は、15 秒です。

表 4-7 Network ビュー : デバイス : Details : VLAN Setting セクション (続き)

フィールド	説明
Max Age Time	プロトコル情報がポートに保管される期間。デフォルト値は、20 秒です。
STP	VLAN で STP がイネーブル/ディセーブルかのステータス。デフォルト値は Enabled です。
Switch Priority	
Switch Priority	ブリッジのプライオリティ。デフォルト値は 32768 です。
Root	Rapid PVST+ のプライマリまたはセカンダリ ルート。デフォルトは、ブランクです。
Diameter	レイヤ 2 ネットワークにおいて任意の 2 つのエンドステーション間で許可される最大ホップ数。デフォルトは、ブランクです。
Hello Time	hello メッセージのブロードキャスト間隔。デフォルトは、ブランクです。
Port Status	
Total Ports	表示のみ。VLAN に含まれるポート数
Blocking Ports	表示のみ。VLAN に含まれるポートで STP ブロッキングステートのポート数
Forwarding Ports	表示のみ。VLAN に含まれるポートで STP フォワーディングステートのポート数

Network ビュー : デバイス : Details : Port Setting セクション

表 4-8 Network ビュー : デバイス : Details : Port Setting セクション

フィールド	説明
Name	表示のみ。ポート名
Mode	表示のみ。ポートモード
Configuration	
Priority	STP ポートプライオリティ。デフォルト値は 128 です。
Cost	<ul style="list-style-type: none"> Auto インターフェイスのメディア速度から得た STP ポートコスト Value 手動で設定したポートコスト。有効値は 1 ~ 200000000 です。
Status	
Role	<p>表示のみ。Rapid PVST+ ポートロール。有効な値は以下のとおりです。</p> <ul style="list-style-type: none"> Root port Designated port Alternate port Backup port Disabled
State	<p>表示のみ。Rapid PVST+ ポートステート。有効な値は以下のとおりです。</p> <ul style="list-style-type: none"> Blocking Learning Forwarding Disabled
Priority	表示のみ。STP ポートプライオリティ。デフォルト値は 128 です。
Cost	表示のみ。STP ポートコスト。コスト値はインターフェイスのメディアスピードから取得します。有効値は 1 ~ 200000000 です。
Link Type	表示のみ。リンクタイプ。有効値は shared と point-to-point です。

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.4-38)
- [標準規格](#) (p.4-38)
- [MIB](#) (p.4-38)

関連資料

関連トピック	マニュアル名
すべての VLAN	第 2 章「VLAN の設定」
MST	第 5 章「MST の設定」
STP 拡張機能	第 6 章「STP 拡張機能の設定」
NX-OS レイヤ 2 スイッチングの設定	『Cisco NX-OS Layer 2 Switching Configuration Guide』
レイヤ 2 インターフェイス	『Cisco DCNM Interfaces Configuration Guide』
DCNM の基本	『Cisco DCNM 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 DCNM Virtual Device Context Configuration Guide』
ライセンス	『Cisco DCNM Licensing Guide』
リリース ノート	『Cisco DCNM 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
<ul style="list-style-type: none"> • CISCO-STP-EXTENSION-MIB • BRIDGE-MIB 	<p>次の URL から、MIB の検索およびダウンロードができます。</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>



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。

Data Center Network Manager の機能の詳細については、『Cisco DCNM Fundamentals Configuration Guide』を参照してください。



(注)

Spanning Tree Protocol (STP; スパニング ツリー プロトコル) パラメータの設定に DCNM を使用する前に、使用しているデバイスのコマンドラインに NX-OS グローバル コマンドを入力してログレベルを設定する必要があります。

```
--logging-level spanning-tree 6
```

```
--logging logfile messages 6
```

```
--logging event link-status default
```

ログレベルについては、『Cisco NX-OS System Management Configuration Guide』を参照してください。



(注)

レイヤ 2 インターフェイスの作成方法については、『Cisco DCNM 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 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 が組み合わせられて、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。

VLAN 3968 ~ 4047 または VLAN 4094 を MST インスタンスにマッピングすることはできません。これらの VLAN は、デバイスによる内部使用のために予約されています。



(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、次の内容を説明します。

- [MST について \(p.5-3\)](#)
- [MST のライセンス要件 \(p.5-13\)](#)
- [MST の前提条件 \(p.5-13\)](#)
- [注意事項および制約事項 \(p.5-14\)](#)
- [MST の設定 \(p.5-15\)](#)
- [統計情報の表示 \(p.5-26\)](#)
- [MST のフィールドの説明 \(p.5-27\)](#)
- [追加情報 \(p.5-32\)](#)



(注) STP および Rapid PVST+ の詳細については、[第4章「Rapid PVST+ の設定」](#)、STP 拡張機能の詳細については、[第6章「STP 拡張機能の設定」](#)を参照してください。

MST について



(注) STP パラメータの設定に DCNM を使用する前に、使用しているデバイスのコマンドラインに `logging-level spanning-tree 6` および `logging logfile messages 6 NX-OS` グローバル コマンドを入力してログレベルを設定する必要があります。ロ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。



(注) レイヤ 2 インターフェイスの作成方法については、『*Cisco DCNM 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、スパンニング 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ンニング 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、領域外のスパンニング 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; スパンニング 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) スパンニング 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 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 \(p.5-3\)](#)
- [MST 領域 \(p.5-4\)](#)
- [MST BPDU \(p.5-5\)](#)
- [MST コンフィギュレーション情報 \(p.5-5\)](#)
- [IST、CIST、および CST \(p.5-6\)](#)
- [ホップカウント \(p.5-8\)](#)
- [境界ポート \(p.5-9\)](#)
- [単一方向リンク障害の検出 \(p.5-9\)](#)
- [ポートコストおよびポート プライオリティ \(p.5-10\)](#)
- [IEEE 802.1D との相互運用性 \(p.5-11\)](#)
- [ハイ アベイラビリティ \(p.5-11\)](#)
- [パーチャライゼーションのサポート \(p.5-12\)](#)

MST の概要



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

MST は、複数の VLAN をスパンニング 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ンニング ツリー インスタンスとは別のスパンニング 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) に影響しないので、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 4 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 4 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、スパンニング 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 スパンニング 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.5-5] 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; 内部スパンニング 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.5-6] 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。



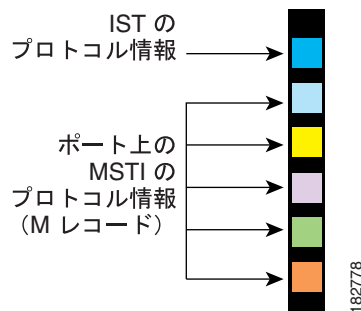
(注)

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 5-1 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.5-6] 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 5-1 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 個の要素を含むテーブル。先頭要素 (0) および最終要素 (4095) は 0 に設定されています。要素番号 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ものとみなします。

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 \(p.5-6\)](#)
- [MST 領域内のスパンニング ツリー動作 \(p.5-6\)](#)
- [MST 領域間のスパンニング ツリー動作 \(p.5-7\)](#)
- [MST 用語 \(p.5-8\)](#)

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4章「Rapid PVST+ の設定」](#)を参照) と異なり、MST は IST、CIST、および CST スパンニング 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ンニング ツリーです。
MST は各 MST 領域内でその他のスパンニング ツリーを確立して、維持します。これらのスパンニング 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ンニング 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ンニング 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 領域内のスパンニング ツリー動作](#)」(p.5-6) および「[MST 領域間のスパンニング ツリー動作](#)」(p.5-7) を参照してください。

MST 領域内のスパンニング 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 5-2 \[p.5-7\]](#)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。

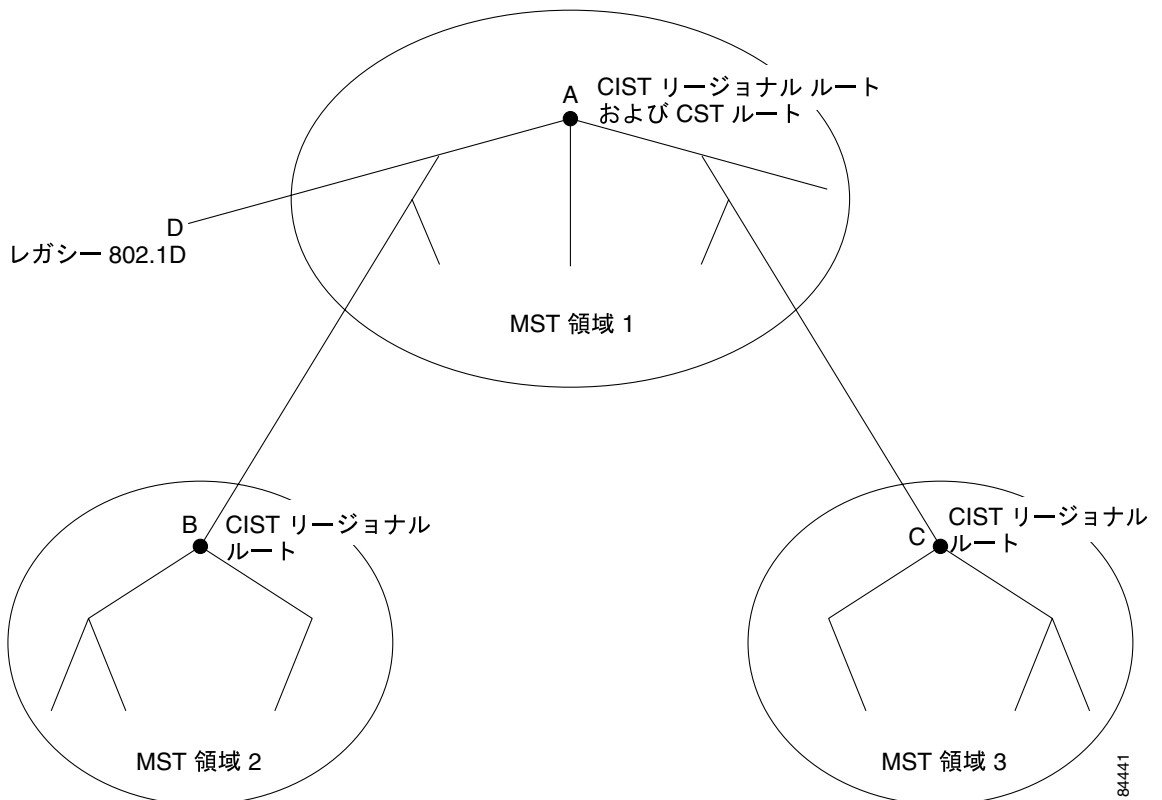
MST 領域間のスパニング ツリー動作

ネットワーク内に複数の領域、または 802.1w 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 5-2 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 5-2 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 は自身のスパンニング 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、最終的なスパンニング 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ンニング 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。スパンニング 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ンニング 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、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。

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。

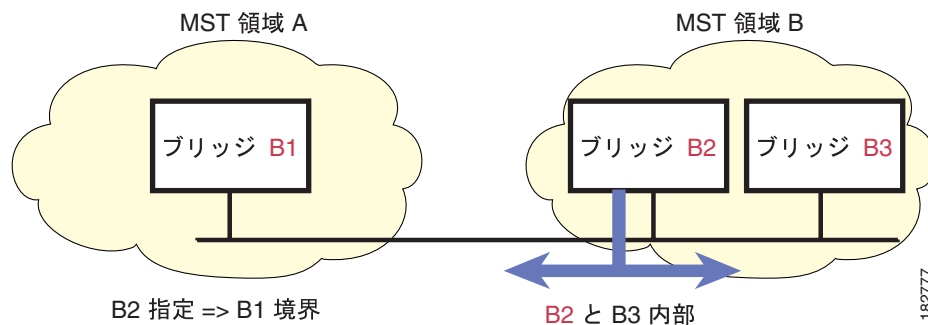
BPDU の 802.1w 部分に格納されているメッセージ有効期間および最大エージング タイムの情報は、領域全体で同じです (IST の場合のみ)。同じ値が、境界にある領域の指定ポートによって伝播されます。

最大エージング タイムは、デバイスがスパンニング 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 5-3 を参照）。

図 5-3 MST 境界ポート



境界では、MST ポートの役割は重要ではありません。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.5-14] 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。



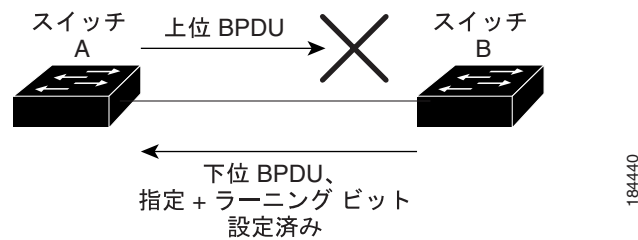
(注)

Unidirectional Link Detection (UDLD; 単方向リンク検出)の詳細については、『*Cisco DCNM Interface 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 5-4 に、ブリッジング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、ブリッジンググループが回避されます。

図 5-4 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 6 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、インターフェー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 802.1D 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ンニングツリー 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。

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。Cisco NX-OS Release 4.0(2) 以降のリリースでは、指定したインターフェイスから先行標準の MSTP メッセージを常時送信するよう設定できます。先行標準 MST メッセージを受信するまで待機せずに、先行標準 MST メッセージの送信を開始できます。

インターフェイスによるプロアクティブな先行標準 MSTP メッセージの送信の設定に関する詳細については、『*Cisco NX-OS Layer 2 Configuration Guide*』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 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。

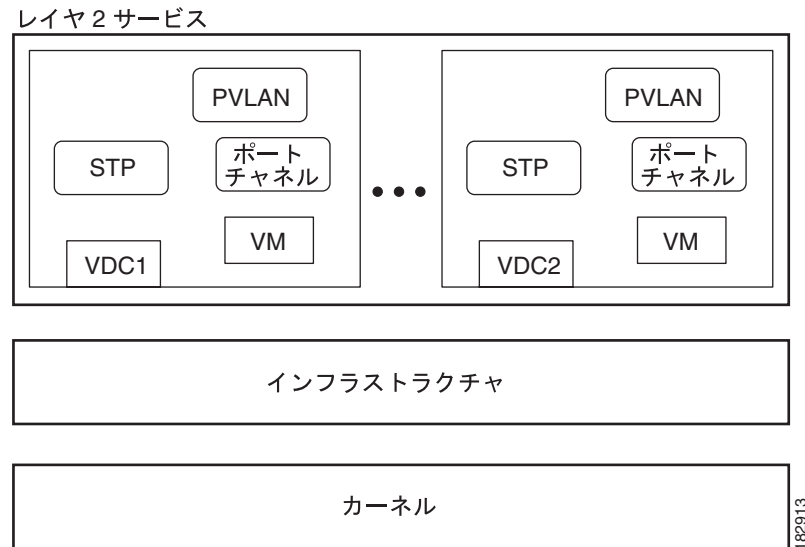


(注) ハイ アベイラビリティ機能の詳細については、『*Cisco NX-OS High Availability and Redundancy Configuration Guide*』を参照してください。

バーチャライゼーションのサポート

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 5-5 を参照)。

図 5-5 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。



(注) VDC およびリソースの割り当ての詳細については、『Cisco DCNM 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
DCNM	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 DCNMに組み込まれており、無料で提供されます。DCNMライセンススキームの詳細については、『 <i>Cisco DCNM Licensing Guide</i> 』を参照してください。
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ライセンス機構の詳細については、『 <i>Cisco NX-OS Licensing Guide</i> 』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、ログレベルを設定する必要があります。ロ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。
- 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。
- 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。
- VLAN 3968 ~ 4047 または VLAN 4094 を MST インスタンスにマッピングすることはできません。これらの VLAN は、デバイスによる内部使用のために予約されています。
- 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.5-21] を参照)。
- 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ない、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。

MST の設定



(注) デバイスで Rapid PVST+ を実行している場合、MST のプリプロビジョニングを行うことができます。メインメニューで、**Tools > Global Preferences > Pre Provisioning** を選択し、この機能の有効化と表示を行う画面にアクセスしたり、画面を非表示にしたりできます。プリプロビジョニングについては、『*Cisco DCNM Fundamentals 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。

- [MST のイネーブル化 \(p.5-15\)](#)
- [MST 名およびリビジョンの指定 \(p.5-17\)](#)
- [MST のデフォルト値への設定 \(p.5-17\)](#)
- [MST インスタンスの追加およびインスタンスと VLAN のマッピング \(p.5-18\)](#)
- [MST インスタンスの削除 \(p.5-20\)](#)
- [VLAN と MSTI のマッピングおよびマッピング解除 \(p.5-21\)](#)
- [プライマリおよびセカンダリ ルートとスイッチ プライオリティの設定 \(p.5-22\)](#)
- [ポート プライオリティおよび MST ポートのコストの設定 \(p.5-23\)](#)
- [ポートごとのデフォルト MST 値の設定 \(p.5-24\)](#)
- [hello タイム、転送遅延時間、最大エージング タイム、最大ホップ カウントの設定 \(p.5-25\)](#)
- [リンク タイプの指定 \(p.5-26\)](#)

MST のイネーブル化

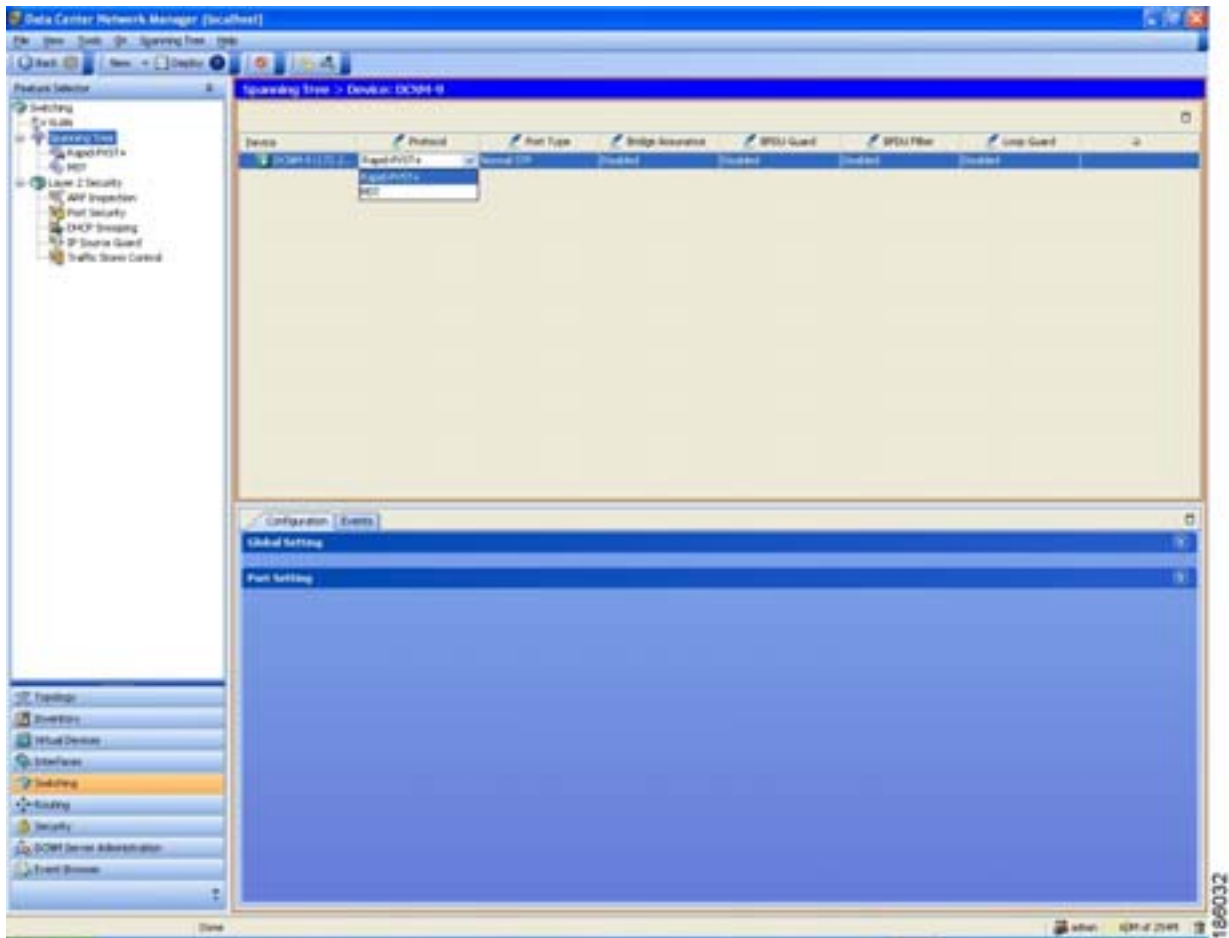
MST をイネーブルにできます。デフォルトは、Rapid PVST+ です。



(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。

Spanning Tree ペインを使用して MST をイネーブルにします ([図 5-6](#) を参照)。

図 5-6 MST のイネーブル化



手順の詳細

デバイスで MST をイネーブルにするには、次の手順を実行します。

-
- ステップ 1** Feature Selector ペインで、**Switching > Spanning Tree** を選択して、Spanning Tree ペインを表示します。
 - ステップ 2** Summary ペインで、MST をイネーブルにするデバイスをクリックします。
Rapid PVST+ はすべての VLAN でデフォルトでイネーブルです。
 - ステップ 3** Protocol フィールドで、ドロップダウン リストをクリックして **MST** を選択します。
 - ステップ 4** (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。
-



- (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、トラフィックは中断されます。

MST 名およびリビジョンの指定

ブリッジに名前と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。

Spanning Tree ペインを使用して MST 名およびリビジョン番号を設定します (図 5-6 を参照)。

手順の詳細

MST 名とリビジョン番号を設定するには、次の手順を実行します。

-
- ステップ 1** Feature Selector ペインで、**Switching > Spanning Tree** を選択して、Spanning Tree ペインを表示します。
 - ステップ 2** Summary ペインで、MST 名とリビジョン番号を指定するデバイスをクリックします。

Summary ペインでデバイスが強調表示され、Details ペインにタブが表示されます。
 - ステップ 3** Details ペインで、**Configuration** タブをクリックします。
 - ステップ 4** **Global Setting** セクションをクリックします。
 - ステップ 5** MST Setting エリアの Name フィールドに、ブリッジの MST 名を入力します。

デフォルトは、ブランクです。
 - ステップ 6** MST Setting エリアの Revision Number フィールドに、MST リビジョン番号を入力します。

デフォルトは、0 です。
 - ステップ 7** (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。
-

MST のデフォルト値への設定

Spanning Tree ペインを使用して MST をデフォルト値に設定します (図 5-6 を参照)。

手順の詳細

MST をデフォルト値に設定するには、次の手順を実行します。

-
- ステップ 1** Feature Selector ペインで、**Switching > Spanning Tree** を選択して、Spanning Tree ペインを表示します。
 - ステップ 2** MST をデフォルト値に設定するデバイスを選択します。
 - ステップ 3** メニューバーで **Spanning Tree > Set to default** を選択します。

この操作によって名前とリビジョン番号が削除され、すべての VLAN が MST インスタンス 0 に戻されます。

ステップ4 (任意)メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。

MST インスタンスの追加およびインスタンスと VLAN のマッピング

VLAN 3968 ~ 4047 または VLAN 4094 を MST インスタンスにマッピングすることはできません。これらの VLAN は、デバイスによる内部使用のために予約されています。

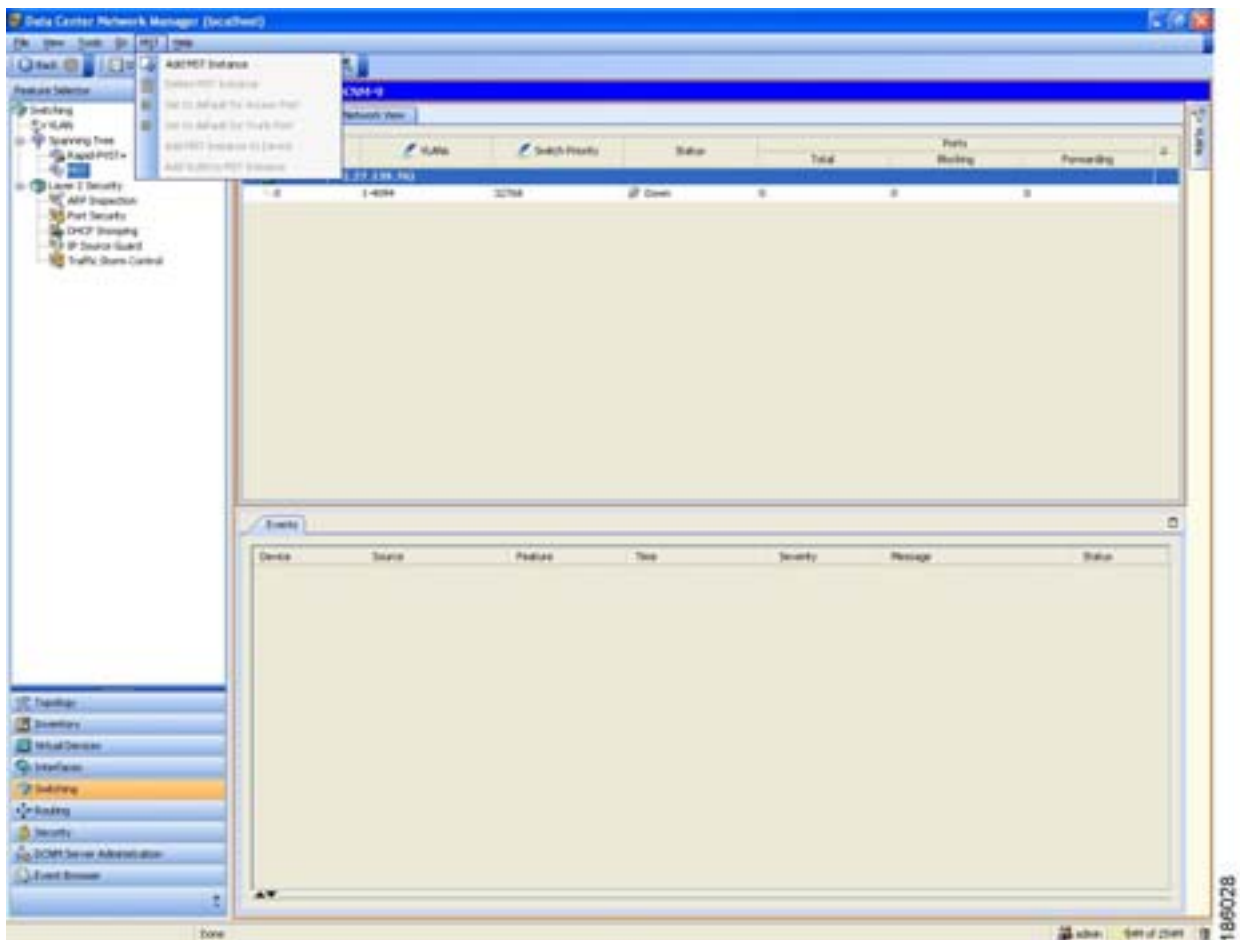


(注)

すべてのデバイスが同じ MST 領域に含まれるよう、すべてのデバイスで MST 名とリビジョン番号に同一の内容を指定し、すべてのデバイスで VLAN/MST インスタンス間マッピングが同一になるようにします。

MST ペインを使用して MST を追加し、VLAN をインスタンスにマッピングします([図 5-7](#) を参照)。

図 5-7 MST の設定



手順の詳細

MST インスタンスを追加するには、次の手順を実行します。

ステップ 1 Feature Selector ペインで、**Switching > Spanning Tree > MST** を選択して、MST ペインを表示します。

ステップ 2 Summary ペインで、**Device View** タブをクリックします。

ステップ 3 Summary ペインで、MST インスタンスを追加または削除するデバイスをクリックします。

Summary ペインが展開し、デバイスに現在設定されている MST インスタンスが表示されます。

ステップ 4 メニューバーで **MST > Add MST Instance** を選択します。

システムによってインスタンスが追加されます。MST ID と VLAN フィールドはブランクのままです。

ステップ 5 MST ID フィールドに新しい MST 用の番号を入力します。

ステップ 6 VLANs フィールドに、新しい MST にマッピングする VLAN を入力します。



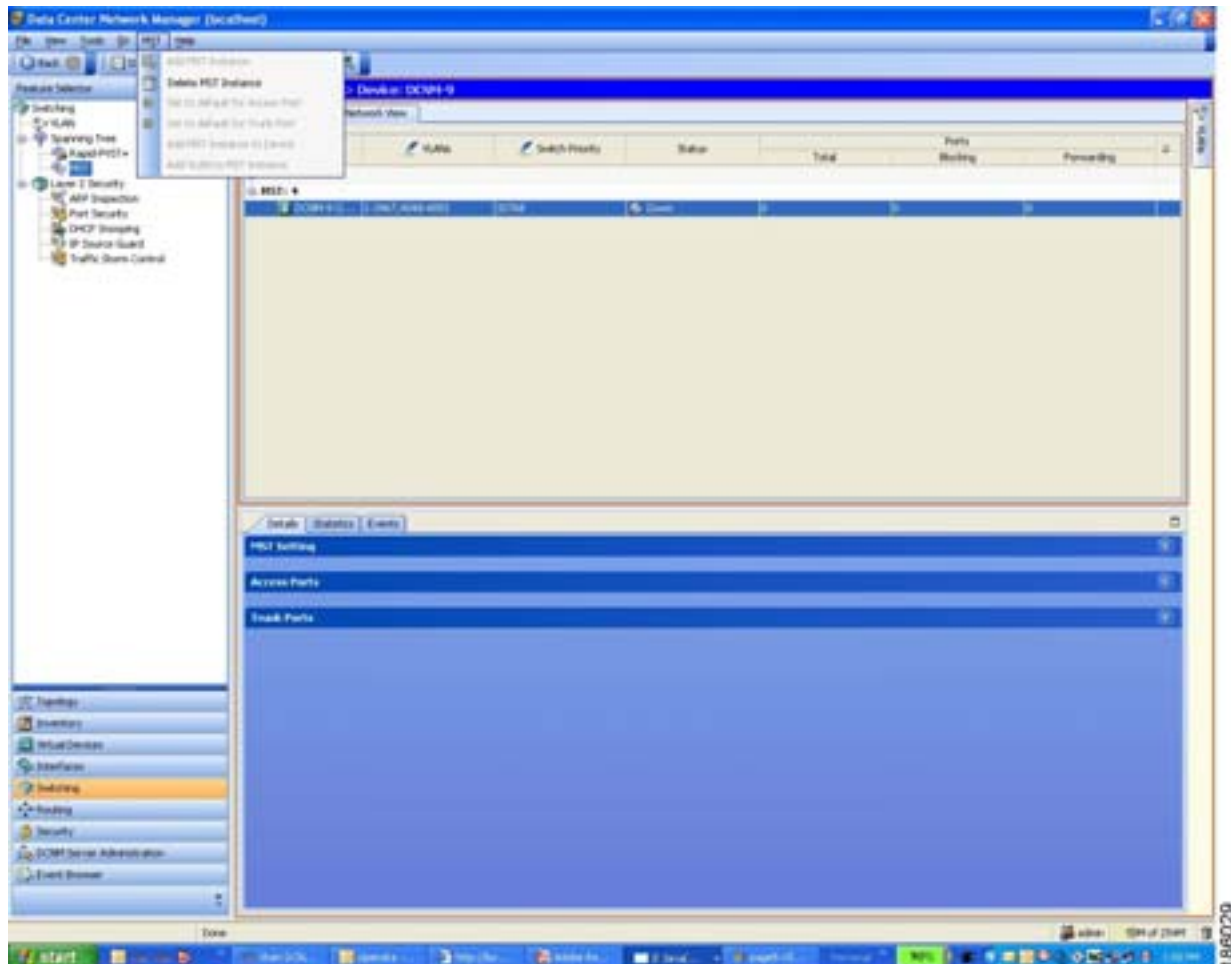
(注) 新しく作成した MST インスタンスには、VLAN を最低 1 つ追加する必要があります。

ステップ 7 (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。

MST インスタンスの削除

MST ペインを使用して MST インスタンスを削除します (図 5-8 を参照)。

図 5-8 MST インスタンスの削除



手順の詳細

MST インスタンスを削除するには、次の手順を実行します。

-
- ステップ 1** Feature Selector ペインで、Switching > Spanning Tree > MST を選択して、MST ペインを表示します。
 - ステップ 2** Summary ペインで、Network View タブをクリックします。
 - ステップ 3** Summary ペインで、MST instance をクリックします。
Summary ペインが展開し、その MST インスタンスが現在設定されているデバイスが表示されます。
 - ステップ 4** メニューバーで MST > Delete MST Instance を選択します。
 - ステップ 5** (任意) メニューバーで File > Deploy を選択し、デバイスに変更を適用します。
-

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。

VLAN 3968 ~ 4047 または VLAN 4094 を MST インスタンスにマッピングすることはできません。これらの VLAN は、デバイスによる内部使用のために予約されています。



(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。

MST ペインを使用して VLAN/MST インスタンス間マッピングを作成します (図 5-7 を参照)。

手順の詳細

VLAN と MST インスタンスのマッピングおよびマッピング解除を行うには、次の手順を実行します。

- ステップ 1** Feature Selector ペインで、**Switching > Spanning Tree > MST** を選択して、MST ペインを表示します。
- ステップ 2** Summary ペインで、**Device View** タブをクリックします。
- ステップ 3** Summary ペインで、MST インスタンスを追加または削除するデバイスをクリックします。
Summary ペインが展開し、デバイスに現在設定されている MST インスタンスが表示されます。
- ステップ 4** VLAN を追加または削除する MST をクリックします。
- ステップ 5** メニューバーで **MST > Add VLAN to MST Instance** を選択します。
- ステップ 6** 新しい MST に VLAN を追加します。
- ステップ 7** (任意) メニューバーで **MST Remove VLAN** を選択し、MST インスタンスから VLAN を削除してマッピングを解除します。
- ステップ 8** (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。

プライマリおよびセカンダリ ルートとスイッチ 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、プライマリおよびセカンダリ ルートまたは MST インスタンスのスイッチ プライオリティを設定できます。この設定では、直径と hello タイムの選択も行うことができます。



(注) 特定のスイッチ プライオリティ値を設定するよりも、プライマリおよびセカンダリ ルートを指定することを推奨します。

複数のバックアップ ルート ブリッジを設定する場合は、複数のデバイスをセカンダリ ルートとして指定する必要があります。プライマリ ルート ブリッジを設定するときに使用したのと同じネットワーク直径および hello タイムをセカンダリ ルートに使用してください。

MST ペインを使用して、デバイスをプライマリまたはセカンダリ ルートに設定し、スイッチ プライオリティを設定します (図 5-8 を参照)。

手順の詳細

プライマリおよびセカンダリ ルートの設定またはスイッチ プライオリティの設定を行うには、次の手順を実行します。

- ステップ 1** Feature Selector ペインで、**Switching > MST** を選択して、MST ペインを表示します。
- ステップ 2** Summary ペインで、設定するデバイスをクリックします。
Summary ペインが展開し、MST インスタンスが表示されます。
- ステップ 3** Summary ペインで、プライマリおよびセカンダリ ルート、またはスイッチ プライオリティを指定する MST インスタンスをクリックします。
Details ペインにタブが表示されます。
- ステップ 4** Details ペインで、**Details** タブをクリックします。
- ステップ 5** Details タブで、**MST Setting** セクションをクリックします。
- ステップ 6** (任意) Switch Priority エリアの Root フィールドでドロップダウン リストをクリックし、**primary** をクリックしてデバイスをプライマリ ルートに設定します。
- ステップ 7** (任意) Switch Priority エリアの Root フィールドでドロップダウン リストをクリックし、**secondary** をクリックしてデバイスをセカンダリ ルートに設定します。
- ステップ 8** (任意) Switch Priority エリアの Switch Priority フィールドでドロップダウン リストをクリックし、スイッチ プライオリティ値をクリックしてスイッチ プライオリティを特定の値に設定します。
- ステップ 9** Diameter フィールドでドロップダウン リストをクリックし、直径に設定する値をクリックします。
直径のデフォルト値は 7 です。

ステップ 10 Hello Time フィールドでドロップダウン リストをクリックし、hello タイム メッセージの間隔（秒数）に設定する値をクリックします。

hello タイムのデフォルト値は 2 秒です。

ステップ 11（任意）メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。

ポート プライオリティおよび MST ポートのコストの設定

ループが発生すると、MST はポート プライオリティとコストを使用して、フォワーディング ステートにするインターフェイスを選択します。MST パス コストのデフォルト値は、インターフェイスのメディア速度から取得されます。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およびコスト値を、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および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。

MST ペインを使用して、MST アクセス ポートおよびトランク ポート別にポート プライオリティおよびポート コスト値を設定します（[図 5-8](#) を参照）。

手順の詳細

ポート プライオリティおよびポート コストを設定するには、次の手順を実行します。

ステップ 1 Feature Selector ペインで、**Switching > MST** を選択して、MST ペインを表示します。

ステップ 2 Summary ペインで、設定するデバイスをクリックします。

Summary ペインが展開し、MST インスタンスが表示されます。

ステップ 3 Summary ペインで、ポート プライオリティおよびポート コストを設定する MST インスタンスをクリックします。

Details ペインにタブが表示されます。

ステップ 4 Details ペインで、**Details** タブをクリックします。

ステップ 5 Details タブで、**Access Ports** セクションをクリックしてアクセス ポートを設定するか、**Trunk Ports** セクションをクリックしてトランク ポートを設定します。

セクションが展開し、MST インスタンスのポートが表示されます。

ステップ 6 プライオリティおよびコストを設定するポートをクリックします。

ステップ 7 Priority フィールドでドロップダウン リストをクリックし、ポートの MST プライオリティとして設定する値を選択します。

デフォルト値は 128 です。

ステップ 8 Cost フィールドで、**auto** をクリックしてポートのコストをディセーブルにします。

デフォルト値は 128 です。

ステップ 9 値を入力してポートのコストを設定します。

デフォルトのポート コストは、ポートの帯域幅から判別されます。

ステップ 10 (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。

ポートごとのデフォルト MST 値の設定

MST アクセス ポートおよびトランク ポート別にデフォルト値を設定します (図 5-8 を参照)。

手順の詳細

特定のポートのデフォルト MST 値を設定するには、次の手順を実行します。

ステップ 1 Feature Selector ペインで、**Switching > MST** を選択して、MST ペインを表示します。

ステップ 2 Summary ペインで、設定するデバイスをクリックします。

Summary ペインが展開し、MST インスタンスが表示されます。

ステップ 3 Summary ペインで、ポート プライオリティおよびポート コストを設定する MST インスタンスをクリックします。

Details ペインにタブが表示されます。

ステップ 4 Details ペインで、**Details** タブをクリックします。

ステップ 5 Details タブで、**Access Ports** セクションをクリックしてアクセス ポートを設定するか、**Trunk Ports** セクションをクリックしてトランク ポートを設定します。

セクションが展開し、MST インスタンスのポートが表示されます。

ステップ 6 MST デフォルト値を設定するポートをクリックします。

ステップ 7 メニューバーで、**MST > Set to default for Access Port** を選択してアクセス ポートのデフォルトを設定するか、**Set to default for Trunk Port** を選択してトランク ポートのデフォルトを設定します。

ステップ 8 (任意) メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。

hello タイム、転送遅延時間、最大エージング タイム、最大ホップ カウントの設定

hello タイムは、デバイス上のすべてのインスタンスに対してルート ブリッジが生成する設定メッセージの間隔です。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。領域内の最大ホップを設定し、それをその領域内にあるすべての MST インスタンスに適用できます。ホップ カウントは、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。

Spanning Tree ペインを使用して、hello タイム、転送遅延時間、最大エージング タイム、最大ホップ カウントを設定します（図 5-6 を参照）。

手順の詳細

MST の hello タイム、転送遅延時間、最大エージング タイム、最大ホップ カウントを設定するには、次の手順を実行します。

-
- ステップ 1** Feature Selector ペインで、**Switching > Spanning Tree** を選択して、Spanning Tree ペインを表示します。
 - ステップ 2** Summary ペインで、MST 名とリビジョン番号を指定するデバイスをクリックします。

Summary ペインでデバイスが強調表示され、Details ペインにタブが表示されます。
 - ステップ 3** Details ペインで、**Configuration** タブをクリックします。
 - ステップ 4** **Global Setting** セクションをクリックします。
 - ステップ 5** MST Setting エリアの Hello Time フィールドでドロップダウン リストをクリックし、hello タイムに設定する値を選択します。

デフォルトは、2 秒です。
 - ステップ 6** MST Setting エリアの Forwarding Delay Time フィールドで、転送遅延時間に設定する値を入力します。

デフォルトは、15 秒です。
 - ステップ 7** MST Setting エリアの Max Age Time フィールドで、最大エージング タイムに設定する値を入力します。

デフォルトは、20 秒です。
 - ステップ 8** MST Setting エリアの Max Hop Count フィールドで、最大ホップ カウントに設定する値を入力します。

デフォルトは、20 です。
 - ステップ 9** （任意）メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。
-

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 リンク上にものみ確立されます。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。

Spanning Tree ペインを使用してリンク タイプを設定します（[図 5-6](#) を参照）。

手順の詳細

リンク タイプを設定するには、次の手順を実行します。

ステップ 1 Feature Selector ペインで、**Switching > Spanning Tree** を選択して、Spanning Tree ペインを表示します。

ステップ 2 Summary ペインで、デバイスをクリックします。

ステップ 3 Details ペインで、**Configuration** タブをクリックします。

ステップ 4 Details ペインで、**Port Setting** セクションをクリックします。

Port Setting セクションが展開します。

ステップ 5 Port Setting セクションで設定するインターフェイスをクリックします。

ステップ 6 Link Type カラムで、ドロップダウン リストをクリックしてリンク タイプを選択します。

Link Type のデフォルトは Auto です。

ステップ 7 （任意）メニューバーで **File > Deploy** を選択し、デバイスに変更を適用します。

統計情報の表示

Statistics タブに次のウィンドウが表示されます。

- Spanning Tree Statistics 送受信した BPDU を含む Rapid PVST+ の情報を表示します。


MSTのフィールドの説明

これらのフィールドの説明は、MSTの設定に使用されます。ここでは、次の内容について説明します。

- [Device ビュー：インスタンス：Details：MST Settings セクション \(p.5-27\)](#)
- [Device ビュー：インスタンス：Details：Access Ports セクション \(p.5-28\)](#)
- [Device ビュー：インスタンス：Details：Trunk Ports セクション \(p.5-29\)](#)
- [Network ビュー：デバイス：Details：MST Settings セクション \(p.5-30\)](#)
- [Network ビュー：デバイス：Details：Access Ports セクション \(p.5-30\)](#)
- [Network ビュー：デバイス：Details：Trunk Ports セクション \(p.5-31\)](#)

Device ビュー：インスタンス：Details：MST Settings セクション

表 5-1 Device ビュー：インスタンス：Details：MST Settings セクション

フィールド	説明
MST Instance	表示のみ。MST インスタンスを一意に識別する番号
Device	表示のみ。VLAN の設定対象デバイス名
VLANs	MST インスタンスに含まれる VLAN。デフォルトは、VLAN1 です。  (注) インスタンス 0 で作業する場合は、このフィールドを変更することはできません。
Switch Priority	
Switch Priority	ブリッジのプライオリティ。デフォルト値は 32768 です。
Root	Rapid PVST+ のプライマリまたはセカンダリ ルート。デフォルトは、ブランクです。
Diameter	レイヤ 2 ネットワークにおいて任意の 2 つのエンド ステーション間で許可される最大ホップ数。デフォルトは、ブランクです。
Hello Time	hello メッセージのブロードキャスト間隔。デフォルトは、ブランクです。
Port Status	
Total Ports	表示のみ。MST インスタンスに含まれるポート数
Blocking Ports	表示のみ。MST インスタンスに含まれるポートで STP ブロッキング ステートのポート数
Forwarding Ports	表示のみ。MST インスタンスに含まれるポートで STP フォワーディング ステートのポート数

Device ビュー : インスタンス : Details : Access Ports セクション

表 5-2 Device ビュー : インスタンス : Details : Access Ports セクション

フィールド	説明
Name	表示のみ。ポート名
Mode	表示のみ。ポートモード
Configuration	
Priority	MST ポート プライオリティデフォルト値は 128 です。
Cost	<ul style="list-style-type: none"> Auto インターフェイスのメディア速度から得た STP ポート コスト Value 手動で設定したポート コスト。有効値は 1 ~ 200000000 です。
Status	
Role	<p>表示のみ。MST ポート ロール。有効な値は以下のとおりです。</p> <ul style="list-style-type: none"> Root port Designated port Alternate port Backup port Disabled
State	<p>表示のみ。MST ポート ステート。有効な値は以下のとおりです。</p> <ul style="list-style-type: none"> Blocking Learning Forwarding Disabled
Priority	表示のみ。MST ポート プライオリティ。デフォルト値は 128 です。
Cost	表示のみ。MST ポート コスト。コスト値はインターフェイスのメディア スピードから取得します。有効値は 1 ~ 200000000 です。
Link Type	表示のみ。リンク タイプ。デフォルトは自動です。
Boundary Port	表示のみ。MST 領域間の境界ポートを表示します。
PreStd Port	表示のみ。MST 領域間のポートおよび先行標準ポートを表示します。


Device ビュー : インスタンス : Details : Trunk Ports セクション

表 5-3 Device ビュー : インスタンス : Details : Trunk Ports セクション

フィールド	説明
Name	表示のみ。ポート名
Configuration	
Priority	MST ポート プライオリティデフォルト値は 128 です。
Cost	<ul style="list-style-type: none"> • Auto インターフェイスのメディア速度から得た STP ポート コスト • Value 手動で設定したポート コスト。有効値は 1 ~ 200000000 です。
Status	
Role	<p>表示のみ。MST ポート ロール。有効な値は以下のとおりです。</p> <ul style="list-style-type: none"> • Root port • Designated port • Alternate port • Backup port • Disabled
State	<p>表示のみ。MST ポート ステート。有効な値は以下のとおりです。</p> <ul style="list-style-type: none"> • Blocking • Learning • Forwarding • Disabled
Priority	表示のみ。MST ポート プライオリティ。デフォルト値は 128 です。
Cost	表示のみ。MST ポート コスト。コスト値はインターフェイスのメディア スピードから取得します。有効値は 1 ~ 200000000 です。
Link Type	表示のみ。リンク タイプ。デフォルトは自動です。
Boundary Port	表示のみ。
PreStd Port	表示のみ。

Network ビュー : デバイス : Details : MST Settings セクション

表 5-4 Network ビュー : デバイス : Details : MST Settings セクション

フィールド	説明
MST Instance	表示のみ。MST インスタンスを一意に識別する番号
Device	表示のみ。VLAN の設定対象デバイス名
VLANs	MST インスタンスに含まれる VLAN。デフォルトは、VLAN1 です。  (注) インスタンス 0 で作業する場合は、このフィールドを変更することはできません。
Switch Priority	
Switch Priority	ブリッジのプライオリティ。デフォルト値は 32768 です。
Root	Rapid PVST+ のプライマリまたはセカンダリ ルート。デフォルトは、ブランクです。
Diameter	レイヤ 2 ネットワークにおいて任意の 2 つのエンド ステーション間で許可される最大ホップ数。デフォルトは、ブランクです。
Hello Time	hello メッセージのブロードキャスト間隔。デフォルトは、ブランクです。
Port Status	
Total Ports	表示のみ。MST インスタンスに含まれるポート数
Blocking Ports	表示のみ。MST インスタンスに含まれるポートで STP ブロッキング ステートのポート数
Forwarding Ports	表示のみ。MST インスタンスに含まれるポートで STP フォワーディング ステートのポート数

Network ビュー : デバイス : Details : Access Ports セクション

表 5-5 Network ビュー : デバイス : Details : Access Ports セクション

フィールド	説明
Name	表示のみ。ポート名
Mode	表示のみ。ポート モード
Configuration	
Priority	MST ポート プライオリティデフォルト値は 128 です。
Cost	<ul style="list-style-type: none"> Auto インターフェイスのメディア速度から得た STP ポート コスト Value 手動で設定したポート コスト。有効値は 1 ~ 200000000 です。
Status	
Role	表示のみ。MST ポート ロール。有効な値は以下のとおりです。 <ul style="list-style-type: none"> Root port Designated port Alternate port Backup port Disabled
State	表示のみ。MST ポート ステート。有効な値は以下のとおりです。 <ul style="list-style-type: none"> Blocking Learning Forwarding Disabled

表 5-5 Network ビュー : デバイス : Details : Access Ports セクション (続き)

フィールド	説明
Priority	表示のみ。MST port priority. デフォルト値は 128 です。
Cost	表示のみ。MST ポート コスト。コスト値はインターフェイスのメディア スピードから取得します。有効値は 1 ~ 200000000 です。
Link Type	表示のみ。リンク タイプ。デフォルトは自動です。
Boundary Port	表示のみ。
PreStd Port	表示のみ。

Network ビュー : デバイス : Details : Trunk Ports セクション

表 5-6 Network ビュー : デバイス : Details : Trunk Ports セクション

フィールド	説明
Name	表示のみ。ポート名
Configuration	
Priority	MST ポート プライオリティデフォルト値は 128 です。
Cost	<ul style="list-style-type: none"> Auto インターフェイスのメディア速度から得た STP ポート コスト Value 手動で設定したポート コスト。有効値は 1 ~ 200000000 です。
Status	
Role	表示のみ。MST ポート ロール。有効な値は以下のとおりです。 <ul style="list-style-type: none"> Root port Designated port Alternate port Backup port Disabled
State	表示のみ。MST ポート ステート。有効な値は以下のとおりです。 <ul style="list-style-type: none"> Blocking Learning Forwarding Disabled
Priority	表示のみ。MST ポート プライオリティ。デフォルト値は 128 です。
Cost	表示のみ。MST ポート コスト。コスト値はインターフェイスのメディア スピードから取得します。有効値は 1 ~ 200000000 です。
Link Type	表示のみ。リンク タイプ。デフォルトは自動です。
Boundary Port	表示のみ。
PreStd Port	表示のみ。

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.5-32)
- 標準規格 (p.5-32)
- MIB (p.5-32)

関連資料

関連トピック	マニュアル名
Rapid PVST+	第4章「Rapid PVST+の設定」
STP 拡張機能	第6章「STP 拡張機能の設定」
NX-OS レイヤ2 スイッチングの設定	『Cisco NX-OS Layer 2 Switching Configuration Guide』
レイヤ2 インターフェイス	『Cisco DCNM Interfaces Configuration Guide』
DCNM の基本	『Cisco DCNM 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 DCNM Virtual Device Context Configuration Guide』
ライセンス	『Cisco DCNM Licensing Guide』
リリース ノート	『Cisco DCNM 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
<ul style="list-style-type: none"> • CISCO-STP-EXTENSION-MIB • BRIDGE-MIB 	<p>次の URL から、MIB の検索およびダウンロードができます。</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>



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。

Data Center Network Manager (DCNM) 機能の詳細については、『*Cisco DCNM Fundamentals 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。

- [STP 拡張機能の概要 \(p.6-2\)](#)
- [STP 拡張機能のライセンス要件 \(p.6-10\)](#)
- [STP 拡張機能の前提条件 \(p.6-10\)](#)
- [注意事項および制約事項 \(p.6-11\)](#)
- [STP 拡張機能の設定 \(p.6-12\)](#)
- [STP 拡張機能の設定フィールドの説明 \(p.6-16\)](#)
- [追加情報 \(p.6-18\)](#)



(注) STP および Per VLAN Rapid Spanning Tree (Rapid PVST+) の詳細は第 4 章「[Rapid PVST+ の設定](#)」を、Multiple Spanning Tree (MST) の詳細は第 5 章「[MST の設定](#)」を参照してください。

STP 拡張機能の概要



(注) DCNM を使用して STP パラメータを使用する前に、デバイスのコマンドラインに次の 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。

```
--logging-level spanning-tree 6
--logging logfile messages 6
--logging event link-status default
```

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。



(注) レイヤ 2 インターフェイスの作成に関する詳細については、『Cisco DCNM 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、スパンニング 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 PVT 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でも適用できます。



(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 \(p.6-3\)](#)
- [ブリッジ保証 \(p.6-3\)](#)
- [BPDU ガード \(p.6-6\)](#)
- [BPDU フィルタリング \(p.6-6\)](#)
- [ループ ガード \(p.6-7\)](#)
- [ルート ガード \(p.6-8\)](#)
- [STP 拡張機能の適用 \(p.6-8\)](#)
- [PVST シミュレーション \(p.6-9\)](#)
- [ハイ アベイラビリティ \(p.6-9\)](#)
- [バーチャライゼーションのサポート \(p.6-9\)](#)

STP ポート タイプ

スパンニング 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。デフォルトのスパンニング 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、誤ってスパンニング 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、およびスパンニング 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 リンクのスパンニング 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状態になり、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ンニングツリーの状態移行が再開されます。

図6-1に、一般的なSTPトポロジを示します。また、図6-2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6-1 標準的なSTPトポロジのネットワーク

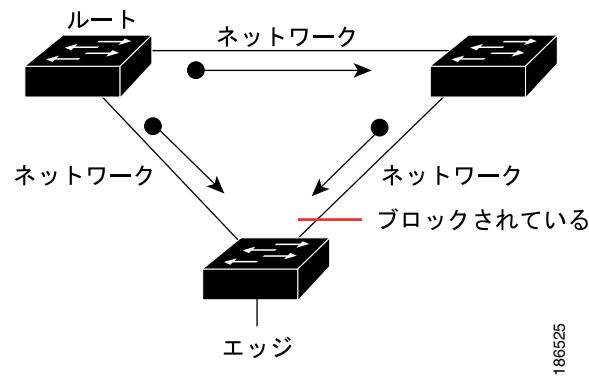


図6-2 ブリッジ保証を実行していないネットワークの問題

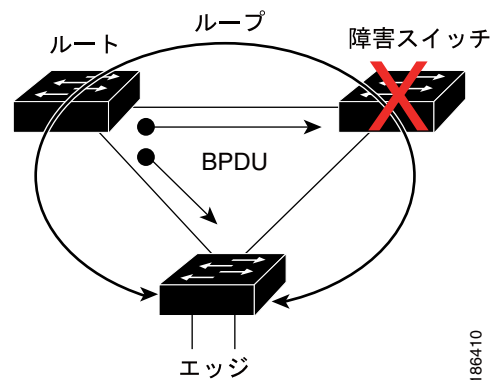


図 6-3 に、ブリッジ保証をイネーブルにしたネットワークで、すべての STP ネットワーク ポートから双方向 BPDU が発行される一般的な STP トポロジを示します。図 6-4 は、ネットワーク上でブリッジ保証をイネーブルにした場合、図 6-2 で示したネットワーク上の問題が発生しない理由を示しています。

図 6-3 ブリッジ保証を実行しているネットワークの STP トポロジ

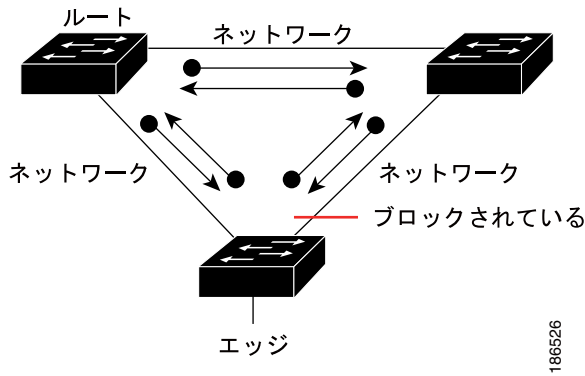
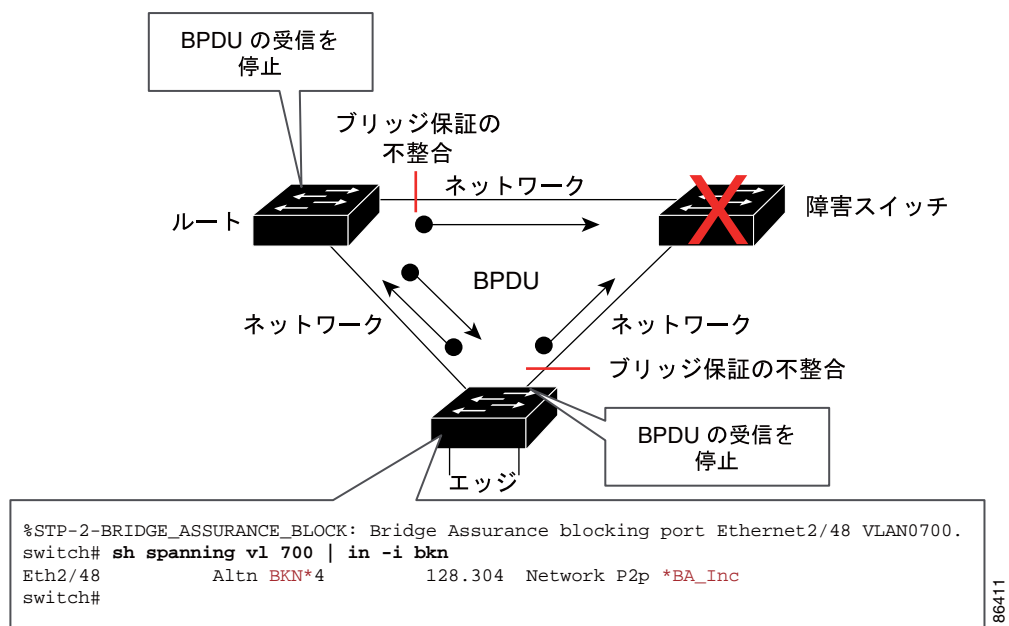


図 6-4 ブリッジ保証によるネットワーク上の問題の回避



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、稼働中のスパンニング 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ンニング 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ため、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ンニング 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ンニング 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。稼働中のスパンニング 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ンニング 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、スパンニング 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ッキング 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 6-1 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 6-1 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、このポートはスパンニング 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 4 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 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。

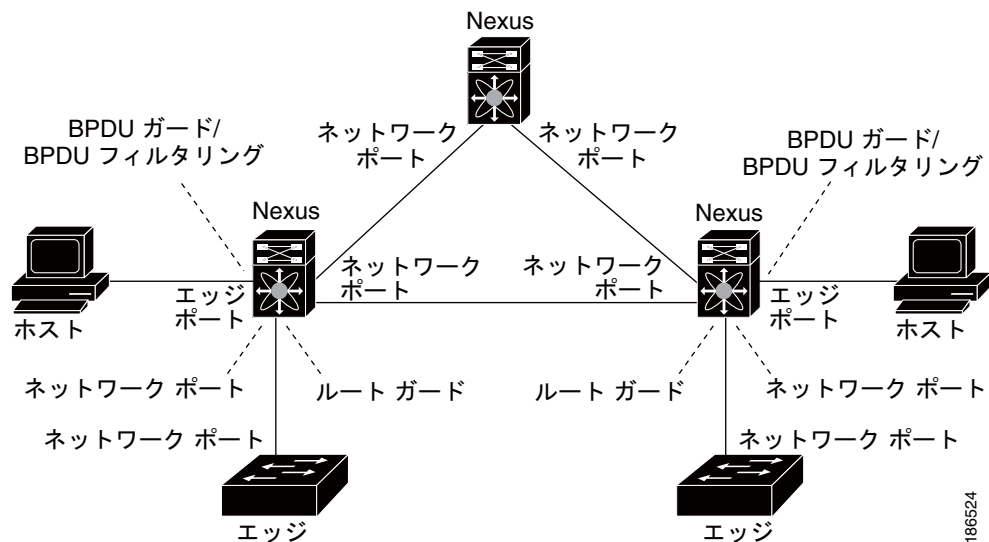
ルート ガードを使用して、ルート ブリッジをネットワークに強制的に配置できます。ルート ガードでは、ルート ガードをイネーブルにしたポートが指定ポートになります。通常、ルート ブリッジ上の複数のポートが接続されている場合を除き、ルート ブリッジのポートはすべて指定ポートです。ブリッジは、ルート ガードがイネーブルであるブリッジ ポート上で優位 BPDU を受信すると、そのポートをルート不整合 STP ステートに移行します。このように、ルート ガードによってルート ブリッジの配置を制御できます。

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 6-5 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。ホスト インターフェイスで BPDU ガードまたは BPDU フィルタリングをイネーブルにする必要があります。

図 6-5 STP 拡張機能を適正に設定したネットワーク



186524

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ものが、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、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 PVST+ 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 DCNM 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
DCNM	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 DCNM にバンドルされ、無料で提供されます。DCNM ライセンス機構の詳細については、『 <i>Cisco DCNM Licensing Guide</i> 』を参照してください。
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、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、『 <i>Cisco NX-OS Licensing Guide</i> 』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。

注意事項および制約事項

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 を送信するチャン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、チャンネル内の他のリンクが正常に動作していても、ループ ガードによりチャン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ンネルを形成すると、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、新しいチャン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。
- チャンネルがループ ガードによりブロックされ、チャン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。チャン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。
- 直接の管理制御下でないネットワーク 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。

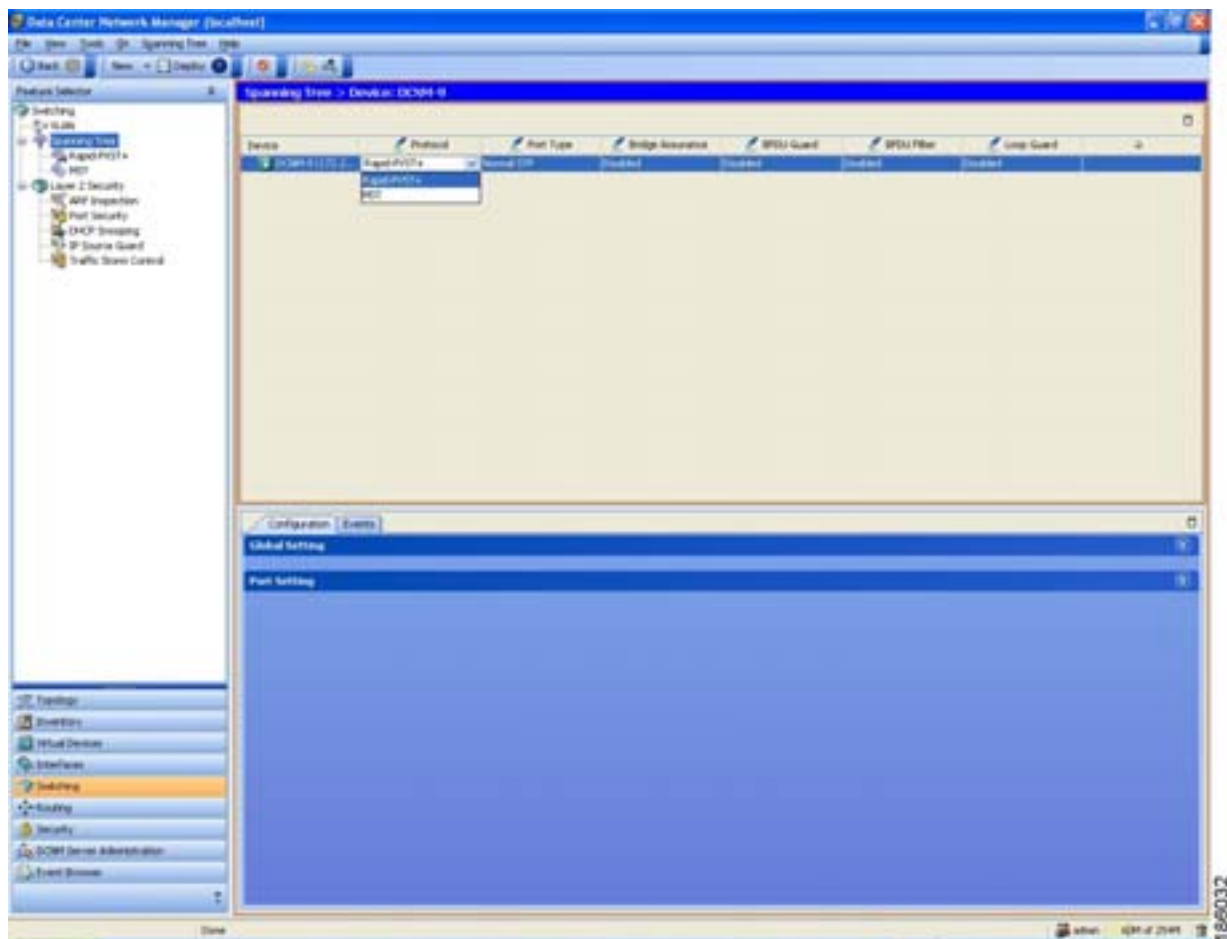
- STP 拡張機能のデフォルト値の設定 (p.6-12)
- STP 拡張機能のグローバル設定 (p.6-13)
- PVST シミュレーションのグローバル設定 (p.6-14)
- STP 拡張機能のインターフェイス単位での設定 (p.6-15)

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。

STP 拡張機能のデフォルト値の設定

STP 拡張機能をデフォルト設定に戻すには、Spanning Tree ペインを使用します (図 6-6 を参照)。

図 6-6 STP 拡張機能の設定



手順の詳細

STP 拡張機能をグローバルまたはポート単位でデフォルト設定にするには、次の手順を実行します。

-
- ステップ 1** Feature Selector ペインから、**Switching > Spanning Tree** を選択して Spanning Tree ペインを開きます。
 - ステップ 2** Summary ペインで、デバイス全体についてグローバルにデフォルト設定にするデバイスをクリックします。
 - ステップ 3** メニュー バーから **Spanning-Tree > Set to default** を選択します。
 - ステップ 4** Details ペインで、ポートをデフォルト設定にするために **Configuration** タブをクリックします。
 - ステップ 5** **Port Setting** セクションをクリックします。

Port Setting セクションが展開され、ポートが表示されます。
 - ステップ 6** Port Setting セクションで、設定するインターフェイスを選択します。
 - ステップ 7** メニュー バーで **Spanning-Tree > Set to default** を選択します。
 - ステップ 8** (任意) デバイスに変更を適用するには、メニュー バーから **File > Deploy** を選択します。
-

STP 拡張機能のグローバル設定

STP 拡張機能をグローバルに設定するには、Spanning Tree ペインを使用します (図 6-6 を参照)。

手順の詳細

STP 拡張機能をグローバルに設定するには、次の手順を実行します。

-
- ステップ 1** Feature Selector ペインから、**Switching > Spanning Tree** を選択して Spanning Tree ペインを開きます。
 - ステップ 2** Summary ペインでデバイスをクリックします。
 - ステップ 3** Details ペインで **Configuration** タブをクリックします。
 - ステップ 4** Details ペインで **Global Setting** セクションをクリックします。

Global Setting セクションが展開されます。
 - ステップ 5** Port Type ドロップダウン リストからポートタイプを選択します。

デフォルトのポートタイプは、Normal STP です。
 - ステップ 6** Bridge Assurance ドロップダウン リストから、**Enabled** または **Disabled** を選択します。

ブリッジ保証は、デフォルトでイネーブルです。

ステップ7 BPDU Guard ドロップダウン リストから、**Enabled** または **Disabled** を選択します。

デフォルトでは、BPDU ガードはディセーブルです。

ステップ8 BPDU Filter ドロップダウン リストから、**Enabled** または **Disabled** を選択します。

デフォルトでは、BPDU フィルタはディセーブルです。

ステップ9 Loop Guard ドロップダウン リストから、**Enabled** または **Disabled** を選択します。

デフォルトでは、ループ ガードはディセーブルです。

ステップ10 (任意) デバイスに変更を適用するには、メニュー バーから **File > Deploy** を選択します。

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。

PVST シミュレーションを設定するのは、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状態に移行します。このポートは、BPDU を受信しなくなるまでは不整合状態のままですが、そのあとは標準 STP の状態移行を再開します。

PVST シミュレーションを設定するには、Spanning Tree ペインを使用します (図 6-6 を参照)。

手順の詳細

PVST シミュレーションをグローバルに設定するには、次の手順を実行します。

ステップ1 Feature Selector ペインから、**Switching > Spanning Tree** を選択して Spanning Tree ペインを開きます。

ステップ2 Summary ペインで、MST 名とリビジョン番号を指定するデバイスをクリックします。

Summary ペインで選択したデバイスが強調表示され、Details ペインにタブが表示されます。

ステップ3 Details ペインで **Configuration** タブをクリックします。

ステップ4 **Global Setting** セクションをクリックします。

ステップ5 MST Setting エリアの Simulate PVST フィールドで、ドロップダウン リストをクリックし、**Enabled** をクリックします。

デフォルトはイネーブルです。

ステップ 6 (任意) デバイスに変更を適用するには、メニュー バーから **File > Deploy** を選択します。

STP 拡張機能のインターフェイス単位での設定

STP 拡張機能をインターフェイス単位で設定するには、Spanning Tree ペインを使用します ([図 6-6](#) を参照)。

手順の詳細

STP 拡張機能をインターフェイス単位で設定するには、次の手順を実行します。

ステップ 1 Feature Selector ペインから、**Switching > Spanning Tree** を選択して Spanning Tree ペインを開きます。

ステップ 2 Summary ペインでデバイスをクリックします。

ステップ 3 Details ペインで **Configuration** タブをクリックします。

ステップ 4 Details ペインで **Port Setting** セクションをクリックします。

Port Setting セクションが展開されます。

ステップ 5 Port Setting セクションで、設定するインターフェイスをクリックします。

ステップ 6 Port Type カラムで、ドロップダウン リストをクリックし、ポート タイプを選択します。

デフォルトでは、各インターフェイスのポート タイプは Default に設定されています。これにより、ポート タイプは、グローバルに設定されたポート タイプになります。

ステップ 7 BPDU Guard カラムで、ドロップダウン リストをクリックし、BPDU ガード設定を選択します。

デフォルトでは、各インターフェイスの BPDU ガード設定は Default に設定されています。これにより、インターフェイスは、グローバルに設定された BPDU ガード値になります。

ステップ 8 BPDU Filter カラムで、ドロップダウン リストをクリックし、BPDU フィルタ設定をクリックします。

デフォルトでは、各インターフェイスの BPDU フィルタ設定は Default に設定されています。これにより、インターフェイスは、グローバルに設定された BPDU フィルタ値になります。

ステップ 9 Guard カラムで、ドロップダウン リストをクリックし、ループ ガードまたはループ ガード設定を選択します。

デフォルトでは、各インターフェイスのガード設定は Default に設定されています。これにより、インターフェイスは、グローバルに設定されたループ ガード値になります。

ステップ 10 (任意) デバイスに変更を適用するには、メニュー バーから **File > Deploy** を選択します。

STP 拡張機能の設定フィールドの説明

ここでは、STP タイプの設定、さまざまな MST の設定、および STP 拡張機能の設定に使用するフィールドについて、次の内容を説明します。

- デバイス : 設定 : Global Settings セクション (p.6-16)
- デバイス : 設定 : Port Setting セクション (p.6-17)

デバイス : 設定 : Global Settings セクション

表 6-2 デバイス : 設定 : Global Settings セクション

フィールド	説明
STP 設定	
Device	表示のみ。デバイスの IP アドレスの名前。
Protocol	デバイスで使用されている STP プロトコル。値は PVRST または MST です。デフォルトは PVRST です。
Port Type	デバイスのグローバル STP ポート タイプ。値は Edge、Network、または Normal STP です。デフォルトのポート タイプは、Normal STP です。
Bridge Assurance	ブリッジ保証機能。値はイネーブルまたはディセーブルです。デフォルトは Enabled です。
BPDU Guard	ブリッジ保証機能。値はイネーブルまたはディセーブルです。デフォルトは Disabled です。
BPDU Filter	ブリッジ保証機能。値はイネーブルまたはディセーブルです。デフォルトは Disabled です。
Loop Guard	ループガード機能。値はイネーブルまたはディセーブルです。デフォルトは Disabled です。
Path Cost	パスコスト機能。値はショートまたはロングです。デフォルトはショートです。  (注) このフィールドは、Rapid PVST+ のみに適用されます。MST では、パスコスト方式は常にロングです。
MST 設定	
Name	MST 領域の名前。最大 34 文字までの英数字を入力できます。デフォルトは空白です。
Hello Time	MST プロトコルの hello タイム。指定できる範囲は 1 ~ 10 秒です。デフォルトは 2 秒です。
Revision Number	現在の MST コンフィギュレーションのリビジョン。指定できる範囲は 0 ~ 65535、デフォルト値は 0 です。
Simulate PVST	PVST シミュレーション。値はイネーブルまたはディセーブルです。デフォルトは Enabled です。
Digest	表示のみ。VLAN/MST 間マッピングの MD5 ダイジェスト。
Pre-Standard Digest	表示のみ。先行標準キーを使用した VLAN/MST 間マッピングの MD5 ダイジェスト。
Forward Delay Time	インターフェイスがフォワーディングを開始するまで、ラーニング ステートが継続する時間。指定できる範囲は 4 ~ 30 秒、デフォルト値は 15 秒です。
Max Age Time	ポートで受信したプロトコル情報がデバイスに保管される時間です。指定できる範囲は 6 ~ 40 秒、デフォルト値は 20 秒です。
Max Hop Count	BPDU が廃棄されるまで、領域内で許可されるホップの数。指定できる範囲は 1 ~ 255 ホップ、デフォルト値は 20 ホップです。

デバイス : 設定 : Port Setting セクション

表 6-3 デバイス : 設定 : Port Setting セクション

フィールド	説明
Name	表示のみ。インターフェイスの名前。
Priority	インターフェイスの STP ポート プライオリティ。指定できる範囲は 0 ~ 224 で、32 単位で設定します。デフォルト値は 128 です。
Cost	インターフェイスの STP ポート コスト。範囲は 1 ~ 200,000,000 です。デフォルト値は、インターフェイスのメディア速度から抽出されます。
Port Type	STP ポート タイプの有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Network 他のスイッチまたはブリッジに接続する場合のみ使用します。 • Edge access ホスト ポートに接続する場合のみ使用します。 • Edge trunk ホスト ポートへ接続する場合で、複数の VLAN にトラフィックを伝送するときのみ使用します。 • Disable ポートを STP 標準ポートに設定します。 • Default ポートをグローバル STP ポート タイプ設定に戻します。 デフォルトは Default です。
BPDU Guard	特定のインターフェイスの BPDU ガード機能。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Enable • Disable • Default ポートをグローバル BPDU ガード設定に戻します。 デフォルトは Default です。
BPDU Filter	特定のインターフェイスの BPDU フィルタ機能。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Enable • Disable • Default ポートをグローバル BPDU フィルタ設定に戻します。 デフォルトは Default です。
Guard	ループガードまたはルートガード。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Loop • None • Root デフォルトは Default です。
Simulate PVST	インターフェイス単位の PVST シミュレーション。有効な値は、次のとおりです。 <ul style="list-style-type: none"> • Enabled • Disabled • Default インターフェイスをデバイスのグローバル PVST シミュレーション設定に戻します。 デフォルトは Default です。

■ 追加情報

表 6-3 デバイス : 設定 : Port Setting セクション (続き)

フィールド	説明
Link Type	<p>インターフェイスのリンク タイプ。有効な値は、次のとおりです。</p> <ul style="list-style-type: none"> Point-to-point Shared Auto 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。 <p>デフォルトは Auto です。</p>

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 \(p.6-18 \)](#)
- [標準規格 \(p.6-18 \)](#)
- [MIB \(p.6-18 \)](#)

関連資料

関連トピック	マニュアル名
Rapid PVST+	第 4 章 「 Rapid PVST+ の設定 」
MST	第 5 章 「 MST の設定 」
NX-OS レイヤ 2 スイッチングの設定	『 <i>Cisco NX-OS Layer 2 Switching Configuration Guide</i> 』
レイヤ 2 インターフェイス	『 <i>Cisco DCNM Interfaces Configuration Guide</i> 』
DCNM fundamentals	『 <i>Cisco DCNM Security Configuration Guide</i> 』
ハイ アベイラビリティ	『 <i>Cisco NX-OS High Availability and Redundancy Guide</i> 』
システム管理	『 <i>Cisco NX-OS System Management Configuration Guide</i> 』
VDC	『 <i>Cisco DCNM Virtual Device Context Configuration Guide</i> 』
ライセンス	『 <i>Cisco DCNM Licensing Guide</i> 』
リリース ノート	『 <i>Cisco DCNM Release Notes, Release 4.0</i> 』

標準規格

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

MIB

MIB	MIB リンク
<ul style="list-style-type: none"> • CISCO_STP_EXTENSION MIB • BRIDGE MIB 	<p>次の URL から、MIB の検索およびダウンロードができます。</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>



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
すべての VLAN	VDC ごとに 4096 ボックスごとに 16,384 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 4096 個の Rapid PVST+ システムごとに 16,000 個の Rapid PVST+ 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 5-5
 - MST 5-5
 - MST 領域 5-5
 - Rapid PVST+ 4-6, 4-9
 - TC 時間タイマー 4-9
 - エッジポート 6-3
 - 交換の結果 4-6
 - 説明 4-6
 - バージョン 4-10, 5-8, 5-11
 - ブリッジ保証 6-4
 - ポートチャンネル 6-11
 - ホップカウント 5-8
 - 優位 6-8
- BPDU ガード
- インターフェイス単位の設定 6-15
 - グローバル設定 6-13
 - 説明 6-6
 - プライベート VLAN ポート 3-9
- BPDU フィルタリング
- インターフェイス単位の設定 6-15
 - エッジポート 6-7
 - グローバル 6-7
 - グローバル設定 6-13
 - 説明 6-6
 - ポート単位 6-7
- Bridge Protocol Data Unit、BPDU を参照
- C**
- CIST
- 説明 5-6
- CIST リージョナルルート 5-6
- Common and Internal Spanning Tree、CIST を参照
- Common Spanning Tree、CST を参照
- CST
- 説明 5-6
- H**
- hello タイム
- MST の設定 5-25
 - VLAN 単位の RPVST+ の設定 4-32
 - 説明 4-11
- I**
- IEEE 802.1D
- 用語 4-2
- IEEE 802.1s
- 用語 4-2
- IEEE 802.1w
- 用語 4-2
- Internal Spanning Tree、IST を参照
- IST
- BPDU 5-5
 - MST 5-4
 - 説明 5-6
- M**
- MAC アドレス リダクション
- MST 5-4
 - Rapid PVST+ 4-5
- MIB
- MST 5-32
 - Rapid PVST+ 4-38
 - STP 拡張機能 6-18
 - VLAN 3-20
 - プライベート VLAN 3-20
- MST
- 5-1
 - BPDU 5-5, 5-8
 - CIST リージョナルルート 5-7
 - hello タイム 5-25
 - IEEE 802.1D との相互運用性 5-11
 - IEEE 802.1w 5-4

- Rapid PVST+ との相互運用 6-9
 - VLAN/MST マッピング 5-4, 5-5, 5-18, 5-21
 - イネーブル化 5-15
 - インスタンス 5-4
 - インスタンスと VLAN のマッピング 5-18
 - インスタンスの削除 5-20
 - インスタンスの追加 5-18
 - 境界ポート 5-9
 - コンフィギュレーション情報 5-4
 - 最大エージングタイム 5-8, 5-25
 - 最大ホップカウント 5-8, 5-25
 - スイッチ プライオリティ 5-22
 - 制約事項 5-14
 - 説明 5-4 5-11
 - 先行標準 MSTP との相互運用性 5-11
 - 他の機能との相互運用性 5-14
 - 注意事項 5-14
 - デフォルト設定 6-16
 - デフォルト値の設定 5-17
 - 転送遅延時間 5-25
 - 統計情報 5-26
 - トラブルシューティング 5-1, 5-3
 - 名前 5-5
 - フィールドの説明 5-27
 - プリプロビジョニング 4-22, 5-15
 - プロトコル移行 5-11
 - ポートコスト 5-23
 - ポート プライオリティ 5-23
 - ポートごとのデフォルト値の設定 5-24
 - ライセンス 5-13
 - リビジョン番号 5-4, 5-5
 - リビジョン番号の設定 5-17
 - 領域名の設定 5-17
 - ルートブリッジ 6-9
 - ルートの設定 5-22
 - ログレベル 5-1, 5-3
 - MST インスタンス
 - 数 5-4
 - MST 領域
 - サポートされているスパンニング ツリー インスタンス 5-4
 - 説明 5-4
 - Multiple Spanning Tree Protocol、MST を参照
- P
- PortFast
 - エッジポート 6-3
 - PVLAN、プライベート VLAN を参照
 - PVST シミュレーション
 - グローバル設定 6-14
 - 説明 6-9
 - デフォルト 6-14
 - ルートブリッジ 6-9
- R
- Rapid per VLAN Spanning Tree +、Rapid PVST+ を参照
 - Rapid PVST+
 - BPDU 4-9
 - IEEE 802.1D との相互運用性 4-2, 4-9, 4-18
 - IEEE 802.1Q との相互運用性 4-2, 4-18
 - IEEE 802.1s との相互運用性 4-18
 - MST との相互運用 4-18, 6-9
 - VLAN 単位 4-2
 - VLAN 単位のイネーブル化 4-25
 - イネーブル化 4-23
 - インターフェイスごとのデフォルト値 4-30
 - 期限切れ 4-8
 - 高速コンバージェンス 4-9
 - 指定ポート 4-8
 - スイッチ プライオリティ 4-26
 - すべてのパラメータをデフォルトに設定 4-24
 - 制約事項 4-21
 - 説明 4-8 4-18
 - 他の機能との相互作用 4-21
 - 注意事項 4-21
 - デフォルト設定 6-16
 - 統計情報 4-35
 - トポロジ変更 4-9
 - トラブルシューティング 4-2, 5-1
 - フィールドの説明 4-35
 - プロトコル タイマー 4-11
 - ポートの移行 4-12
 - ライセンス 4-20
 - ルートスイッチ 4-8
 - ルートの設定 4-26
 - ログレベル 4-2, 5-1
 - RSTP
 - BPDU 4-16

- アクティブトポロジ 4-12
 - 高速コンバージェンス 4-8
- S**
- Spanning-Tree Protocol、STP を参照
- STP
- BPDU 4-4
 - MAC アドレス リダクション 4-5
 - MST 5-4
 - PortFast 4-8, 6-3
 - VLAN 単位 4-2
 - 異議メカニズム 4-16, 5-9
 - エッジポート 4-8, 6-3
 - 説明 4-3 4-7
 - デフォルト モード 4-2, 4-24, 5-15
 - トポロジ 4-4, 4-7, 6-7
 - トラブルシューティング 4-26, 6-2, 6-8
 - ネットワークポート 6-3
 - バーチャライゼーション 4-19, 5-12
 - パスコスト 4-6
 - 複数のインスタンス 4-19, 5-12
 - プライベート VLAN 3-9
 - ブリッジンググループ 4-3
 - プロトコル移行 4-18
 - ポートステート 4-13
 - ポートロール 4-12
 - 用語 4-2
 - ルートブリッジ 4-7
 - ルートポート 4-6
 - ロギングレベル 6-2
- STP 拡張機能
- インターフェイス単位の設定
 - ポートタイプ 6-15
 - 制約事項 6-11
 - 説明 6-3 6-9
 - 注意事項 6-11
 - デフォルト値の設定 6-12, 6-13
 - バーチャライゼーション 6-9
 - ベストプラクティス 6-8
 - ライセンス 6-10
- STP ポートタイプ
- 説明 6-3
- SVI
- VLAN インターフェイス 2-3
- U**
- UDLD
- MST 5-9
 - Rapid PVST+ 4-16
 - ループガード 6-11
- Unidirectional Link Detection、UDLD を参照
- V**
- VDC
- MST 5-12
 - STP 拡張機能 6-9
 - プライベート VLAN 3-8
- Virtual Device Context、VDC を参照
- VLAN
- Rapid PVST+ 4-2
 - SVI 2-3
 - 拡張システム ID 2-4
 - 削除 2-5, 2-8
 - 作成 2-8, 2-10
 - 制約事項 2-7
 - 説明 2-2 2-6
 - 注意事項 2-7
 - 統計情報 2-11
 - バーチャライゼーション 2-6
 - 変更 2-10
 - ポートの割り当て 2-5
 - 予約範囲 2-4
 - ライセンス 2-7
- VLAN インターフェイス
- VLAN 間の通信 2-3
 - イネーブル化 3-6
 - トラブルシューティング 3-7
 - プライベート VLAN 3-7, 3-17
- VLAN 統計情報
- 表示 2-11
- VLAN トラフィック
- 配信 2-2
 - ルーティング 2-3
- VLAN の作成
- デフォルトのステート 2-5
- VLAN の範囲
- 説明 2-4
- VLAN の変更
- 許可されるパラメータ 2-5

- VLAN 番号
 - 許可される番号 2-4
 - 予約範囲 2-4
- VLAN プライオリティ
 - Rapid PVST+ 4-17
- あ
- アクセスポート
 - 作成 2-5
- い
- インスタンス
 - MST 5-4
- インターフェイス単位の設定 6-15
- え
- エッジポート
 - PortFast 6-3
 - Rapid PVST+ 4-8
 - 説明 6-3
- か
- 拡張システム ID
 - VLAN 2-4
- 仮想 LAN
 - VLAN を参照
- 関連資料 xv
- き
- 境界ポート
 - STP 5-9
- こ
- コミュニティ VLAN
 - 説明 3-5
 - プライベート VLAN 3-5
- コミュニティポート
 - プライベート VLAN 3-4
- さ
- 最大エージング タイム
 - MST の設定 5-25
 - VLAN 単位の RPVST+ の設定 4-33
 - 説明 4-11
- 最大ホップ カウント
 - MST の設定 5-25
- し
- 指定ポート
 - BPDU 4-9
 - Rapid PVST+ 4-8
 - 説明 4-12
- 上限
 - 説明 (表) A-1
- 資料
 - 追加資料 xv
- せ
- 制約事項
 - MST 5-14
 - Rapid PVST+ 4-21
 - STP 拡張機能 6-11
 - プライベート VLAN 3-9
- セカンダリ VLAN 3-3
 - VLAN インターフェイスへのマッピング 3-16
 - コミュニティ 3-3
 - 独立 3-3
 - プライマリ VLAN との関連付け 3-4, 3-6, 3-15
- 設定の上限
 - 説明 (表) A-1
- た
- 代替ポート
 - 説明 4-12
- 代表スイッチ
 - 説明 4-12
- 代表ブリッジ
 - 説明 4-6
- タイマー
 - STP 4-11

- ち
- 注意事項
- MST 5-14
 - Rapid PVST+ 4-21
 - STP 拡張機能 6-11
 - プライベート VLAN 3-9
- て
- 提案合意ハンドシェイク
- BPDU 4-9
 - Rapid PVST+ 4-10
- デフォルト設定
- STP 4-2
- 転送遅延時間
- MST の設定 5-25
 - VLAN 単位の RPVST+ の設定 4-33
 - 説明 4-11
- と
- 統計情報
- Rapid PVST+ 4-35
- 独立 VLAN
- セカンダリ プライベート VLAN 3-3
 - 定義 3-4
 - プライマリ VLAN 3-4
- 独立ポート
- プライベート VLAN 3-4
- トランク ポート
- 作成 2-5
- ね
- ネットワーク ポート
- 説明 6-3
 - ブリッジ保証 6-4
- は
- バーチャライゼーション
- STP 4-19, 5-12
 - STP 拡張機能 6-9
 - VLAN 2-6
- プライベート VLAN 3-8
- パス コスト
- 説明 4-6
- パスコスト方式
- MST 5-10
 - Rapid PVST+ 4-17
 - 設定 4-29
- バックアップ ポート
- 説明 4-12
- ふ
- フィールドの説明
- MST 5-27
 - Rapid PVST+ 4-35
 - プライベート VLAN 3-19
- フォワーディング ポート ステート
- 説明 4-13
- プライベート VLAN 3-4
- STP 3-9
 - SVI 3-7
 - VLAN インターフェイス 3-2, 3-6, 3-7, 3-16
 - アソシエーション 3-15, 3-18
 - 変更 3-6
 - イネーブル化 3-2, 3-13
 - コミュニティ VLAN 3-3, 3-5, 3-14
 - 制約事項 3-9
 - セカンダリ VLAN 3-3
 - 設定 3-14
 - セカンダリ VLAN 入力トラフィックのルーティング 3-16
 - 設定時の注意事項 3-10
 - 説明 3-2 3-7
 - 他の機能との相互作用 3-9
 - 端末へのアクセス 3-7
 - 注意事項 3-9
 - 通信 3-2, 3-7
 - 統計情報 3-19
 - 独立 VLAN 3-3, 3-4, 3-14
 - トラフィックの配信 3-16
 - トラブルシューティング 3-2
 - バーチャライゼーション 3-8
 - フィールドの説明 3-19
 - 複数デバイスにまたがる 3-7
 - プライベート VLAN 外との通信 3-5
 - プライベート VLAN のアソシエーション 3-6

- プライマリ VLAN 3-3, 3-14
- ブロードキャスト ドメイン 3-2
- ブロードキャスト トラフィック 3-6
- ポート 3-18
 - コミュニティ 3-4
 - 設定時の注意事項 3-10
 - 独立 3-4
 - 無差別 3-4
- ホスト ポート 3-18
- マッピング 3-7, 3-16
- 無差別ポート 3-18
- ライセンス 3-8
- 利点 3-3
- ルーティング 3-2
- プライベート VLAN ポート
 - BPDU ガード 3-9
 - コミュニティ ポート 3-4
 - 制約事項 3-10
 - 独立ポート 3-4
 - トラフィックの配信 3-5
 - トランク ポート 3-4
 - ブロードキャスト トラフィック 3-6
 - 無差別ポート 3-4
- プライマリ VLAN
 - セカンダリ VLAN との関連付け 3-4, 3-6, 3-15
 - トラフィックの配信 3-5
 - プライベート VLAN 3-3, 3-4
 - 無差別ポート 3-5
- ブリッジ ID
 - 拡張システム ID 4-4
- ブリッジ保証
 - グローバル設定 6-13
 - サポートされるプロトコルとリンク タイプ 6-3
 - 説明 6-3 6-6
 - ネットワーク ポート 6-4
- ブリッジンググループ
 - STP 4-3
 - ループガード 6-7
- ブロードキャスト トラフィック
 - VLAN 2-2
 - プライベート VLAN 3-6
- ブロッキング ポート ステート
 - 説明 4-13
- ほ
- ポート
 - レイヤ 2 3-2, 3-4, 3-10, 4-9, 6-3
- ポート コスト
 - 値 4-17, 5-10
 - 設定 4-29, 5-23
- ポート ステート
 - STP 4-13
- ポート タイプ
 - グローバル設定 6-13
- ポート チャンネル
 - BPDU 6-11
 - STP 6-11
- ポート プライオリティ
 - Rapid PVST+ 4-17
 - Rapid PVST+ 用の設定 4-28
 - 設定 5-23
- ポート ロール
 - STP 4-12
- ホスト ポート 3-4
 - エッジポート 4-9, 6-3
 - プライベート VLAN 3-4, 3-6
- ま
- マッピング
 - プライベート VLAN 3-7
- マルチキャスト トラフィック
 - VLAN 2-2
- む
- 無差別ポート 3-4
 - コミュニティ VLAN 3-5
 - 独立 VLAN 3-5
 - プライマリ VLAN 3-5
 - プライマリ VLAN 内の数 3-5
- も
- モード
 - デフォルト設定 6-16

ら

ラーニング ポート ステート

説明 4-13

ライセンス

MST 5-13

Rapid PVST+ 4-20

STP 拡張機能 6-10

VLAN 2-7

プライベート VLAN 3-8

り

リンク タイプ

Rapid PVST+ 4-9

設定 4-34, 5-26

ポイントツーポイント 4-9

リンク障害

単一方向の検出 4-16, 5-9

る

ルート ガード

設定 6-15

説明 6-8

ルート ブリッジ

MST 6-9

PVST シミュレーション 6-9

選定 4-7

複数のバックアップ 5-22

ルート ガード 6-8

ルート ポート

BPDU 4-9

説明 4-6, 4-12

ループ ガード

インターフェイス単位の設定 6-15

グローバル設定 6-13

説明 6-7

リンク タイプ 6-7