Cisco Nexus 7000 シリーズ NX-OS レイヤ 2 スイッチング コンフィギュレーション ガイド

初版：2011 年 09 月 27 日

最終更新：2012 年 06 月 06 日

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

Text Part Number: OL-25755-01-J

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

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。 シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、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、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

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。

© 2011-12 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xi

対象読者 xi

マニュアルの構成 xi

表記法 xii

関連資料 xiv

マニュアルの入手方法およびテクニカル サポート xv

新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

概要 5

レイヤ 2 イーサネット スイッチングの概要 5

VLANs 6

Private VLANs 6

Spanning Tree 6

STP Overview 6

Rapid PVST+ 7

MST 7

STP Extensions 7

Virtualization 8

関連資料 9

レイヤ 2 スイッチングの設定 11

レイヤ 2 スイッチングについて 11

レイヤ 2 イーサネット スイッチングの概要 12

セグメント間のフレーム スイッチング 12

アドレス テーブルの構築およびアドレス テーブルの変更 12

スーパーバイザおよびモジュール上で一貫した MAC アドレス テーブル 13

レイヤ 3 スタティック MAC アドレス 13

スイッチングのハイ アベイラビリティ 14
レイヤ 2 スイッチングのバーチャライゼーションのサポート 14
レイヤ 2 スイッチングのライセンス要件 14
MAC アドレス設定の前提条件 14
MAC アドレスの設定に関する注意事項および制約事項 15
レイヤ 2 スイッチングのデフォルト設定 15
レイヤ 2 スイッチングの設定手順 16
スタティック MAC アドレスの設定 16
レイヤ 3 インターフェイス上のスタティック MAC アドレスの設定 17
MAC テーブルのエージング タイムの設定 19
VLAN の学習モードの設定 20
MAC アドレス テーブルの整合性検査 21
MAC テーブルからのダイナミック アドレスのクリア 22
レイヤ 2 スイッチング設定の確認 23
レイヤ 2 スイッチングの設定例 23
レイヤ 2 スイッチングの追加情報（CLI バージョン） 24
レイヤ 2 スイッチングの設定の機能履歴（CLI バージョン） 25
VLAN の設定 27
Information About VLANs 27
VLANs Overview 28
VLAN Ranges 29
Creating, Deleting, and Modifying VLANs 31
High Availability for VLANs 31
Virtualization Support for VLANs 32
Licensing Requirements for VLANs 32
Prerequisites for Configuring VLANs 33
Guidelines and Limitations for Configuring VLANs 33
VLAN のデフォルト設定 33
Configuring a VLAN 34
VLAN の作成と削除（CLI バージョン） 34
VLAN コンフィギュレーション サブモードの開始 36
VLAN の設定 37
予約された VLAN の範囲の変更 40

VLAN 作成前の VLAN 設定 41
VLAN ロング ネームのイネーブル化 42
VLAN の設定の確認 43
VLAN 統計情報の表示とクリア 44
VLAN の設定例 44
VLAN の追加情報（CLI バージョン） 44
VLAN 設定の機能履歴（CLI バージョン） 46
VTP の設定 47
VTP の概要 47
VTP 47
VTP の概要 48
VTP モード 48
インターフェイス単位の VTP 49
VTP プルーニング 49
VTP プルーニングとスパニングツリー プロトコル 50
デフォルト設定 50
VTP の設定 51
VTP プルーニングの設定 53
NX-OS を使用したプライベート VLAN の設定 57
Information About Private VLANs 57
プライベート VLAN の概要 58
Primary and Secondary VLANs in Private VLANs 58
Private VLAN Ports 59
Primary, Isolated, and Community Private VLANs 60
プライマリ VLAN とセカンダリ VLAN のアソシエーション 62
Broadcast Traffic in Private VLANs 63
Private VLAN Port Isolation 63
Private VLANs and VLAN Interfaces 63
Private VLANs Across Multiple Devices 64
High Availability for Private VLANs 64
Virtualization Support for Private VLANs 64
Licensing Requirements for Private VLANs 64
Prerequisites for Private VLANs 65
Guidelines and Limitations for Configuring Private VLANs 65

Secondary and Primary VLAN Configuration 65
Private VLAN Port Configuration 67
Limitations with Other Features 67
プライベート VLAN のデフォルト設定 68
Configuring a Private VLAN 69
プライベート VLAN のイネーブル化（CLI バージョン） 69
プライベート VLAN としての VLAN の設定（CLI バージョン） 70
セカンダリ VLAN とプライマリ プライベート VLAN の関連付け（CLI バージョン） 72
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（CLI バージョン） 75
プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定 77
プライベート VLAN 独立トランク ポートとしてのレイヤ 2 インターフェイスの設定 79
プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定 83
プライベート VLAN 無差別トランク ポートとしてのレイヤ 2 インターフェイスの設定 85
プライベート VLAN 設定の確認 89
プライベート VLAN の統計情報の表示とクリア 90
プライベート VLAN の設定例 90
プライベート VLAN の追加情報（CLI バージョン） 91
プライベート VLAN 設定の機能履歴（CLI バージョン） 92
Cisco NX-OS を使用した Rapid PVST+ の設定 93
Information About Rapid PVST+ 93
STP 94
Overview of STP 94
How a Topology is Created 95
ブリッジ ID 95
Bridge Priority Value 95
Extended System ID 96
STP MAC Address Allocation 96
BPDUs 97
Election of the Root Bridge 98
Creating the Spanning Tree Topology 98

Rapid PVST+ 99
Overview of Rapid PVST+ 99
Rapid PVST+ BPDUs 100
Proposal and Agreement Handshake 101
Protocol Timers 102
Port Roles 103
Rapid PVST+ Port State Overview 104
ブロッキング ステート 105
Learning State 105
Forwarding State 105
Disabled State 106
Summary of Port States 106
Synchronization of Port Roles 106
Processing Superior BPDU Information 107
Processing Inferior BPDU Information 108
Detecting Unidirectional Link Failure:Rapid PVST+ 108
Port Cost 108
Port Priority 109
Rapid PVST+ and IEEE 802.1Q Trunks 109
Rapid PVST+ Interoperation with Legacy 802.1D STP 110
Rapid PVST+ Interoperation with 802.1s MST 110
High Availability for Rapid PVST+ 110
Virtualization Support for Rapid PVST+ 111
Licensing Requirements for Rapid PVST+ 111
Prerequisites for Configuring Rapid PVST+ 112
Guidelines and Limitations for Configuring Rapid PVST+ 112
Rapid PVST+ のデフォルト設定 113
Rapid PVST+ の設定 115
Rapid PVST+ の設定に関する注意事項 115
Rapid PVST+ のイネーブル化（CLI バージョン） 115
Rapid PVST+ の VLAN 単位でのディセーブル化またはイネーブル化（CLI バージョン） 117
ルート ブリッジ ID の設定 119
セカンダリ ルート ブリッジの設定（CLI バージョン） 121

VLAN の Rapid PVST+ のブリッジ プライオリティの設定 123
Rapid PVST+ ポート プライオリティの設定（CLI バージョン） 124
Rapid PVST+ パスコスト方式およびポート コストの設定（CLI バージョン） 126
VLAN の Rapid PVST+ hello タイムの設定（CLI バージョン） 128
VLAN の Rapid PVST+ 転送遅延時間の設定（CLI バージョン） 129
VLAN の Rapid PVST+ 最大エージング タイムの設定（CLI バージョン） 131
Rapid PVST+ のリンク タイプの指定（CLI バージョン） 132
Rapid PVST+ 用のプロトコルの再初期化 134
Rapid PVST+ の設定の確認 134
Rapid PVST+ 統計情報の表示およびクリア（CLI バージョン） 135
Rapid PVST+ の設定例 135
Rapid PVST+ の追加情報（CLI バージョン） 136
Rapid PVST+ の設定の機能履歴（CLI バージョン） 137
Cisco NX-OS を使用した MST の設定 139
Information About MST 139
MST Overview 140
MST Regions 140
MST BPDUs 141
MST Configuration Information 141
IST, CIST, and CST 142
IST, CIST, and CST Overview 142
Spanning Tree Operation Within an MST Region 143
Spanning Tree Operations Between MST Regions 143
MST Terminology 144
Hop Count 145
境界ポート 145
Detecting Unidirectional Link Failure:MST 146
Port Cost and Port Priority 147
Interoperability with IEEE 802.1D 147
High Availability for MST 148
Virtualization Support for MST 148
Licensing Requirements for MST 149
Prerequisites for MST 149
Guidelines and Limitations for Configuring MST 149

MST のデフォルト設定 151
Configuring MST 152
MST のイネーブル化（CLI バージョン） 152
MST コンフィギュレーション モードの開始 154
MST の名前の指定 156
MST 設定のリビジョン番号の指定 157
MST 領域での設定の指定 159
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（CLI バージョン） 162
プライベート VLAN でセカンダリ VLAN をプライマリ VLAN として同じ MSTI にマッピングするには 164
ルート ブリッジの設定 166
MST セカンダリ ルート ブリッジの設定 168
MST スイッチ プライオリティの設定 170
MST ポート プライオリティの設定 172
MST ポート コストの設定 173
MST hello タイムの設定 175
MST 転送遅延時間の設定 177
MST 最大エージング タイムの設定 178
MST 最大ホップ カウントの設定 179
先行標準MSTPメッセージを事前に送信するインターフェイスの設定（CLIバージョン） 180
MST のリンク タイプの指定（CLI バージョン） 182
MST 用のプロトコルの再初期化 184
MST 設定の確認 184
MST 統計情報の表示およびクリア（CLI バージョン） 185
MST の設定例 185
MST の追加情報（CLI バージョン） 187
MST 設定の機能履歴（CLI バージョン） 188
Cisco NX-OS を使用した STP 拡張の設定 189
Information About STP Extensions 189
STP Port Types 190
STP Edge Ports 190

Bridge Assurance 190
BPDU ガード 192
BPDU フィルタリング 193
Loop Guard 194
Root Guard 195
STP 拡張機能の適用 195
PVST Simulation 195
High Availability for STP 196
Virtualization Support for STP Extensions 196
Licensing Requirements for STP Extensions 196
Prerequisites for STP Extensions 197
Guidelines and Limitations for Configuring STP Extensions 197
STP 拡張機能のデフォルト設定 198
Configuring STP Extensions Steps 199
スパニングツリー ポート タイプのグローバルな設定 199
指定インターフェイスでのスパニングツリー エッジ ポートの設定 201
指定インターフェイスでのスパニングツリー ネットワーク ポートの設定 203
BPDU ガードのグローバルなイネーブル化 205
指定インターフェイスでの BPDU ガードのイネーブル化 207
BPDU フィルタリングのグローバルなイネーブル化 209
指定インターフェイスでの BPDU フィルタリングのイネーブル化 210
ループ ガードのグローバルなイネーブル化 213
指定インターフェイスでのループ ガードまたはルート ガードのイネーブル化 215
PVST シミュレーションのグローバル設定（CLI バージョン） 217
ポートごとの PVST シミュレーションの設定 219
STP 拡張機能の設定の確認 221
STP 拡張機能の設定例 221
STP 拡張機能の追加情報（CLI バージョン） 221
STP 拡張機能の設定の機能履歴（CLI バージョン） 222
レイヤ 2 スイッチングの設定の制限 225
レイヤ 2 スイッチングの設定の制限 225

はじめに

ここでは、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』の対象読者、構成、および表記法について説明します。 また、関連マニュアルの入手方法についても説明します。

この章は、次の内容で構成されています。

- 対象読者，xi ページ
- マニュアルの構成，xi ページ
- 表記法，xii ページ
- 関連資料，xiv ページ
- マニュアルの入手方法およびテクニカル サポート，xv ページ

対象読者

このマニュアルは、Cisco NX-OS デバイスの設定と保守を担当する、経験のあるユーザを対象としています。

マニュアルの構成

このマニュアルは、次の章で構成されています。

章	説明
新機能および変更された機能に関する情報	新機能と変更された機能に対するリリース固有の情報について説明します。
概要	各機能を要約して説明します。
レイヤ 2 スイッチングの設定	従来のイーサネット レイヤ2スイッチングについて説明します。

章	説明
VLAN の設定	VLAN 設定の詳細について説明します。
NX-OS を使用したプライベート 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。
NX-OS を使用した Rapid PVST+ の設定	IEEE 802.1D STP に関する情報、および Rapid PVST+ 設定の詳細について説明します。
Cisco NX-OS を使用した MST の設定	MST 設定の詳細情報について説明します。
NX-OS を使用した STP 拡張の設定	シスコ独自の STP 拡張機能である Bridge Assurance、BPDU 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。
Cisco NX-OS レイヤ 2 スイッチング機能の設定の上限	レイヤ 2 スイッチング機能の制限について説明します。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	角カッコで囲まれているものは、省略可能な要素（キーワードまたは引数）です。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。 角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。

表記法	説明
variable	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。 stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてstringとみなされます。

例では、次の表記法を使用しています。

表記法	説明
screen フォント	スイッチが表示する端末セッションおよび情報は、screenフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、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に記載されていない参照資料を紹介しています。

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

関連資料

Cisco NX-OS のマニュアルは、次の URL から入手できます。

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

Cisco NX-OS ソフトウェアの関連マニュアルは、次のとおりです。

リリース ノート

『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.x*』

NX-OS コンフィギュレーション ガイド

『*Cisco Nexus 7000 Series NX-OS Configuration Examples, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide, Release 6.x*』

『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x*』

『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』

『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』

『*Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide*』

『*Cisco Nexus 7000 Series NX-OS OTV Configuration Guide*』

『*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 6.x*』

『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x*』

『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x*』

『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x*』

『*Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*』

『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』

『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Quick Start*』

『*Cisco Nexus 7000 Series OTV Quick Start Guide*』

『*Configuring Feature Set for FabricPath*』

『*Configuring the Cisco Nexus 2000 Series Fabric Extender*』

NX-OS コマンド リファレンス

『*Cisco Nexus 7000 Series NX-OS Command Reference Master Index*』

『*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*』

『*Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference*』

『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Command Reference*』

『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』

『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』

『*Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference*』

『*Cisco Nexus 7000 Series NX-OS OTV Command Reference*』

『*Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*』

『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』

『*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference*』

『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference*』

その他のソフトウェアのマニュアル

『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』

『Cisco Nexus 7000 Series NX-OS MIB Quick Reference』

『*Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 6.x*』

『Cisco Nexus 7000 Series NX-OS Troubleshooting Guide』

『*Cisco NX-OS Licensing Guide*』

『Cisco NX-OS System Messages Reference』

『*Cisco NX-OS XML Interfaces User Guide*』

マニュアルの入手方法およびテクニカル サポート

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

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

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

新機能および変更された機能に関する情報

- 新機能および変更された機能に関する情報，1 ページ

新機能および変更された機能に関する情報

ここでは、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』に記載されている新機能および変更された機能について、リリース固有の情報を示します。

この Cisco NX-OS リリースに関する追加情報を確認するには、『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.x*』を参照してください。

次の表に、このマニュアルに記載されている新機能と変更された機能の概要を示します。

表 *1*：『*Cisco Nexus 7000* シリーズ *NX-OS* レイヤ *2* スイッチング コンフィギュレーション ガイド』における新機能と変更された機能

機能	説明	変更されたリリース
VLAN の学習モード	VLAN の学習モードを設定できます。	6.0(1)
ダイナミック システムに予約されている VLAN 範囲	システムによって予約されている VLAN の範囲を変更できます。	5.2(1)

新機能および変更された機能に関する情報

機能	説明	変更されたリリース
VLAN トランキング プロトコル	サーバモード、クライアント モード、トランスペアレントモード、およびオフモードで VTP バージョン 1 および 2 を実行できます。 VTP プルーニングもサポートされます。	5.1(1)
プライベート VLAN の独立トランク ポートおよび無差別トランク ポート	プライベート VLAN の独立トランク ポートおよび無差別トランク ポートを設定できます。	5.0(2)
レイヤ 3 インターフェイスのスタティック MAC アドレス	レイヤ 3 インターフェイスのスタティック MAC アドレスを設定できます。	4.2(1)
vPC がイネーブルな場合に拡張される MAC テーブルの表示	**show mac address-table** コマンドを実行すると、vPC 機能をイネーブルにして設定した追加情報を表示します。	4.1(3)
イネーブルになっている機能の表示	デバイス上でイネーブルになっている機能を表示できます。	4.1(2)
VLAN トランキング プロトコル	トランスペアレント モードで VTP を実行できます。	4.1(2)

新機能および変更された機能に関する情報

機能	説明	変更されたリリース
レイヤ 2 の整合性	**show forwarding consistency l2** コマンドを実行すると、MAC アドレス テーブルでモジュール間に不整合があるエントリが表示されます。	4.1(2)

新機能および変更された機能に関する情報

第 2 章

概要

この章では、レイヤ 2 機能をサポートする Cisco NX-OS デバイスの概要について説明します。

この章は、次の内容で構成されています。

- レイヤ 2 イーサネット スイッチングの概要，5 ページ
- VLANs，6 ページ
- Private VLANs，6 ページ
- Spanning Tree，6 ページ
- Virtualization，8 ページ
- 関連資料，9 ページ

レイヤ 2 イーサネット スイッチングの概要

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

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

衝突はイーサネット ネットワークに重大な輻輳を引き起こしますが、有効な解決策の 1 つは全二重通信です。 一般的に、10/100 Mbps イーサネットは半二重モードで動作するので、各ステーションは送信または受信のどちらかしか実行できません。 これらのインターフェイスを全二重モードに設定すると、2 つのステーション間で同時に送受信を実行できます。 パケットを双方向に同時に送ることができるので、有効なイーサネット帯域幅は 2 倍になります。 1/10 ギガビット イーサネットは、全二重モードだけで動作します。

VLANs

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment.

Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in that VLAN. Each VLAN is considered as a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a bridge or a router.

All ports, including the management port, are assigned to the default VLAN (VLAN1) when the device first comes up. A VLAN interface, or switched virtual interface (SVI), is a Layer 3 interface that is created to provide communication between VLANs.

The devices support 4094 VLANs in accordance with the IEEE 802.1Q standard. These VLANs are organized into several ranges, and you use each range slightly differently. Some of these VLANs are reserved for internal use by the device and are not available for configuration.

（注） Inter-Switch Link (ISL) trunking is not supported on the Cisco NX-OS.

Private VLANs

Private VLANs provide traffic separation and security at the Layer 2 level.

A private VLAN is one or more pairs of a primary VLAN and a secondary VLAN, all with the same primary VLAN. The two types of secondary VLANs are isolated and community VLANs. Hosts on isolated VLANs communicate only with hosts in the primary VLAN. Hosts in a community VLAN can communicate only among themselves and with hosts in the primary VLAN but not with hosts in isolated VLANs or in other community VLANs.

Regardless of the combination of isolated and community secondary VLANs, all interfaces within the primary VLAN comprise one Layer 2 domain, and therefore, require only one IP subnet.

Spanning Tree

This section discusses the implementation of the Spanning Tree Protocol (STP) on the software. Spanning tree is used to refer to IEEE 802.1w and IEEE 802.1s. When the IEEE 802.1D Spanning Tree Protocol is referred to in the publication, 802.1D is stated specifically.

STP Overview

STP provides a loop-free network at the Layer 2 level. Layer 2 LAN ports send and receive STP frames, which are called Bridge Protocol Data Units (BPDUs), at regular intervals. Network devices do not forward these frames but use the frames to construct a loop-free path.

802.1D is the original standard for STP, and many improvements have enhanced the basic loop-free STP. You can create a separate loop-free path for each VLAN, which is named Per VLAN Spanning Tree (PVST+).

Additionally, the entire standard was reworked to make the loop-free convergence process faster to keep up with the faster equipment. This STP standard with faster convergence is the 802.1w standard, which is known as Rapid Spanning Tree (RSTP). Now, these faster convergence times are available as you create STP for each VLAN, which is known as Per VLAN Rapid Spanning Tree (Rapid PVST+).

Finally, the 802.1s standard, Multiple Spanning Trees (MST), allows you to map multiple VLANs into a single spanning tree instance. Each instance runs an independent spanning tree topology.

Although the software can interoperate with legacy 802.1D systems, the system runs Rapid PVST+ and MST. You can use either Rapid PVST+ or MST in a given VDC; you cannot mix both in one VDC. Rapid PVST+ is the default STP protocol for Cisco NX-OS devices.

（注） Cisco NX-OS uses the extended system ID and MAC address reduction; you cannot disable these features.

In addition, Cisco has created some proprietary features to enhance the spanning tree activities.

Rapid PVST+

Rapid PVST+ is the default spanning tree mode for the software and is enabled by default on the default VLAN and all newly created VLANs.

A single instance, or topology, of RSTP runs on each configured VLAN, and each Rapid PVST+ instance on a VLAN has a single root device. You can enable and disable STP on a per-VLAN basis when you are running Rapid PVST+.

MST

The software also supports MST. The multiple independent spanning tree topologies enabled by MST provide multiple forwarding paths for data traffic, enable load balancing, and reduce the number of STP instances required to support a large number of VLANs.

MST incorporates RSTP, so it also allows rapid convergence. MST improves the fault tolerance of the network because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).

（注） Changing the spanning tree mode disrupts the traffic because all spanning tree instances are stopped for the previous mode and started for the new mode.

You can force specified interfaces to send prestandard, rather than standard, MST messages using the command-line interface.

STP Extensions

The software supports the following Cisco proprietary features:

- Spanning tree port types—The default spanning tree port type is normal. You can configure interfaces connected to Layer 2 hosts as edge ports and interfaces connected to Layer 2 switches or bridges as network ports.

- Bridge Assurance—Once you configure a port as a network port, Bridge Assurance sends BPDUs on all ports and moves a port into the blocking state if it no longer receives BPDUs. This enhancement is available only when you are running Rapid PVST+ or MST.
- BPDU Guard—BPDU Guard shuts down the port if that port receives a BPDU.
- BPDU Filter—BPDU Filter suppresses sending and receiving BPDUs on the port.
- Loop Guard—Loop Guard prevents the nondesignated ports from transitioning to the STP forwarding state, which prevents loops in the network.
- Root Guard—Root Guard prevents the port from becoming the root in an STP topology.

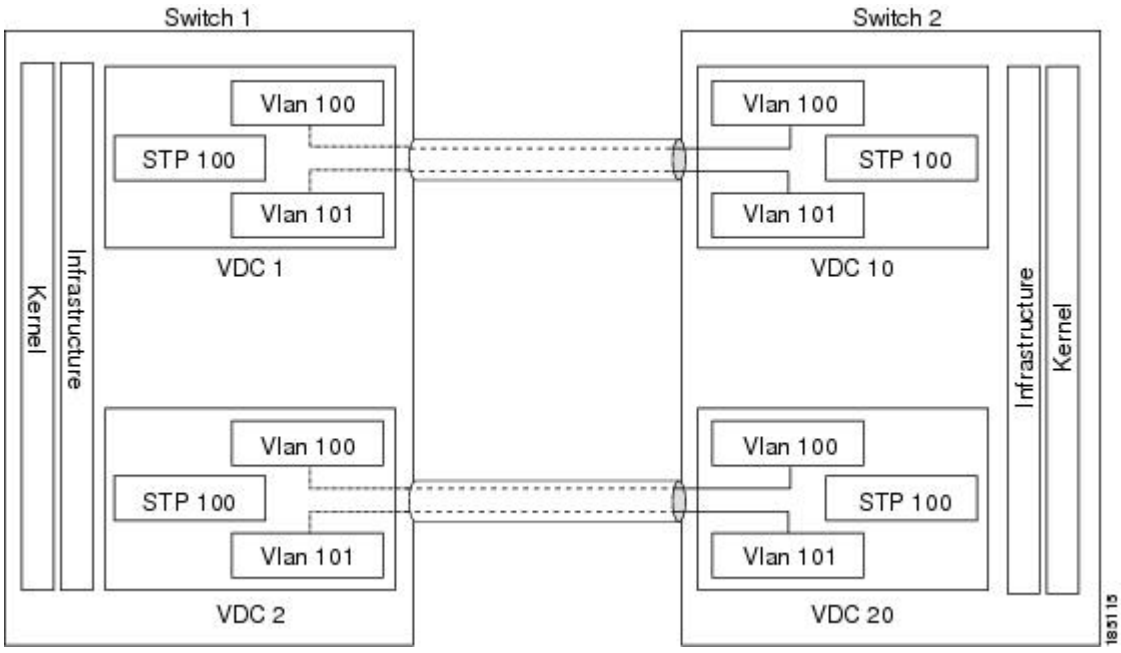
Virtualization

Cisco NX-OS devices introduce support for multiple virtual device contexts (VDCs) on a single switching device. Each VDC is treated as a standalone device with specific resources, such as physical interfaces, allocated to each VDC by the network admin role. An administrator is assigned to each VDC and that administrator has a limited view of the system, within that specific VDC. Faults are also isolated to within the specific VDC.

This VDC concept applies to all features on Cisco NX-OS, including all Layer 2 switching features.

All processes work independently in each VDC. You can reuse the process identification numbers in different VDCs. This figure shows how to reuse the VLAN 100 identifier in each separate VDC.

図 *1* : ***VDCs with Layer 2 Services***



Each VDC acts as a standalone device with Layer 2 services available. VDCs allow you to share a physical device among several logical functions. You can provision and assign entirely separate Layer 2 resources to individual VDCs.

You can configure several VDCs, and each VDC is a group of physical device resources. You assign resources and user roles for each VDC. VDCs allows flexible resources as well as enhanced fault isolation.

VDCs allow the separation of processes and management environments, providing well-defined fault and administrative boundaries between logical devices. Each VDC can be considered as a separate device with its own configuration, resources, users, and management interface.

VDCs define different administrator levels, or roles, that can access and administer each VDC. Commands outside the scope of a given user role are either hidden from that user's view or can return an error if the command is entered. This feature limits the number of users who can access the entire physical device and introduce traffic-disrupting misconfigurations.

（注） See the 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』, for complete information on virtual device contexts (VDCs) and assigning resources.

See the 『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』, for information on restartability and seamless transitions.

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 Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』
-
- 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』
- 『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x*』
- 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
- 『*Cisco NX-OS Licensing Guide*』
- 『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』
- 『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x*』

第 3 章

レイヤ 2 スイッチングの設定

この章では、Cisco NX-OS を使用してレイヤ 2 スイッチングを設定する方法について説明します。

この章は、次の内容で構成されています。

- レイヤ 2 スイッチングについて，11 ページ
- レイヤ 2 スイッチングのライセンス要件，14 ページ
- MAC アドレス設定の前提条件，14 ページ
- MAC アドレスの設定に関する注意事項および制約事項，15 ページ
- レイヤ 2 スイッチングのデフォルト設定，15 ページ
- レイヤ 2 スイッチングの設定手順，16 ページ
- レイヤ 2 スイッチング設定の確認，23 ページ
- レイヤ 2 スイッチングの設定例，23 ページ
- レイヤ 2 スイッチングの追加情報（CLI バージョン），24 ページ
- レイヤ 2 スイッチングの設定の機能履歴（CLI バージョン），25 ページ

レイヤ 2 スイッチングについて

（注） インターフェイスの作成の詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』を参照してください。

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

（注） ハイ アベイラビリティ機能の詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

レイヤ 2 イーサネット スイッチングの概要

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

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

衝突はイーサネット ネットワークに重大な輻輳を引き起こしますが、有効な解決策の 1 つは全二重通信です。 一般的に、10/100 Mbps イーサネットは半二重モードで動作するので、各ステーションは送信または受信のどちらかしか実行できません。 これらのインターフェイスを全二重モードに設定すると、2 つのステーション間で同時に送受信を実行できます。 パケットを双方向に同時に送ることができるので、有効なイーサネット帯域幅は 2 倍になります。 1/10 ギガビット イーサネットは、全二重モードだけで動作します。

セグメント間のフレーム スイッチング

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

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

デバイスは、LAN ポート間で効率的にフレームをスイッチングするために、アドレス テーブルを管理しています。 デバイスは、フレームを受信すると、受信した LAN ポートに、送信側ネットワーク デバイスの Media Access Control（MAC; メディア アクセス コントロール）アドレスを関連付けます。

アドレス テーブルの構築およびアドレス テーブルの変更

デバイスは、受信したフレームの送信元 MAC アドレスを使用して、アドレス テーブルをダイナミックに構築します。 自分のアドレス テーブルに登録されていない宛先 MAC アドレスを持つフレームを受信すると、デバイスは、そのフレームを同じ VLAN のすべての LAN ポート（受信したポートは除く）に送出します。 宛先端末が応答を返してきたら、デバイスは、その応答パケットの送信元 MAC アドレスとポート ID をアドレス テーブルに追加します。 以降、その宛先へのフレームを、すべての LAN ポートに送出せず、単一の LAN ポートだけに転送します。

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

Cisco NX-OS Release 4.1(5) 以降では、Virtual Port Channels（vPC; 仮想ポート チャネル）ピア リンクで接続された両方のデバイスに同じスタティック MAC アドレスを手動で設定する必要があります。 MAC アドレス テーブルの表示が拡張されて、vPC を使用している MAC アドレスに関する情報が表示されるようになりました。

vPC に関する情報については、『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』を参照してください。

アドレス テーブルは、ハードウェアの I/O モジュールに応じて多数の MAC アドレス エントリを格納できます。 デバイスは、設定可能なエージング タイマーによって定義されるエージング メカニズムを使用しているため、アドレスが非アクティブな状態のまま指定時間（秒）が経過すると、そのアドレスはアドレス テーブルから削除されます。

MAC ポートのセキュリティについては、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

スーパーバイザおよびモジュール上で一貫した MAC アドレス テーブル

各モジュールのすべての MAC アドレス テーブルが、スーパーバイザ上の MAC アドレスと正確に一致するのが理想的です。 Cisco NX-OS 4.1(2) 以降では、**show forwarding consistency l2** コマンドを入力すると、デバイスが不一致、欠落、および余分な MAC アドレス エントリを表示します。

レイヤ 3 スタティック MAC アドレス

リリース 4.2 以降では、すべてのレイヤ 3 インターフェイスに対してスタティック MAC アドレスを設定できます。 レイヤ 3 インターフェイスのデフォルトの MAC アドレスは、VDC MAC アドレスです。

スタティック MAC アドレスは、次のレイヤ 3 インターフェイスに設定できます。

- レイヤ 3 インターフェイス
- レイヤ 3 サブインターフェイス
- レイヤ 3 ポート チャネル
- VLAN ネットワーク インターフェイス

（注） トンネル インターフェイスにはスタティック MAC アドレスを設定できません。

レイヤ 3 インターフェイスの設定の詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』を参照してください。

スイッチングのハイ アベイラビリティ

従来のイーサネット スイッチングごとに、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。 リリース 4.2(1) 以降では、レイヤ 3 インターフェイス上にスタティック MAC アドレスを設定している場合、ソフトウェアをダウングレードするために、これらのポートの設定を解除する必要があります。

（注） ハイ アベイラビリティ機能の詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

レイヤ 2 スイッチングのバーチャライゼーションのサポート

デバイスは Virtual Device Context（VDC; 仮想デバイス コンテキスト）をサポートしており、MAC アドレス テーブルの設定と操作は VDC にローカルです。

（注） VDC およびリソースの割り当ての詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

レイヤ 2 スイッチングのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	レイヤ 2 スイッチングにライセンスは必要ありません。 ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OS のライセンス スキームの詳細は、『*Cisco NX-OS Licensing Guide*』を参照してください。

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

MAC アドレス設定の前提条件

MAC アドレスには次の前提条件があります。

- デバイスにログインしていること。
- 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。

MAC アドレスの設定に関する注意事項および制約事項

MAC アドレスの設定に関する注意事項と制約事項は次のとおりです。

MAC アドレス テーブル	時間別グループ
M1 ラインカード	128,000 エントリ
F1 ラインカード	16,000 ～ 256,000 エントリ
F2 ラインカード	16,000 ～ 192,000 エントリ

NX-OS Release 6.0.1 以降、学習モード機能がサポートされます。 学習モードには次の注意事項と制限があります。

ラインカード	クラシックイーサネット（CE）で非会話型の学習をサポート	クラシックイーサネット（CE）で会話型学習をサポート	FabricPath の会話型学習	FabricPath の非会話型の学習
M1	Yes	該当せず	該当せず	該当せず
F1	Yes	Yes	Yes	No
F2	Yes	Yes	Yes	Yes（スイッチ仮想インターフェイス（SVI）が設定されている場合）。

レイヤ 2 スイッチングのデフォルト設定

次の表に、レイヤ 2 スイッチングのパラメータのデフォルト設定を示します。

表 *2*：レイヤ *2* スイッチング パラメータのデフォルト値

パラメータ	デフォルト
エージング タイム	1800 秒

NX-OS Release 6.0.1 以降、学習モード機能がサポートされます。 次の表に、デフォルトの学習モード パラメータを示します。

表 *3*：デフォルトの学習モード パラメータ

パラメータ	デフォルト
クラシック イーサネット（CE）VLAN	非会話型
FabricPath VLAN	会話型

レイヤ 2 スイッチングの設定手順

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

スタティック MAC アドレスの設定

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

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**mac address-table static** *mac-address* **vlan** *vlan-id* {[**drop** | **interface** {*type slot/port*} | **port-channel** *number*]} 例： `switch(config)# mac-address-table static 1.1.1 vlan 2 interface ethernet 1/2`	レイヤ 2 MAC アドレス テーブルに追加するスタティック MAC アドレスを指定します。

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

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

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

```
switch# config t
switch(config)# mac address-table static 1.1.1 vlan 2 interface ethernet 1/2
switch(config)#
```

レイヤ 3 インターフェイス上のスタティック MAC アドレスの設定

リリース 4.2(1) から、レイヤ 3 インターフェイス上にスタティック MAC アドレスを設定できるようになりました。 ブロードキャストまたはマルチキャストのアドレスは、スタティック MAC アドレスとして設定できません。

（注） トンネル インターフェイス上には、スタティック MAC アドレスを設定できません。

レイヤ 3 インターフェイスの設定の詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』を参照してください。

はじめる前に

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

手順の概要

1. **config t**
2. **interface** [**ethernet** *slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*]
3. **mac-address** *mac-address*
4. **exit**
5. （任意） **show interface** [**ethernet** *slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*]
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** [**ethernet** *slot/port*	**ethernet** *slot/port.number*	**port-channel** *number*	**vlan** *vlan-id*] 例： `switch(config)# interface ethernet 7/3`	レイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 （注） スタティック MAC アドレスを割り当てる前に、レイヤ 3 インターフェイスを作成する必要があります。

ステップ 3	**mac-address** *mac-address*
	
	例：
	`switch(config-if)# mac-address 21ab.47dd.ff89`
	`switch(config-if)#`
		レイヤ 3 インターフェイスに追加するスタティック MAC アドレスを指定します。

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

	コマンドまたはアクション	目的
ステップ 5	**show interface** [**ethernet** *slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*] 例： `switch# show interface ethernet 7/3`	（任意） レイヤ 3 インターフェイスに関する情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、スロット 7、ポート 3 上のレイヤ 3 インターフェイスにスタティック MAC アドレスを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 7/3
switch(config-if)# mac-address 21ab.47dd.ff89
switch(config-if)#
```

MAC テーブルのエージング タイムの設定

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

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

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

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

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

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

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

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

VLAN の学習モードの設定

NX-OS Release 6.0.1 以降、VLAN の学習モードの設定がサポートされます。 設定された学習モードに基づいて、Cisco NX-OS ソフトウェアは、会話型または非会話型のいずれでも MAC をハードウェアにインストールできます。

はじめる前に

VLAN の学習モードを設定する前に、正しい VDC を開始していることを確認します（または **switchto vdc** コマンドを入力します）。

手順の概要

1. **config t**
2. **mac address-table learning-mode conversational** *vlan-range of CE-vlans*
3. **exit**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**mac address-table learning-mode conversational** *vlan-range of CE-vlans* 例： `switch(config)# mac address-table learning-mode conversational vlan1`	レイヤ 2 MAC アドレス テーブルに学習モードを指定します。 会話型学習と非会話型学習が選択できます。

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

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

```
switch# config t
switch(config)# mac address-table learning-mode conversational vlan1
switch(config)# end
switch(config)# show mac address-table learning-mode
```

MAC アドレス テーブルの整合性検査

リリース 4.1(2) から、 スーパーバイザ上の MAC アドレス テーブルとすべてのモジュールの一致を確認できるようになりました。

手順の概要

1. **show forwarding consistency l2** {*module_number*}

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**show forwarding consistency l2** {*module_number*}
	
	例：
	`switch# show forwarding consistency l2 7`
	`switch#`
		スーパーバイザと指定のモジュールの間の、矛盾、不足、余分な MAC アドレスを表示します。

次に、スーパーバイザと指定のモジュールの間の、MAC アドレス テーブル内の矛盾、不足、余分なエントリを表示する例を示します。

```
switch# show forwarding consistency l2 7
switch#
```

MAC テーブルからのダイナミック アドレスのクリア

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

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear mac address-table dynamic** {**address** *mac_addr*} {**interface** [**ethernet** *slot/port*	**loopback** *number*	**port-channel** *channel-number*]} {**vlan** *vlan_id*} 例： `switch# clear mac address-table dynamic`	レイヤ 2 の MAC アドレス テーブルから、ダイナミック アドレス エントリをクリアします。

	コマンドまたはアクション	目的
ステップ 2	**show mac address-table** 例： `switch# show mac address-table`	（任意） MAC アドレス テーブルを表示します。

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

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

レイヤ 2 スイッチング設定の確認

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

コマンド	目的
show mac address-table	MAC アドレス テーブルに関する情報を表示します。
show mac address-table aging-time	MAC アドレス テーブルに設定されているエージング タイムの情報を表示します。
show mac address-table static	MAC アドレス テーブルのスタティック エントリの情報を表示します。
show interface [*interface*] **mac-address**	インターフェイスの MAC アドレスとバーンドイン MAC アドレスを表示します。
show forwarding consistency l2 {*module*}	モジュールとスーパーバイザのテーブル間の不一致、不明、および追加の MAC アドレスを表示します。

これらのコマンド出力の詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』を参照してください。

レイヤ 2 スイッチングの設定例

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

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

レイヤ 2 スイッチングの追加情報（CLI バージョン）

関連資料

関連項目	参照先
ポート セキュリティ、スタティック MAC アドレス	『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x*』
インターフェイス	『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』
ハイ アベイラビリティ	『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』
仮想デバイス コンテキスト（VDC）	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
システム管理	『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x*』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.x*』

標準

標準	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。	—

レイヤ 2 スイッチングの設定の機能履歴（CLI バージョン）

次の表に、この機能のリリースの履歴を示します。

表 *4*：レイヤ *2* スイッチングの設定の機能履歴

機能名	リリース	機能情報	
VLAN の学習モード	6.0(1)	VLANに、会話型または非会話型の学習モードを設定できます。	
レイヤ3インターフェイススタティック MAC アドレス	4.2(1)	レイヤ3インターフェイスにスタティック MAC アドレスを設定できます。	
show mac address-table	4.1(2)	vPCがイネーブルおよび実行中であるときの、追加情報を表示します。	
レイヤ 2 の整合性	4.1(2)	**show forwarding consistency l2** コマンドを実行すると、MAC アドレステーブルでモジュール間に不整合があるエントリが表示されます。	

第 4 章

VLAN の設定

この章では、Cisco NX-OS デバイス上で仮想 LAN（VLAN）を設定する方法について説明します。

この章は、次の内容で構成されています。

- Information About VLANs，27 ページ
- Licensing Requirements for VLANs，32 ページ
- Prerequisites for Configuring VLANs，33 ページ
- Guidelines and Limitations for Configuring VLANs，33 ページ
- VLAN のデフォルト設定，33 ページ
- Configuring a VLAN，34 ページ
- VLAN の設定の確認，43 ページ
- VLAN 統計情報の表示とクリア，44 ページ
- VLAN の設定例，44 ページ
- VLAN の追加情報（CLI バージョン），44 ページ
- VLAN 設定の機能履歴（CLI バージョン），46 ページ

Information About VLANs

（注） Beginning with Cisco Release 5.2(1) for Cisco Nexus 7000 Series devices, you can create Fibre Channel over Ethernet (FCoE) VLANs. For more information, see the 『*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*』.

You can use VLANs to divide the network into separate logical areas at the Layer 2 level. VLANs can also be considered as broadcast domains.

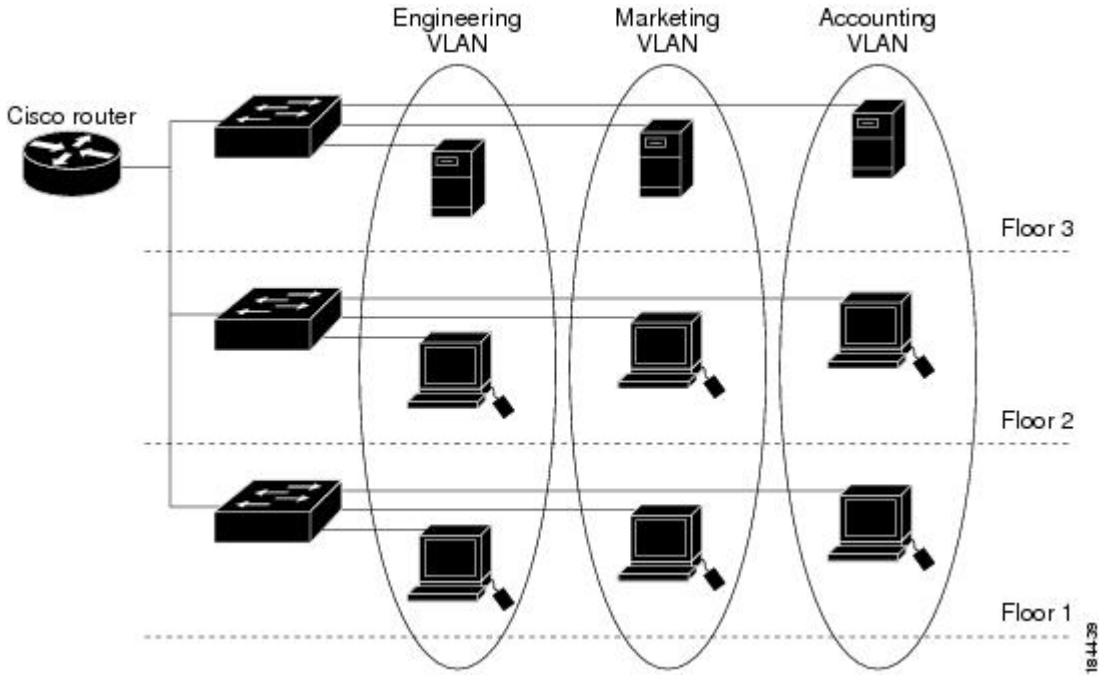
Any switch port can belong to a VLAN, and unicast broadcast and multicast packets are forwarded and flooded only to end stations in that VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router.

VLANs Overview

A VLAN is a group of end stations in a switched network that is logically segmented by function or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment.

Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in that VLAN. Each VLAN is considered as a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router. The following figure shows VLANs as logical networks. The stations in the engineering department are assigned to one VLAN, the stations in the marketing department are assigned to another VLAN, and the stations in the accounting department are assigned to another VLAN.

図 *2* : ***VLANs as Logically Defined Networks***



VLANs are usually associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. To communicate between VLANs, you must route the traffic.

By default, a newly created VLAN is operational; that is, the newly created VLAN is in the no shutdown condition. Additionally, you can configure VLANs to be in the active state, which is passing traffic, or the suspended state, in which the VLANs are not passing packets. By default, the VLANs are in the active state and pass traffic.

A VLAN interface, or switched virtual interface (SVI), is a Layer 3 interface that is created to provide communication between VLANs. In order to route traffic between VLANs, you must create and configure a VLAN interface for each VLAN. Each VLAN requires only one VLAN interface.

（注） See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』 for complete information on configuring VLAN interfaces, and subinterfaces, as well as assigning IP addresses. This feature must be enabled before you can configure VLAN interfaces.

VLAN Ranges

（注） The extended system ID is always automatically enabled in Cisco NX-OS devices.

The device supports up to 4094 VLANs in accordance with the IEEE 802.1Q standard in each VDC. The software organizes these VLANs into ranges, and you use each range slightly differently.

This table describes the VLAN ranges.

表 *5*：*VLAN Ranges*

VLANs Numbers	Range	Usage
1	Normal	Cisco default. You can use this VLAN, but you cannot modify or delete it.
2—1005	Normal	You can create, use, modify, and delete these VLANs.
1006—3967 and 4048—4093	Extended	You can create, name, and use these VLANs. You cannot change the following parameters: • The state is always active. • The VLAN is always enabled. You cannot shut down these VLANs.
3968-4047 and 4094	Internally allocated	These 80 VLANs and VLAN 4094 are allocated for internal device use. You cannot create, delete, or modify any VLANs within the block reserved for internal use.

VLANs Numbers	Range	Usage
3968-4095 （注） 4095 is reserved and unused as per 802.1Q standard.	Internally allocated	Beginning with Cisco release 5.2(1) for Cisco Nexus 7000 Series devices, VLANs 3968 to 4095 are reserved for internal use in each VDC by default. You can change the reserved VLANs to any other 128 contiguous VLAN range. When you reserve such a range, it frees up the range of VLANs that were allocated for internal use by default, and all of those VLANs are available for user configuration except for VLAN 4095. All VDCs inherit the new reserved range of VLANs. （注） VLAN 0 is reserved for 8.01.p trafffic.

The software allocates a group of VLAN numbers for features like multicast and diagnostics, that need to use internal VLANs for their operation. You cannot use, modify, or delete any of the VLANs in the reserved group. You can display the VLANs that are allocated internally and their associated use.

Beginning with Cisco NX-OS Release 5.2(1), the system allocates a block of 128 reserved VLANs (3968 to 4094) for these internal uses. You can change the block of 128 reserved VLANs to occupy another range of 128 adjacent VLANs. For example, you can change the reserved block of VLANs to be 400 to 528. You cannot assign a previously created VLAN as part of the 128 range of reserved VLANs. Anytime you change the reserved block of VLANs for the device, you must do the following:

- Enter the **copy running-configuration startup-configuration** command
- Reload the device

（注） When you change the range of reserved VLANs, the existing configurations for the new range of VLANs get deleted. A warning note is displayed as in the following example:

```
switch(config)# system vlan 2000 reserve
This will delete all configs on vlans 2000-2127. Continue anyway? (y/n) [no] y
Note: After switch reload, VLANs 2000-2127 will be reserved for internal use.
      This requires copy running-config to startup-config before
      switch reload. Creating VLANs within this range is not allowed.
switch(config)#
```

To return to the default block of reserved VLANs (3968 to 4094), you must enter the **no system reserve vlan** command. The write-erase procedure does not restore the default reserved VLAN range to 3968 to 4094.

Creating, Deleting, and Modifying VLANs

Beginning with Cisco NX-OS Release 5.1(1) , you can configure a VLAN without actually creating the VLAN. This procedure is used for IGMP snooping, VTP, and other configurations.

（注） By default, all Cisco NX-OS ports are Layer 3 ports.

VLANs are numbered from 1 to 4094 for each VDC. All ports that you have configured as switch ports belong to the default VLAN when you first bring up the switch as a Layer 2 device. The default VLAN (VLAN1) uses only default values, and you cannot create, delete, or suspend activity in the default VLAN.

You create a VLAN by assigning a number to it; you can delete VLANs and move them from the active operational state to the suspended operational state. If you attempt to create a VLAN with an existing VLAN ID, the device goes into the VLAN submode but does not create the same VLAN again.

Newly created VLANs remain unused until Layer 2 ports are assigned to the specific VLAN. All the ports are assigned to VLAN1 by default.

Depending on the range of the VLAN, you can configure the following parameters for VLANs (except the default VLAN):

- VLAN name
- VLAN state
- Shutdown or not shutdown

（注） See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』 for information on configuring ports as VLAN access or trunk ports and assigning ports to VLANs.

When you delete a specified VLAN, the ports associated to that VLAN become inactive and no traffic flows. When you delete a specified VLAN from a trunk port, only that VLAN is shut down and traffic continues to flow on all the other VLANs through the trunk port.

However, the system retains all the VLAN-to-port mapping for that VLAN, and when you reenable or re-create, that specified VLAN, the system automatically reinstates all the original ports to that VLAN. The static MAC addresses and aging time for that VLAN are not restored when the VLAN is reenabled.

（注） Commands entered in the VLAN configuration submode are immediately executed. Beginning with Cisco release 5.1 for Nexus 7000 series devices, you must exit the VLAN configuration submode for configuration changes to take effect.

High Availability for VLANs

The software supports high availability for both stateful and stateless restarts, as during a cold reboot, for VLANs. For the stateful restarts, the software supports a maximum of three retries. If you try more than 3 times within 10 seconds of a restart, the software reloads the supervisor module.

You can upgrade or downgrade the software seamlessly when you use VLANs.

（注） See the 『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』, for complete information on high availability features.

Virtualization Support for VLANs

The software supports virtual device contexts (VDCs), and VLAN configuration and operation are local to the VDC.

（注） See the 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』, for complete information on VDCs and assigning resources.

Each VLAN must have all of its ports in the same VDC. If you do not have enough resources allocated to the VDC, the software returns an error message.

When you create a new VDC, the device automatically creates a new default VLAN, VLAN1, and internally reserves VLANs for device use.

You can re-use the same numbers for VLANs in different VDCs.

One or more VLANs can be associated with a role to either allow or disallow the user to configure it. When a VLAN is associated with a role, the corresponding interfaces will also be subjected to the same check. For instance, if a role is allowed to access VLAN1, then that role also has access to the interfaces that have that VLAN. If an interface does not have the VLAN associated with a role, that interface is not accessible to that role.

Licensing Requirements for VLANs

The following table shows the licensing requirements for this feature.

Product	License Requirement
Cisco NX-OS	VLANs require no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the 『*Cisco NX-OS Licensing Guide*』.

However, using VDCs requires an Advanced Services license.

Prerequisites for Configuring VLANs

VLANs have the following prerequisites:

- You must be logged onto the device.
- If necessary, install the Advanced Services license and enter the desired VDC. Ensure that you have allocated enough resources for that VDC. See the 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』, for information on creating VDCs and allocating resources.
- You must create the VLAN before you can do any modification of that VLAN.

Guidelines and Limitations for Configuring VLANs

VLANs have the following configuration guidelines and limitations:

- The maximum number of VLANs per VDC is 4094.
- You can reuse VLAN ID numbers in different VDCs. For example, you can have VLAN10 in the default VDC and a completely separate VLAN10 in a newly created VDC, such as VDC 2.
- You can configure a single VLAN or a range of VLANs.
- You cannot create, modify, or delete any VLANs that are within the group of VLANs reserved for internal use.
- VLAN1 is the default VLAN. You cannot create, modify, or delete this VLAN.
- VLANs 1006 to 4094 are always in the active state and are always enabled. You cannot suspend the state or shut down these VLANs.

VLAN のデフォルト設定

次の表に、VLAN パラメータのデフォルト設定を示します。

表 *6*：*VLAN* パラメータのデフォルト値

パラメータ	デフォルト
VLANs	イネーブル
VLAN	VLAN1：スイッチ ポートとして設定したポートは、VLAN1 に割り当てられます。
VLAN ID	1

パラメータ	デフォルト
VLAN 名	• デフォルト VLAN（VLAN1）- default • 他のすべての VLAN：VLAN *vlan-id*
VLAN ステート	アクティブ
STP	イネーブル：Rapid PVST+ がイネーブル
VTP	ディセーブル
VTP バージョン	1

Configuring a VLAN

（注） See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』, for information on assigning Layer 2 interfaces to VLANs (access or trunk ports). All interfaces are in VLAN1 by default.

（注） If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

VLAN の作成と削除（CLI バージョン）

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。

VLAN を作成すると、その 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 に関連するポートは非アクティブになります。 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たままで、削除した VLAN を除く他のすべての VLAN からのトラフィックが引き続き転送されます。

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

（注） VLAN コンフィギュレーション サブモードで VLAN の作成と削除を行うこともできます。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**vlan** {*vlan-id* | *vlan-range*}
	
	例：
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		VLAN または VLAN の範囲を作成します。 割り当て済みの VLAN 番号を入力すると、その VLAN の VLAN コンフィギュレーション サブモードが開始されます。 内部的に割り当てられている VLAN に割り当てられている番号を入力すると、エラー メッセージが返されます。 VLAN の範囲を入力し、指定 VLAN の 1 つ以上が、内部的に割り当てられた VLAN の範囲外である場合、コマンドは範囲外の VLAN だけで有効になります。 指定できる範囲は 2 ～ 4094 です。VLAN1 はデフォルト VLAN であり、作成や削除はできません。 内部使用のために予約されている VLAN の作成や削除はできません。

ステップ 3	**exit**
	
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		VLAN モードを終了します。

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

次の例は、15 ～ 20 の範囲で VLAN を作成する方法を示しています。

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

VLAN コンフィギュレーション サブモードの開始

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

- Name
- State
- Shut down

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**vlan** {*vlan-id* | *vlan-range*}
	
	例：
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		VLAN 設定サブモードにします。 このサブモードでは、VLAN または VLAN 範囲に対して、名前の指定、ステートの設定、ディセーブル化、およびシャット ダウンを実行できます。
		VLAN1 または内部的に割り当てられた VLAN に対しては、これらの値を変更できません。

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

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

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

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

VLAN の設定

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

- Name
- State
- Shut down

（注） デフォルト VLAN または内部的に割り当てられた VLAN の作成、削除、変更はできません。また、一部の VLAN では変更できないパラメータがあります。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**vlan** {*vlan-id*	*vlan-range*}
		
		例：
		`switch(config)# vlan 5`
		`switch(config-vlan)#`
			VLAN設定サブモードにします。 既存の VLAN ではない場合、指定した VLAN が作成され、VLAN コンフィギュレーション サブモードが開始されます。

ステップ 3	**name** *vlan-name* 例： `switch(config-vlan)# name accounting`	VLANに名前を付けます。 32 文字までの英数字を入力して VLAN に名前を付けることができます。 VLAN1 または内部的に割り当てられている VLAN の名前は変更できません。 デフォルト値は VLANxxxx であり、xxxx は、VLAN ID 番号と等しい 4 桁の数字（先行ゼロも含む）を表します。

	コマンドまたはアクション	目的
ステップ 4	**state** {**active** | **suspend**} 例： `switch(config-vlan)# state active`	VLAN のステート（アクティブまたは一時停止）を設定します。VLAN ステートを一時停止にすると、その VLAN に関連付けられたポートが非アクティブになり、VLAN のトラフィック転送が停止します。デフォルト ステートは active です。デフォルト VLAN および VLAN 1006 ～ 4094 のステートを一時停止にすることはできません。
ステップ 5	**no shutdown** 例： `switch(config-vlan)# no shutdown`	VLAN をイネーブルにします。デフォルト値は no shutdown（イネーブル）です。デフォルト VLAN の VLAN1、または VLAN 1006 ～ 4094 はシャットダウンできません。

ステップ 6	**exit**
	
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		VLAN コンフィギュレーション サブモードを終了します。

ステップ 7	**show vlan** 例： `switch# show vlan`	（任意） VLAN の情報およびステータスを表示します。
ステップ 8	**show vtp status** 例： `switch# show vtp status`	（任意） VLAN トランキング プロトコル（VTP）の情報およびステータスを表示します。
ステップ 9	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 （注） VLAN コンフィギュレーション サブモードで入力したコマンドはすぐに実行されます。Nexus 7000 シリーズ デバイスの Cisco Release 5.1 以降では、コンフィギュレーションの変更を反映するために VLAN コンフィギュレーション サブモードを終了する必要があります。

次の例は、VLAN 5 のオプション パラメータを設定する方法を示しています。

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

予約された VLAN の範囲の変更

予約されたVLANの範囲を変更するには、コンフィギュレーションモードで作業を行う必要があります。 このコマンドを入力すると、次の作業をする必要があります。

- **copy running-config startup-config** コマンドを入力
- デバイスのリロード

手順の概要

1. **config t**
2. **system vlan** {*start-vlan*} **reserve**
3. **copy running-config startup-config**
4. **reload**
5. （任意） **show system vlan reserved**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**system vlan** {*start-vlan*} **reserve**
	
	例：
	`switch(config)# system vlan 2000 reserve`
	`This will delete all configs on vlans 2000-2127. Continue anyway? (y/n) [no] y`
	`Note: After switch reload, VLANs 2000-2127 will be reserved for internal use.`
	`This requires copy running-config to startup-config before switch reload. Creating VLANs within this range is not allowed.`
	`switch(config)#`
		目的の範囲の開始 VLAN ID を指定することにより、予約済みの VLAN の範囲を変更できます。
		
		予約済みの VLAN を、128 の隣接する他の VLAN 範囲に変更できます。 このような範囲を予約すると、内部使用のためにデフォルトで割り当てられた VLAN 範囲が解放され、それらの VLAN はすべて VLAN 4094 を除くユーザ設定に使用できます。 すべての VDC は予約された新しい VLAN の範囲を継承します。
		
		（注） 予約済み VLAN（3968 ～ 4094）のデフォルトの範囲に戻すには、**no system vlan reserve** コマンドを入力する必要があります。

ステップ 3	**copy running-config startup-config**
	
	例：
	`switch(config)# copy running-config startup-config`
	`switch(config)#`
		実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
		
		（注） 予約済みのブロックを変更した場合、このコマンドを入力する必要があります。

	コマンドまたはアクション	目的
ステップ 4	**reload** 例： `switch(config)# reload`	ソフトウェアをリロードし、VLAN の範囲の変更が有効になります。 このコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x*』を参照してください。
ステップ 5	**show system vlan reserved** 例： `switch(config)# show system vlan reserved`	（任意） VLAN 範囲に対して設定された変更を表示します。

次に、予約済みの VLAN 範囲を変更する例を示します。

```
switch# config t
switch(config)# system vlan 2000 reserve
switch(config)# copy running-config startup-config
switch(config)# reload
switch(config)# show system vlan reserved
```

（注） この変更を有効にするには、デバイスをリロードする必要があります。

VLAN 作成前の VLAN 設定

Cisco NX-OS Release 5.1(1) 以降は、VLAN を作成する前に、VLAN を設定できます。 この手順は、IGMP スヌーピング、VTP および他の設定に使用されます。

（注） **show vlan** コマンドでは、**vlan** コマンドを使用してそれを作成しない限り、これらの VLAN は表示されません。

手順の概要

1. **config t**
2. **vlan configuration** {*vlan-id*}

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーションモードを開始します。

ステップ 2	**vlan configuration** {*vlan-id*}
	
	例：
	`switch(config)# vlan configuration 20`
	`switch(config-vlan-config)#`
		実際にこれらを作成しないで VLAN を設定できるようにします。

次に、これを作成する前に VLAN を設定する例を示します。

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

VLAN ロング ネームのイネーブル化

Cisco NX-OS Release 6.1.0 以降では、128 文字までの VLAN ロング ネームを設定できます。

はじめる前に

VTP はトランスペアレントまたはオフ モードである必要があります。 VTP は、クライアントまたはサーバ モードにすることはできません。 VTP の詳細については「VTP の設定」の章を参照してください。

手順の概要

1. **configure terminal**
2. **system vlan long-name**
3. （任意） **copy running-config startup-config**
4. **show running-config vlan**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**system vlan long-name** 例： `switch(config)# system vlan long-name`	128 文字までの VLAN 名をイネーブルにできます。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。
ステップ 4	**show running-config vlan** 例： `switch(config)# show running-config vlan`	システム VLAN のロング ネーム機能がイネーブルであることを確認します。

次に、VLAN ロング ネームをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# system vlan long-name
switch(config)# copy running config startup config
switch(config)# show running-config vlan
```

VLAN の設定の確認

VLAN の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config vlan *vlan-id*	VLAN 情報を表示します。
show vlan [**all-ports** | **brief** | **id** *vlan-id* | **name** *name* | **dot1q tag native**]	VLAN 情報を表示します。
show vlan summary	VLAN 情報の要約を表示します。
show vtp status	VTP 情報を表示します。
show system vlan reserved	システムに予約されている VLAN 範囲を表示します。

これらのコマンド出力の詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』を参照してください。

VLAN 統計情報の表示とクリア

VLAN の設定情報を表示するには、次のいずれかの作業を行います。

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

VLAN の設定例

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

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

VLAN の追加情報（CLI バージョン）

関連資料

関連項目	参照先
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』
NX-OS レイヤ 2 スイッチングの設定	『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』
インターフェイス、VLAN インターフェイス、IP アドレス指定、ポート チャネル	『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』

関連項目	参照先
マルチキャスト ルーティング	『*Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide*』
NX-OS の基礎	『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x*』
ハイ アベイラビリティ	『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』
システム管理	『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x*』
仮想デバイス コンテキスト（VDC）	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.x*』

標準

標準	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 のリンク
CISCO-VLAN-MEMBERSHIP MIB には、次のものが含まれます。 • vmMembership Table • MIBvmMembershipSummaryTable • MIBvmMembershipSummaryTable	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

VLAN 設定の機能履歴（CLI バージョン）

次の表に、この機能のリリースの履歴を示します。

表 *7*：*VLAN* 設定の機能履歴

機能名	リリース	機能情報
VLAN ロング ネーム設定します。	6.1(1)	VLANロング ネームを設定できます。
ダイナミック システムに予約されている VLAN 範囲	5.2(1)	システムが予約する VLAN の範囲を変更できます。
VLAN を作成する前に、VLAN を設定します。	5.1(1)	VLAN を作成する前に、VLAN を設定できます。
変更なし	4.2(1)	--
VLAN トランキング プロトコル	4.1(2)	デバイスは VTP をトランスペアレント モードで実行します。

第 5 章

VTP の設定

この章では、Cisco NX-OS デバイスで VLAN トランキング プロトコル（VTP）および VTP プルーニングを設定する方法について説明します。

この章は、次の内容で構成されています。

- VTP の概要，47 ページ
- デフォルト設定，50 ページ
- VTP の設定，51 ページ
- VTP プルーニングの設定，53 ページ

VTP の概要

Cisco NX-OS Release 5.1(1) 以降、VTP および VTP プルーニングは、VTP バージョン 1 および 2 でサポートされます。 Release 5.1(1) よりも前のリリースでは、VTP トランスペアレント モードだけがサポートされていました。

（注） Cisco NX-OS Release 5.1(1) 以降、実際に VLAN を作成しないで VLAN を設定できます。 詳細については、VLAN 作成前の VLAN 設定，（41 ページ）を参照してください。

VTP

VTP is a Layer 2 messaging protocol that maintains VLAN consistency by managing the addition, deletion, and renaming of VLANs within a VTP domain. A VTP domain is made up of one or more network devices that share the same VTP domain name and that are connected with trunk interfaces. Each network device can be in only one VTP domain.

Layer 2 trunk interfaces, Layer 2 port channels, and virtual port channels (vPCs) support VTP functionality.

The VTP is disabled by default on the device. You can enable and configure VTP using the command-line interface (CLI). When VTP is disabled, the device does not relay any VTP protocol packets.

For information about enabling and configuring VTP, see the 『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』.

（注） Before Release 5.1(1), VTP worked only in transparent mode in the Cisco Nexus 7000 Series devices, allowing you to extend a VTP domain across the device.

When the device is in the VTP transparent mode, the device relays all VTP protocol packets that it receives on a trunk port to all other trunk ports. When you create or modify a VLAN that is in VTP transparent mode, those VLAN changes affect only the local device. A VTP transparent network device does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements.

（注） VLAN 1 is required on all trunk ports used for switch interconnects if VTP is supported in the network. Disabling VLAN 1 from any of these ports prevents VTP from functioning properly.

If you enable VTP, you must configure either version 1 or version 2. If you are using VTP in a Token Ring environment, you must use version 2.

VTP の概要

VTP は、各ルータまたは LAN デバイスがトランク ポートのフレームでアドバタイズメントを送信することを可能にします。 これらのフレームは、すべてのネイバーデバイスで受信できるマルチキャストアドレスに送信されます。 これらは通常のブリッジングの手順では転送されません。アドバタイズメントは、送信側デバイスの VTP 管理ドメイン、設定のリビジョン番号、認識している VLAN、既知の各 VLAN の特定のパラメータを示します。 これらのアドバタイズメントの検知によって、同じ管理ドメイン内のすべてのデバイスは、送信デバイスで設定されている新しい VLAN について学習します。 このプロセスは、管理ドメイン内の 1 台の装置だけに新しい VLAN を作成し、設定できます。またその後、同じ管理ドメイン内の他のすべてのデバイスによって情報が自動的に学習されます。

デバイスが VLAN について学習すると、デバイスはデフォルトでトランク ポートからその VLAN 上のすべてのフレームを受信し、必要に応じて、他のトランク ポートへそれらを転送します。 このプロセスは、不要な VLAN のトラフィックがデバイスに送信されるのを防ぎます。 VTP プルーニングと呼ばれる VTP の拡張は、ブロードキャスト トラフィックの範囲を制限し、帯域幅を節約するために定義されたものです。 Release 5.1(1) 以降、Cisco NX-OS ソフトウェアでは、VTP プルーニングをサポートします。

VTP は、Cisco Discovery Protocol（CDP）など他のプロセスで読み取ることができる共有ローカル データベースで、ドメインおよびモードに関する情報をパブリッシュします。

VTP モード

Release 5.1(1) 以降では、VTP は次のモードでサポートされます。

- トランスペアレント：他のすべてのトランク ポートにトランク ポート上で受信したすべての VTP プロトコル パケットを中継することが可能です。 VTP トランスペアレント モードの VLAN を作成または変更するとき、それらの VLAN の変更は、ローカル デバイスだけに影響します。 VTP トランスペアレント ネットワーク デバイスは、VLAN 設定をアドバタイズせず、受信したアドバタイズに基づいて同期化することもありません。 これらの VLAN はトークン リング用に予約されているため、VTP クライアント/サーバ モードで VLAN を 1002 ～ 1005 に設定できません。
- サーバ：ネットワーク全体で VLAN の作成、削除、および変更が可能です。 VTP バージョンなど、その他の設定オプションを設定し、VTP ドメイン全体で VTP プルーニングをオン/オフすることもできます。 VTP サーバは、同一 VTP ドメイン内の他のスイッチに、自らの VLAN設定をアドバタイズし、トランク リンクを介して受信したメッセージに基づいて、自らの VLAN設定を他のスイッチと同期させます。 Release 5.1(1) 以降、サーバ モードがデフォルトのモードです。 VLAN 情報はブート フラッシュに格納され、リブート後に削除されません。
- クライアント：VTP クライアントは、VTP サーバと同様に動作しますが、VTP クライアント上で VLAN の作成、変更、または削除を行うことはできません。
- オフ：非トランスペアレント モードと同様に動作しますが、VTP パケットを転送しません。 オフ モードでは、VTP を実行しないで CISCO-VTP-MIB を使用して VLAN をモニタすることができます。 Cisco Nexus 7000 シリーズ デバイスでは、VTP が条件付きサービスであるため、MIB は、対応する機能がイネーブルの場合にだけロードされます。 CISCO-VTP-MIB はこの規則に従いません。 VLAN マネージャによってロードされ、VTP のプロセスがイネーブルまたはディセーブルのどちらになっているか、常に正しい値を返します。

Cisco NX-OS リリース 6.1（1）以降、VTP がトランスペアレントまたはオフ モードの場合、128 文字までの VLAN ロング ネームを設定できます。 VTP がクライアント モードまたはサーバ モードの場合、VLAN ロング ネームをイネーブルにできません。 詳細については、「VLAN の設定」の章を参照してください。

インターフェイス単位の VTP

VTP では、VTP トラフィックを制御するために、ポート単位で VTP プロトコルをイネーブル、またはディセーブルにすることができます。 トランクがスイッチまたはエンドデバイスに接続されている場合、着信 VTP パケットをドロップし、この特定のトランクで VTP アドバタイズメントを防ぎます。 デフォルトでは、VTP はすべてのスイッチ ポートでイネーブルになります。

VTP プルーニング

VLAN アーキテクチャは VLAN 内でアクティブになっているデバイスが存在しないスイッチにつながる場合でも、VLAN がトランク ポート間で送信される際にすべてのフラッディング トラフィックが必要です。 この方法では、無駄なネットワーク帯域幅が発生します。

VTP プルーニングは、すべてのアクティブなネットワーク デバイスに到達可能なトランク ポートだけにフラッディング トラフィックを制限することによって、ネットワーク帯域幅の使用状況を

最適化します。 このプロトコルが使用されている場合、適切な Join メッセージを受信できない限り、トランク ポートは特定の VLAN のためのフラッディング トラフィックを受信しません。

Join メッセージは、すでに VTP プロトコルのバージョン 1 でサポートされているものに加えて、新しいメッセージ タイプとして定義されます。 VTP を実装すると、生成するサマリー アドバタイズメントのメッセージの最後に特別な TLV を付けることにより、この拡張がサポートされます。 VTP トランスペアレント モードでは、VTP はすべての VTP パケットを中継し、プルーニングは VTP のサマリー パケットでスイッチによる TLV の処理を必要とします。 VTP トランスペアレント モードでは、プルーニングを使用できません。

VTP プルーニングとスパニングツリー プロトコル

VTP は起動時に STP を照会し、STP によって生成される通知をリスニングすることによってスパニングツリー プロトコル（STP）フォワーディング ステートでトランク ポートのリストを保持します。

VTP は、STP との相互作用によって、プルーニングまたは結合されたステートにトランク ポートを設定します。 STP は、トランク ポートがブロッキング ステートまたはフォワーディング ステートになると、VTP に通知します。 VTP は、トランク ポートがプルーニングまたは結合されると STP に通知します。

デフォルト設定

次の表に、VTP パラメータのデフォルト設定を示します。

表 *8*：デフォルトの *VTP* パラメータ

パラメータ	デフォルト
VTP	ディセーブル
VTP モード	トランスペアレント
VTP ドメイン	ブランク
VTP バージョン	1
VTP プルーニング	ディセーブル
インターフェイス単位の VTP	イネーブル

VTP の設定

VTP の設定

Cisco NX-OS デバイスで VTP を設定できます。

（注） VTP がネットワークのトランスペアレント モードで使用されている場合、スイッチの相互接続に使用されるすべてのトランク ポートで VLAN 1 が必要です。 これらのポートのいずれかから VLAN 1 をディセーブルにすると、VTP はトランスペアレント モードで適切に機能しなくなります。

（注） Release 5.1(1) よりも前のリリースでは、VTP はトランスペアレント モードでのみ動作していました。

はじめる前に

正しい仮想デバイス コンテキスト（VDC）を開始していることを確認します（または**switchto vdc** コマンドを入力します）。 VDC が異なっていても同じ VLAN 名と ID を使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の概要

1. **config t**
2. **feature vtp**
3. **vtp domain** *domain-name*
4. **vtp version** {**1** | **2**}
5. **vtp mode** {**client** | **server**| **transparent**| **off**}
6. **vtp file** *file-name*
7. **vtp password** *password-value*
8. **exit**
9. （任意） **show vtp status**
10. （任意） **show vtp counters**
11. （任意） **show vtp interface**
12. （任意） **show vtp password**
13. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**feature vtp**
	
	例：
	`switch(config)# feature vtp`
	`switch(config)#`
		デバイスの VTP をイネーブルにします。 デフォルトはディセーブルです。

ステップ 3	**vtp domain** *domain-name* 例： `switch(config)# vtp domain accounting`	このデバイスを参加させる VTP ドメインの名前を指定します。 デフォルトは空白です。
ステップ 4	**vtp version** {**1** | **2**} 例： `switch(config)# vtp version 2`	使用する VTP バージョンを設定します。 デフォルトはバージョン 1 です。
ステップ 5	**vtp mode** {**client** | **server**| **transparent**| **off**} 例： `switch(config)# vtp mode transparent`	VTPモードをクライアント、サーバ、トランスペアレント、またはオフに設定します。
ステップ 6	**vtp file** *file-name* 例： `switch(config)# vtp file vtp.dat`	VTPコンフィギュレーションを保存するIFSファイルシステムのファイルの ASCII ファイル名を指定します。
ステップ 7	**vtp password** *password-value* 例： `switch(config)# vtp password cisco`	VTP 管理ドメインのパスワードを指定します。

ステップ 8	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション サブモードを終了します。

ステップ 9	**show vtp status** 例： `switch# show vtp status`	（任意） バージョン、モードおよびリビジョン番号などのデバイスの VTP 設定に関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 10	**show vtp counters** 例： `switch# show vtp counters`	（任意） デバイスの VTP アドバタイズメントの統計に関する情報を表示します。
ステップ 11	**show vtp interface** 例： `switch# show vtp interface`	（任意） VTP-enabledインターフェイスのリストを表示します。
ステップ 12	**show vtp password** 例： `switch# show vtp password`	（任意） 管理 VTP ドメインのパスワードを表示します。
ステップ 13	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、デバイスでトランスペアレント モードの VTP を設定する例を示します。

```
switch# config t
switch(config)# feature vtp
switch(config)# vtp domain accounting
switch(config)# vtp version 2
switch(config)# vtp mode transparent
switch(config)# exit
switch#
```

VTP プルーニングの設定

Cisco NX-OS デバイスに VTP プルーニングを設定できます。

はじめる前に

デバイス上で VTP をイネーブルにする必要があります。

手順の概要

1. **config t**
2. **vtp pruning**
3. （任意） **no vtp pruning**
4. （任意） **show interface** *interface-identifier* **switchport**
5. **switchport trunk pruning vlan** [**add** | **remove** | **except** | **none** |**all**] *VLAN-IDs*
6. （任意） **show vtp counters**
7. （任意） **clear vtp counters**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**vtp pruning**
	
	例：
	`switch(config)# vtp pruning`
	`switch(config)#`
		デバイス上でVTPプルーニングをイネーブルにします。 デフォルトはディセーブルです。

ステップ 3	**no vtp pruning**
	
	例：
	`switch(config)# no vtp pruning`
	`switch(config)#`
		（任意）
		デバイス上でVTPプルーニングをディセーブルにします。 デフォルトはディセーブルです。

ステップ 4	**show interface** *interface-identifier* **switchport**
	
	例：
	`switch(config)# show interface Ethernet 1/4 switchport`
	`switch(config)#`
		（任意）
		トランク ポートの VTP プルーニングの適格性を表示します。 デフォルトでは、2～1001 のすべての VLAN がプルーニング適格です。

ステップ 5	**switchport trunk pruning vlan** [**add**	**remove**	**except**	**none** |**all**] *VLAN-IDs* 例： `switch(config)# switchport trunk pruning vlan add 20-25`	特定の VLAN を VTP プルーニング適格に設定します。
ステップ 6	**show vtp counters** 例： `switch# show vtp counters`	（任意） VTP プルーニング情報およびカウンタを表示します。

	コマンドまたはアクション	目的
ステップ 7	**clear vtp counters** 例： `switch# clear vtp counters`	（任意） すべての VTP プルーニング カウンタ値をリセットします。

次に、VLAN 9 ～ 54 をプルーニング適格に設定する方法と、VTP 2 ～ 8 および 55 ～ 1001 をプルーニング非適格に設定する方法の例を示します。

```
switch(config-if)# switchport trunk pruning vlan 9-54
```

VLAN 1 は、工場出荷時のデフォルトの VLAN であるため、プルーニング非適格です。 VLAN 1002～1005 は、トークン リング ネットワーク用に予約されています。 VLAN 1006 以上は、プルーニング適格にするために、VTP バージョン 3 が必要です。

第 6 章

NX-OSを使用したプライベートVLANの設定

この章では、Cisco NX-OS デバイスでプライベート 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。

この章は、次の内容で構成されています。

- Information About Private VLANs, 57 ページ
- Licensing Requirements for Private VLANs, 64 ページ
- Prerequisites for Private VLANs, 65 ページ
- Guidelines and Limitations for Configuring Private VLANs, 65 ページ
- プライベート VLAN のデフォルト設定, 68 ページ
- Configuring a Private VLAN, 69 ページ
- プライベート VLAN 設定の確認, 89 ページ
- プライベート VLAN の統計情報の表示とクリア, 90 ページ
- プライベート VLAN の設定例, 90 ページ
- プライベート VLAN の追加情報（CLI バージョン）, 91 ページ
- プライベート VLAN 設定の機能履歴（CLI バージョン）, 92 ページ

Information About Private VLANs

（注） A Layer 2 port can function as either a trunk port, an access port, or a private VLAN port.

（注） Beginning with Cisco NX-OS Release 5.0(2), the system supports private VLAN promiscuous trunk ports and isolated trunk ports. Private VLAN community ports cannot be trunk ports.

（注） You must enable the private VLAN feature before you can configure this feature.

In certain instances where similar systems do not need to interact directly, private VLANs provide additional protection at the Layer 2 level. Private VLANs are an association of primary and secondary VLANs.

A primary VLAN defines the broadcast domain with which the secondary VLANs are associated. The secondary VLANs may either be isolated VLANs or community VLANs. Hosts on isolated VLANs communicate only with associated promiscuous ports in primary VLANs, and hosts on community VLANs communicate only among themselves and with associated promiscuous ports but not with isolated ports or ports in other community VLANs.

In configurations that use integrated switching and routing functions, you can assign a single Layer 3 VLAN network interface to each private VLAN to provide routing. The VLAN network interface is created for the primary VLAN. In such configurations, all secondary VLANs communicate at Layer 3 only through a mapping with the VLAN network interface on the primary VLAN. Any VLAN network interfaces previously created on the secondary VLANs are put out-of-service.

プライベート VLAN の概要

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

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

（注） 特定の VLAN をプライマリまたはセカンダリのどちらかのプライベート VLAN として設定するには、事前に VLAN を作成しておく必要があります。

Primary and Secondary VLANs in Private VLANs

The private VLAN feature addresses two problems that users encounter when using VLANs:

- Each VDC supports up to 4096 VLANs. If a user assigns one VLAN per customer, the number of customers that the service provider can support is limited.
- To enable IP routing, each VLAN is assigned with a subnet address space or a block of addresses, which can result in wasting the unused IP addresses and creating IP address management problems.

Using private VLANs solves the scalability problem and provides IP address management benefits and Layer 2 security for customers.

The private VLAN feature allows you to partition the Layer 2 broadcast domain of a VLAN into subdomains. A subdomain is represented by a pair of private VLANs: a primary VLAN and a secondary VLAN. A private VLAN domain can have multiple private VLAN pairs, one pair for each subdomain. All VLAN pairs in a private VLAN domain share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another.

（注） A private VLAN domain has only one primary VLAN.

Secondary VLANs provide Layer 2 isolation between ports within the same private VLAN. The following two types are secondary VLANs within a primary VLAN:

- Isolated VLANs—Ports within an isolated VLAN cannot communicate with each other at the Layer 2 level.
- Community VLANs—Ports within a community VLAN can communicate with each other but cannot communicate with ports in other community VLANs or in any isolated VLANs at the Layer 2 level.

Private VLAN Ports

（注） Both community and isolated private VLAN ports are labeled as PVLAN host ports. A PVLAN host port is either a community PVLAN port or an isolated PVLAN port depending on the type of secondary VLAN with which it is associated.

The types of private VLAN ports are as follows:

- Promiscuous port—A promiscuous port belongs to the primary VLAN. The promiscuous port can communicate with all interfaces, including the community and isolated host ports, that belong to those secondary VLANs associated to the promiscuous port and associated with the primary VLAN. You can have several promiscuous ports in a primary VLAN. Each promiscuous port can have several secondary VLANs, or no secondary VLANs, associated to that port. You can associate a secondary VLAN to more than one promiscuous port, as long as the promiscuous port and secondary VLANs are within the same primary VLAN. You may want to do this association for load balancing or redundancy purposes. You can also have secondary VLANs that are not associated to any promiscuous port, but these secondary VLANs cannot communicate to the Layer 3 interface.

  Beginning with Cisco NX-OS Release 5.0(2), the primary VLAN becomes inactive after you remove all the mapped secondary VLANs to that primary VLAN.

- Promiscuous trunk—Beginning with Cisco NX-OS Release 5.0(2) and Cisco DCNM Release 5.1(1), on the Cisco Nexus 7000 Series devices, you can configure a promiscuous trunk port to carry traffic for multiple primary VLANs. You map the private VLAN primary VLAN and either all or selected associated VLANs to the promiscuous trunk port. Each primary VLAN and one associated and secondary VLAN is a private VLAN pair, and you can configure a maximum of 16 private VLAN pairs on each promiscuous trunk port.

  （注） Private VLAN promiscuous trunk ports carry traffic for normal VLANs as well as for primary private VLANs.

- Isolated port—An isolated port is a host port that belongs to an isolated secondary VLAN. This port has complete Layer 2 isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports. Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous

ports. You can have more than one isolated port in a specified isolated VLAN, and each port is completely isolated from all other ports in the isolated VLAN.

- Isolated or secondary trunk—Beginning with Cisco NX-OS Release 5.0(2) and Cisco DCNM Release 5.1(1) on the Cisco Nexus 7000 Series devices, you can configure an isolated trunk port to carry traffic for multiple isolated VLANs. Each secondary VLAN on an isolated trunk port must be associated with a different primary VLAN. You cannot put two secondary VLANs that are associated with the same primary VLAN on an isolated trunk port. Each primary VLAN and one associated secondary VLAN is a private VLAN pair, and you can configure a maximum of 16 private VLAN pairs on each isolated trunk port.

（注） Private VLAN isolated trunk ports carry traffic for normal VLANs as well as for secondary private VLANs.

- Community port—A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with associated promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities and from all isolated ports within the private VLAN domain.

（注） Because trunks can support the VLANs that carry traffic between promiscuous, isolated, and community ports, the isolated and community port traffic might enter or leave the device through a trunk interface.

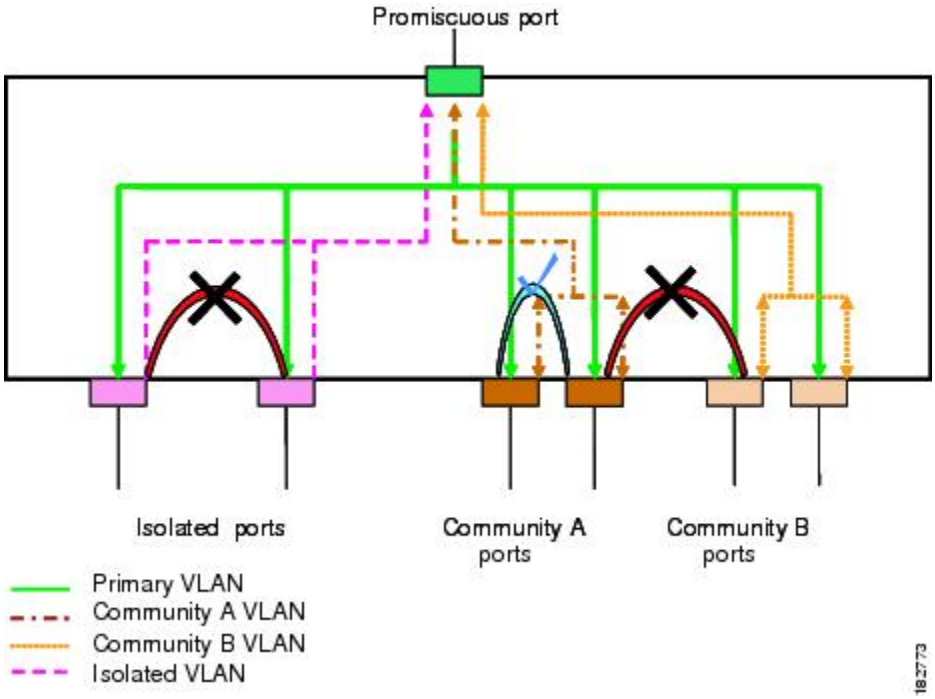
Primary, Isolated, and Community Private VLANs

Because the primary VLAN has the Layer 3 gateway, you associate secondary VLANs with the primary VLAN in order to communicate outside the private VLAN. Primary VLANs and the two types of secondary VLANs, isolated VLANs and community VLANs, have these characteristics:

- Primary VLAN— The primary VLAN carries traffic from the promiscuous ports to the (isolated and community) host ports and to other promiscuous ports.
- Isolated VLAN —An isolated VLAN is a secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports and the Layer 3 gateway. You can configure multiple isolated VLANs in a private VLAN domain, and all the traffic remains isolated within each one. In addition, each isolated VLAN can have several isolated ports, and the traffic from each isolated port also remains completely separate.
- Community VLAN—A community VLAN is a secondary VLAN that carries upstream traffic from the community ports to the promiscuous port gateways and to other host ports in the same community. You can configure multiple community VLANs in a private VLAN domain. The ports within one community can communicate, but these ports cannot communicate with ports in any other community or isolated VLAN in the private VLAN.

This figure shows the Layer 2 traffic flows within a primary, or private VLAN, along with the types of VLANs and types of ports.

図 *3* : ***Private VLAN Layer 2 Traffic Flows***



（注） The private VLAN traffic flows are unidirectional from the host ports to the promiscuous ports. Traffic that egresses the promiscuous port acts like the traffic in a normal VLAN, and there is no traffic separation among the associated secondary VLAN.

A promiscuous port can serve only one primary VLAN, but it can serve multiple isolated VLANs and multiple community VLANs. (Layer 3 gateways are connected to the device through a promiscuous port.) With a promiscuous port, you can connect a wide range of devices as access points to a private VLAN. For example, you can use a promiscuous port to monitor or back up all the private VLAN servers from an administration workstation.

（注） Beginning with Cisco NX-OS Release 5.0(2) for the Nexus 7000 Series devices, you can configure private VLAN promiscuous and isolated trunk ports. These promiscuous and isolated trunk ports carry traffic for multiple primary and secondary VLANs as well as normal VLAN.

Although you can have several promiscuous ports in a primary VLAN, you can have only one Layer 3 gateway per primary VLAN.

In a switched environment, you can assign an individual private VLAN and associated IP subnet to each individual or common group of end stations. The end stations need to communicate only with a default gateway to communicate outside the private VLAN.

（注） You must enable the VLAN interface feature before you can configure the Layer 3 gateway. See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』 for complete information on VLAN network interfaces and IP addressing.

プライマリ VLAN とセカンダリ VLAN のアソシエーション

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。 関連付け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 のみにアソシエートすることができます。

アソシエーションの操作を可能にするには、次の条件を満たす必要があります。

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

（注） アソシエーションが動作していることを確認するには、**show** コマンドの出力を調べます。 関連付けが動作していなくても、エラー メッセージは発行されません

プライマリ VLAN またはセカンダリ VLAN を削除すると、その VLAN に関連付けされたポートは非アクティブになります。 指定の VLAN をプライベート VLAN モードに再変換すると、元の関連付けが回復します。

関連付けがプライベート VLAN トランク ポートで動作していない場合、ポート全体はダウンせずに、その VLAN だけがダウンします。

no private-vlan コマンドを入力すると、VLAN は通常の VLAN モードに戻ります。 その VLAN 上の関連付けはすべて一時停止されますが、インターフェイスはプライベート VLAN モードのままになります。

プライマリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN に関連付けられたすべてのプライベート VLAN は失われます。 ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力した場合、その VLAN とプライベート VLAN のアソシエーションは一時停止します。この VLAN を再作成して以前のセカンダリ VLAN として設定すると元に戻ります。

（注） この動作は、Catalyst デバイスの動作と異なります。

セカンダリ VLAN とプライマリ VLAN の関連付けを変更するには、現在の関連付けを削除してから目的の関連付けを追加します。

Broadcast Traffic in Private VLANs

Broadcast traffic from ports in a private VLAN flows in the following ways:

- The broadcast traffic flows from all promiscuous ports to all ports in the primary VLAN. This broadcast traffic is distributed to all ports within the primary VLAN, including those ports that are not configured with private VLAN parameters.
- The broadcast traffic from all isolated ports is distributed only to those promiscuous ports in the primary VLAN that are associated to that isolated port.
- The broadcast traffic from community ports is distributed to all ports within the port's community and to all promiscuous ports that are associated to the community port. The broadcast packets are not distributed to any other communities within the primary VLAN or to any isolated ports.

Private VLAN Port Isolation

You can use private VLANs to control access to end stations as follows:

- Configure selected interfaces connected to end stations as isolated ports to prevent any communication at Layer 2. For example, if the end stations are servers, this configuration prevents Layer 2 communication between the servers.
- Configure interfaces connected to default gateways and selected end stations (for example, backup servers) as promiscuous ports to allow all end stations access to a default gateway.

Private VLANs and VLAN Interfaces

A VLAN interface to a Layer 2 VLAN is also called a switched virtual interface (SVI). Layer 3 devices communicate with a private VLAN only through the primary VLAN and not through secondary VLANs.

Configure VLAN network interfaces only for primary VLANs. Do not configure VLAN interfaces for secondary VLANs. VLAN network interfaces for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN. You will see the following actions if you misconfigure the VLAN interfaces:

- If you try to configure a VLAN with an active VLAN network interface as a secondary VLAN, the configuration is not allowed until you disable the VLAN interface.
- If you try to create and enable a VLAN network interface on a VLAN that is configured as a secondary VLAN, that VLAN interface remains disabled and the system returns an error.

When the primary VLAN is associated with and mapped to the secondary VLAN, any configuration on the primary VLAN is propagated to the secondary VLANs. For example, if you assign an IP subnet to the VLAN network interface on the primary VLAN, this subnet is the IP subnet address of the entire private VLAN.

（注） You must enable the VLAN interface feature before you configure VLAN interfaces. See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』, for information on VLAN interfaces and IP addressing.

Private VLANs Across Multiple Devices

You can extend private VLANs across multiple devices by trunking the primary, isolated, and community VLANs to other devices that support private VLANs. To maintain the security of your private VLAN configuration and to avoid other uses of the VLANs configured to be private VLANs, configure private VLANs on all intermediate devices, including devices that have no private VLAN ports.

High Availability for Private VLANs

The software supports high availability for both stateful and stateless restarts, as during a cold reboot, for private VLANs. For the stateful restarts, the software supports a maximum of three retries. If you try more than 3 times within 10 seconds of a restart, the software reloads the supervisor module.

You can upgrade or downgrade the software seamlessly, with respect to private VLANs.

Beginning with Cisco NX-OS Release 5.0(2), if you configure private VLAN promiscuous or isolated trunk ports, you must unconfigure those ports in order to downgrade the software.

（注） See the 『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』, for complete information on high-availability features.

Virtualization Support for Private VLANs

The software supports virtual device contexts (VDCs).

（注） See the 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』, for complete information on VDCs and assigning resources.

Each VLAN must have all of its private VLAN ports for both the primary VLAN and all secondary VLANs in the same VDC. Private VLANs cannot cross VDCs.

Licensing Requirements for Private VLANs

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	Private VLANs require no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the 『*Cisco NX-OS Licensing Guide*』.

However, using VDCs requires an Advanced Services license.

Prerequisites for Private VLANs

Private VLANs have the following prerequisites:

- You must be logged onto the device.
- If necessary, install the Advanced Services license and enter the desired VDC.
- You must enable the private VLAN feature.

Guidelines and Limitations for Configuring Private VLANs

Private VLANs have the following configuration guidelines and limitations:

- You must enable private VLANs before the device can apply the private VLAN functionality.
- You must enable the VLAN interface feature before the device can apply this functionality.
- Shut down the VLAN network interface for all VLANs that you plan to configure as secondary VLANs before you configure these VLANs.
- You cannot configure a shared interface to be part of a private VLAN. For more details, see the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』.

Secondary and Primary VLAN Configuration

Follow these guidelines when configuring secondary or primary VLANs in private VLANs:

- You cannot configure the default VLAN (VLAN1) or any of the internally allocated VLANs as primary or secondary VLANs.
- You must use VLAN configuration (config-vlan) mode to configure private VLANs.
- A primary VLAN can have multiple isolated and community VLANs associated with it. An isolated or community VLAN can be associated with only one primary VLAN.
- Although private VLANs provide host isolation at Layer 2, hosts can communicate with each other at Layer 3.

- When a secondary VLAN is associated with the primary VLAN, the STP parameters of the primary VLAN, such as bridge priorities, are propagated to the secondary VLAN. However, STP parameters do not necessarily propagate to other devices. You should manually check the STP configuration to ensure that the spanning tree topologies for the primary, isolated, and community VLANs match exactly so that the VLANs can properly share the same forwarding database.
- For normal trunk ports, note the following:
  - There is a separate instance of STP for each VLAN in the private VLAN.
  - STP parameters for the primary and all secondary VLANs must match.
  - The primary and all associated secondary VLANs should be in the same MST instance.
- For nontrunking ports, note the following:
  - STP is aware only of the primary VLAN for any private VLAN host port; STP does not run on secondary VLANs on a host port.

（注） We recommend that you enable BPDU Guard on all ports that you configure as a host port; do not enable this feature on promiscuous ports.

- For private VLAN promiscuous trunk ports, note the following:
  - You can configure a maximum of 16 private VLAN primary and secondary VLAN pairs on each promiscuous trunk port.
  - The native VLAN must be either a normal VLAN or a private VLAN primary VLAN. You cannot configure a private VLAN secondary VLAN as the native VLAN for a private VLAN promiscuous trunk port.
  - To downgrade a system that has private VLAN promiscuous trunk ports configured, you must unconfigure these ports.
- For private VLAN isolated trunk ports, note the following:
  - You can configure a maximum of 16 private VLAN primary and secondary VLAN pairs on each isolated trunk port.
  - The native VLAN must be either a normal VLAN or a private VLAN secondary VLAN. You cannot configure a private VLAN primary port as the native VLAN for a private VLAN isolated trunk port.
  - To downgrade a system that has private VLAN isolated trunk ports configured, you must unconfigure these ports.
- You can apply different Quality of Service (QoS) configurations to primary, isolated, and community VLANs.
- To apply a VACL to all private VLAN traffic, map the secondary VLANs on the VLAN network interface of the primary VLAN, and then configure the VACLs on the VLAN network interface of the primary VLAN.

- The VACLs that you apply to the VLAN network interface of a primary VLAN automatically apply to the associated isolated and community VLANs only after you have configured the mapping.
- If you do not map the secondary VLAN to the VLAN network interface of the primary VLAN, you can have different VACLs for primary and secondary VLANs, which can cause problems.
- Because traffic in a private VLAN flows in different directions in different VLANs, you can have different VACLs for ingressing traffic and different VACLs for egressing traffic prior to configuring the mapping.

（注） You must keep the same VACLs for the primary VLAN and all secondary VLANs in the private VLAN.

- You can enable DHCP snooping on private VLANs. When you enable DHCP snooping on the primary VLAN, the DHCP configuration is propagated to the secondary VLANs. If you configure DHCP on a secondary VLAN, the configuration does not take effect if the primary VLAN is already configured.
- Before you configure a VLAN as a secondary VLAN, you must shut down the VLAN network interface for the secondary VLAN.
- To prevent interhost communication in isolated private VLANs with a promiscuous port, configure a role-based ACL (RBACL) that disallows hosts in that subnet from communicating with each other.

Private VLAN Port Configuration

Follow these guidelines when configuring private VLAN ports:

- Use only the private VLAN configuration commands to assign ports to primary, isolated, or community VLANs.
- The Layer 2 access ports that are assigned to the VLANs that you configure as primary, isolated, or community VLANs are inactive while the VLAN is part of the private VLAN configuration. Layer 2 trunk interfaces, which may carry private VLANs, are active and remain part of the STP database.
- Do not configure ports that belong to a port-channel group as private VLAN ports. While a port is part of the private VLAN configuration, any port-channel configuration for it is inactive.
- If you delete a VLAN used in the private VLAN configuration, the private VLAN ports that are associated with the VLAN become inactive.

Limitations with Other Features

Consider these configuration limitations with other features when configuring private VLANs:

（注） In some cases, the configuration is accepted with no error messages, but the commands have no effect.

- IGMP runs only on the primary VLAN and uses the configuration of the primary VLAN for all secondary VLANs.

- Any IGMP join request in the secondary VLAN is treated as if it is received in the primary VLAN.
- Private VLANs support these Switched Port Analyzer (SPAN) features:
  - You can configure a private VLAN port as a SPAN source port.
  - You can use VLAN-based SPAN (VSPAN) on primary, isolated, and community VLANs or use SPAN on only one VLAN to separately monitor egress or ingress traffic.
- Private VLAN host or promiscuous ports cannot be a SPAN destination port.
- A destination SPAN port cannot be an isolated port. (However, a source SPAN port can be an isolated port.)
- You can configure SPAN to span both primary and secondary VLANs or to span either one if the user is interested only in ingress or egress traffic.
- After you configure the association between the primary and secondary VLANs, the dynamic MAC addresses that learned the secondary VLANs are flushed.
- After you configure the association between the primary and secondary VLANs, all static MAC addresses that were created on the secondary VLANs are inserted into the primary VLAN. If you delete the association, the static MAC addresses revert to the secondary VLANs only.
- After you configure the association between the primary and secondary VLANs, you cannot create static MAC addresses for the secondary VLANs.
- After you configure the association between the primary and secondary VLANs, if you delete the association, all static MAC addresses that were created on the primary VLANs remain on the primary VLAN only.
- Port security features are not supported with private VLANs.
- In private VLANs, STP controls only the primary VLAN.

（注） See the 『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x*』 for information on configuring static MAC addresses.

プライベート VLAN のデフォルト設定

次の表に、プライベート VLAN のデフォルト設定を示します。

表 *9*：プライベート *VLAN* のデフォルト設定

パラメータ	デフォルト
プライベート VLAN	ディセーブル

Configuring a Private VLAN

You must have already created the VLAN before you can assign the specified VLAN as a private VLAN.

See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』, for information on assigning IP addresses to VLAN interfaces.

（注） If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

プライベート VLAN のイネーブル化（CLI バージョン）

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**feature private-vlan**
	
	例：
	`switch(config)# feature private-vlan`
	`switch(config)#`
		デバイス上でプライベート VLAN 機能をイネーブルにします。
		（注） プライベート VLAN モードのデバイスに動作可能なポートがある場合、**no feature private-vlan** コマンドを適用できません。

	コマンドまたはアクション	目的

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

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

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

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

プライベート VLAN としての VLAN の設定（CLI バージョン）

（注） VLAN をセカンダリ VLAN（つまり、コミュニティ VLAN または独立 VLAN のいずれか）として設定する前に、まず 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。

VLAN は、プライベート VLAN として設定できます。

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

プライベート VLAN 内で、プライマリ VLAN、コミュニティ VLAN、または独立 VLAN として使用するすべての VLAN を作成します。 そのあとで、複数の独立 VLAN および複数のコミュニティ VLAN を 1 つのプライマリ VLAN に関連付けます。 複数のプライマリ VLAN と関連付けを設定できます。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 を削除すると、その VLAN に関連付けされたポートは非アクティブになります。

プライベート VLAN トラック ポート上でセカンダリ VLAN またはプライマリ VLAN のいずれかを削除した場合、その特定の VLAN だけが非アクティブになり、トランク ポートはアップしたままです。

はじめる前に

プライベート VLAN 機能がイネーブルであることを確認してください。

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

手順の概要

1. **config t**
2. **vlan** {*vlan-id* | *vlan-range*}
3. 次のいずれかのコマンドを入力します。
4. **exit**
5. （任意） **show vlan private-vlan** [*type*]
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**vlan** {*vlan-id*	*vlan-range*}
		
		例：
		`switch(config)# vlan 5`
		`switch(config-vlan)#`
			VLAN 設定サブモードにします。

ステップ 3	次のいずれかのコマンドを入力します。	

オプション	説明
private-vlan {**community** | **isolated** | **primary**}	VLAN を、コミュニティ VLAN、独立 VLAN、またはプライマリ プライベート VLAN として設定します。 プライベート VLAN には、1 つのプライマリ VLAN を設定する必要があります。 複数のコミュニティ VLAN と独立 VLAN を設定することができます。
no private-vlan {**community** | **isolated** | **primary**}	指定した VLAN からプライベート VLAN の設定を削除し、通常の VLAN モードに戻します。 プライマリ VLAN またはセカンダリ VLAN を削除すると、その VLAN に関連付けされたポートは非アクティブになります。

	コマンドまたはアクション	目的
	例： `switch(config-vlan)# private-vlan primary`	

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

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

次の例は、VLAN 5 をプライマリ VLAN としてプライベート VLAN に割り当てる方法を示しています。

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

セカンダリ VLAN とプライマリ プライベート VLAN の関連付け（CLI バージョン）

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

- *secondary-vlan-list* パラメータには、スペースを含めないでください。 カンマで区切った複数の項目を含めることができます。 各項目は、単一のセカンダリ VLAN ID、またはセカンダリ VLAN ID をハイフンでつないだ範囲にできます。
- *secondary-vlan-list* パラメータには、複数のコミュニティ VLAN ID と独立 VLAN ID を含めることができます。
- セカンダリ VLAN をプライマリ VLAN にアソシエートするには、*secondary-vlan-list* と入力するか、*secondary-vlan-list* に **add** キーワードを入力します。
- セカンダリ VLAN とプライマリ VLAN とのアソシエーションをクリアするには、*secondary-vlan-list* に **remove** キーワードを入力します。

- セカンダリ VLAN とプライマリ VLAN とのアソシエーションを変更するには、既存のアソシエーションを削除し、次に必要なアソシエーションを追加します。

プライマリ VLAN またはセカンダリ VLAN を削除すると、その VLAN に関連付けされたポートは非アクティブになります。

no private-vlan コマンドを入力すると、VLAN は通常の VLAN モードに戻ります。 その VLAN 上の関連付けはすべて一時停止されますが、インターフェイスはプライベート VLAN モードのままになります。

指定の VLAN をプライベート VLAN モードに再変換すると、元の関連付けが回復します。

プライマリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN に関連付けされたすべてのプライベート VLAN は失われます。 ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力した場合、その VLAN とプライベート VLAN の関連付けは一時停止します。この VLAN を再作成して以前のセカンダリ VLAN として設定すると元に戻ります。

はじめる前に

プライベート VLAN 機能がイネーブルであることを確認してください。

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

手順の概要

1. **config t**
2. **vlan** *primary-vlan-id*
3. 次のいずれかのコマンドを入力します。
4. **exit**
5. （任意） **show vlan private-vlan** [**type**]
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**vlan** *primary-vlan-id*
	
	例：
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		プライベート VLAN の設定作業を行うプライマリ VLAN の番号を入力します。

ステップ 3	次のいずれかのコマンドを入力します。	

	コマンドまたはアクション	目的
	オプション / **説明** **private-vlan association** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*} — セカンダリ VLAN をプライマリ VLANに関連付けます。 **no private-vlan association** — プライマリ VLAN からすべてのアソシエーションを削除し、通常の VLAN モードに戻します。 例： `switch(config-vlan)# private-vlan association 100-105,109`	

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

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

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

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

プライマリ VLAN の VLAN インターフェイスへのセカンダリ VLAN のマッピング（CLI バージョン）

（注） プライベート VLAN 内のプライマリ VLAN の VLAN インターフェイスへの IP アドレスの割り当てについては、『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』を参照してください。

セカンダリ VLAN を、プライマリ VLAN の VLAN インターフェイスにマッピングします。 独立 VLAN およびコミュニティ VLAN は、ともにセカンダリ VLAN と呼ばれます。 プライベート 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 ネットワーク 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。

はじめる前に

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

手順の概要

1. **config t**
2. **interface vlan** *primary-vlan-ID*
3. 次のいずれかのコマンドを入力します。
4. **exit**
5. （任意） **show interface vlan** *primary-vlan-id* **private-vlan mapping**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface vlan** *primary-vlan-ID*
	
	例：
	`switch(config)# interface vlan 5`
	`switch(config-if)#`
		プライベート VLAN の設定作業を行うプライマリ VLAN の番号を入力します。 プライマリ VLAN のインターフェイス コンフィギュレーション モードが開始されます。

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

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

ステップ 5	**show interface vlan** *primary-vlan-id* **private-vlan mapping** 例： `switch(config)# show interface vlan 101 private-vlan mapping`	（任意） インターフェイスのプライベート VLAN 情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

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

レイヤ 2 インターフェイスをプライベート VLAN のホスト ポートとして設定できます。 プライベート VLAN では、ホスト ポートがセカンダリ VLAN の一部です。セカンダリ VLAN は、コミュニティ VLAN または独立 VLAN のいずれかです。

（注） ホスト ポートとして設定されているすべてのインターフェイスで、BPDU ガードをイネーブルにすることを推奨します。

次に、ホスト ポートを、プライマリ VLAN とセカンダリ VLAN の両方にアソシエートします。

はじめる前に

プライベート VLAN 機能がイネーブルであることを確認してください。

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

手順の概要

1. **config t**
2. **interface** *type slot/port*
3. **switchport mode private-vlan host**
4. 次のいずれかのコマンドを入力します。
5. **exit**
6. （任意） **show interface switchport**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

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

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

ステップ 4	次のいずれかのコマンドを入力します。	

オプション	説明
switchport private-vlan host-association {*primary-vlan-id*} {*secondary-vlan-id*}	レイヤ 2 ホスト ポートを、プライベート VLAN のプライマリ VLAN およびセカンダリ VLAN に関連付けます。 セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかとして設定できます。
no switchport private-vlan host-association	プライベート VLAN のアソシエーションをポートから削除します。

	コマンドまたはアクション	目的
	例： `switch(config-if)# switchport private-vlan host-association 10 50`	

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

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

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

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

プライベートVLAN独立トランクポートとしてのレイヤ2インターフェイスの設定

Cisco NX-OS Release 5.0(2) から、レイヤ 2 インターフェイスをプライベート VLAN 独立トランク ポートとして設定できるようになりました。これらの独立トランク ポートは、複数のセカンダリ VLAN と通常の VLAN のトラフィックを伝送します。

（注） プライマリ VLAN とセカンダリ VLAN は、プライベート VLAN 独立トランク ポート上で動作可能になる前に関連付ける必要があります。

はじめる前に

プライベート VLAN 機能がイネーブルであることを確認してください。

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

手順の概要

1. **config t**
2. **interface** {*type slot/port*}
3. **switchport**
4. **switchport mode private-vlan trunk secondary**
5. （任意） **switchport private-vlan trunk native vlan** *vlan-id*
6. **switchport private-vlan trunk allowed vlan** {**add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*}
7. 次のいずれかのコマンドを入力します。
8. **exit**
9. （任意） **show interface switchport**
10. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** {*type slot/port*}
	
	例：
	`switch(config)# interface ethernet 2/11`
	`switch(config-if)#`
		プライベート VLAN 独立トランク ポートとして設定するレイヤ 2 ポートを選択します。

ステップ 3	**switchport**
	
	例：
	`switch(config-if)# switchport`
	`switch(config-if)#`
		レイヤ 2 ポートをスイッチ ポートとして設定します。

ステップ 4	**switchport mode private-vlan trunk secondary**
	
	例：
	`switch(config-if)# switchport mode private-vlan trunk secondary`
	`switch(config-if)#`
		レイヤ2ポートを、複数の独立VLANのトラフィックを伝送する独立トランク ポートとして設定します。
		（注） コミュニティ VLAN は独立トランク ポートにはできません。

	コマンドまたはアクション	目的
ステップ 5	**switchport private-vlan trunk native vlan** *vlan-id* 例： `switch(config-if)# switchport private-vlan trunk native vlan 5`	（任意） 802.1Q トランクのネイティブ VLAN を設定します。有効値の範囲は 1 ～ 3968 および 4048 ～ 4093 です。デフォルト値は 1 です。 （注） プライベート VLAN を独立トランク ポートのネイティブ VLAN として使用している場合は、セカンダリ VLAN または標準 VLAN の値を入力する必要があります。プライマリ VLAN をネイティブ VLAN として設定することはできません。

ステップ 6	**switchport private-vlan trunk allowed vlan** {**add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*}
	
	例：
	`switch(config-if)# switchport private-vlan trunk allowed vlan add 1`
	`switch(config-if)#`
		プライベート VLAN 独立トランク インターフェイスの許容 VLAN を設定します。 有効値の範囲は 1 ～ 3968 および 4048 ～ 4093 です。
		プライベート プライマリ VLAN およびセカンダリ VLAN を独立トランク ポートにマッピングすると、すべてのプライマリ VLAN がこのポートの許可される VLAN リストに自動的に追加されます。
		（注） ネイティブ VLAN が許可される VLAN リストに含まれていることを確認します。このコマンドでは、デフォルトでこのインターフェイス上の VLAN が許可されないため、ネイティブ VLAN トラフィックを通過させるには、ネイティブ VLAN を許可される VLAN として設定する必要があります（関連する VLAN として追加済みでない場合）。

ステップ 7	次のいずれかのコマンドを入力します。	

	コマンドまたはアクション	目的

オプション	説明
switchport private-vlan association trunk {*primary-vlan-id*} {*secondary-vlan-id*}	レイヤ 2 独立トランク ポートを、プライベート VLAN のプライマリ VLAN およびセカンダリ VLAN に関連付けます。セカンダリ VLAN は独立 VLAN である必要があります。 各独立トランク ポートに対し、最大 16 個のプライベート VLAN のプライマリとセカンダリのペアを関連付けられます。 作業中のプライマリ VLAN とセカンダリ VLAN のペアごとに、コマンドを再入力する必要があります。 （注） 独立トランク ポートの各セカンダリ VLAN は、別々のプライマリ VLAN に関連付ける必要があります。 同じプライマリ VLAN に関連付けられた 2 つの独立 VLAN を、プライベート VLAN 独立トランク ポートに接続することはできません。 これを行った場合、最新のエントリが前のエントリを上書きします。
no switchport private-vlan association trunk [*primary-vlan-id* [*secondary-vlan-id*]]	プライベート VLAN 独立トランク ポートからプライベート VLAN の関連付けを削除します。

例：

```
switch(config-if)# switchport private-vlan
association trunk 10 101
switch(config-if)#
```

	コマンドまたはアクション	目的

ステップ 8	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 9	**show interface switchport** 例： `switch# show interface switchport`	（任意） スイッチポートとして設定されているすべてのインターフェイスに関する情報を表示します。
ステップ 10	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、レイヤ 2 ポート 2/1 を、3 つの異なるプライマリ VLAN と関連セカンダリ VLAN に関連付けられたプライベート VLAN 独立トランク ポートとして設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode private-vlan trunk
switch(config-if)# switchport private-vlan trunk allowed vlan add 1
switch(config-if)# switchport private-vlan association trunk 10 101
switch(config-if)# switchport private-vlan association trunk 20 201
switch(config-if)# switchport private-vlan association trunk 30 102
switch(config-if)# exit
switch(config)#
```

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

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

はじめる前に

プライベート VLAN 機能がイネーブルであることを確認してください。

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

手順の概要

1. **config t**
2. **interface** {*type slot/port*}
3. **switchport mode private-vlan promiscuous**
4. 次のいずれかのコマンドを入力します。
5. **exit**
6. （任意） **show interface switchport**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

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

ステップ 3	**switchport mode private-vlan promiscuous** 例： `switch(config-if)# switchport mode private-vlan promiscuous`	レイヤ 2 ポートをプライベート VLAN の無差別ポートとして設定します。
ステップ 4	次のいずれかのコマンドを入力します。	

オプション	説明
switchport private-vlan mapping {*primary-vlan-id*} {*secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list*}	レイヤ 2 ポートを無差別ポートとして設定し、このポートをプライマリ VLAN および選択したセカンダリ VLAN のリストに関連付けます。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかとして設定できます。
no switchport private-vlan mapping	プライベート VLAN から、マッピングをクリアします。

	コマンドまたはアクション	目的
	例： `switch(config-if)# switchport private-vlan mapping 10 50`	

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

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

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

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

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

Cisco NX-OS Release 5.0(2) から、レイヤ 2 インターフェイスをプライベート VLAN 無差別トランク ポートとして設定し、その無差別トランク ポートを複数のプライマリ VLAN に関連付けることができるようになりました。 これらの無差別トランク ポートは、複数のプライマリ VLAN と通常の VLAN のトラフィックを伝送します。

（注） プライマリ VLAN とセカンダリ VLAN は、プライベート VLAN 無差別トランク ポート上で動作可能になる前に関連付ける必要があります。

はじめる前に

プライベート VLAN 機能がイネーブルであることを確認してください。

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

手順の概要

1. **config t**
2. **interface** {*type slot/port*}
3. **switchport**
4. **switchport mode private-vlan trunk promiscuous**
5. （任意） **switchport private-vlan trunk native vlan** *vlan-id*
6. **switchport mode private-vlan trunk allowed vlan** {**add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*}
7. 次のいずれかのコマンドを入力します。
8. **exit**
9. （任意） **show interface switchport**
10. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

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

ステップ 3	**switchport**
	
	例：
	`switch(config-if)# switchport`
	`switch(config-if)#`
		レイヤ 2 ポートをスイッチ ポートとして設定します。

ステップ 4	**switchport mode private-vlan trunk promiscuous**
	
	例：
	`switch(config-if)# switchport mode private-vlan trunk promiscuous`
	`switch(config-if)#`
		レイヤ 2 ポートを、複数のプライベート VLAN と通常の VLAN のトラフィックを伝送するための無差別トランク ポートして設定します。

	コマンドまたはアクション	目的
ステップ 5	**switchport private-vlan trunk native vlan** *vlan-id* 例： `switch(config-if)# switchport private-vlan trunk native vlan 5`	（任意） 802.1Q トランクのネイティブ VLAN を設定します。有効値の範囲は 1 ～ 3968 および 4048 ～ 4093 です。デフォルト値は 1 です。 （注） プライベート VLAN を無差別トランク ポートのネイティブ VLAN として使用している場合は、プライマリ VLAN または標準 VLAN の値を入力する必要があります。セカンダリ VLAN をネイティブ VLAN として設定することはできません。

ステップ 6	**switchport mode private-vlan trunk allowed vlan** {**add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*}
	
	例：
	`switch(config-if)# switchport private-vlan trunk allowed vlan add 1`
	`switch(config-if)#`
		プライベート VLAN 無差別トランク インターフェイスの許可 VLAN を設定します。 有効値の範囲は 1 ～ 3968 および 4048 ～ 4093 です。
		プライベート プライマリ VLAN およびセカンダリ VLAN を無差別トランク ポートにマッピングすると、すべてのプライマリ VLAN がこのポートの許可される VLAN リストに自動的に追加されます。
		（注） ネイティブ VLAN が許可される VLAN リストに含まれていることを確認します。このコマンドでは、デフォルトでこのインターフェイス上の VLAN が許可されないため、ネイティブ VLAN トラフィックを通過させるには、ネイティブ VLAN を許可される VLAN として設定する必要があります（関連する VLAN として追加済みでない場合）。

ステップ 7	次のいずれかのコマンドを入力します。	

	コマンドまたはアクション	目的
	オプション / 説明	
	switchport private-vlan mapping trunk *primary-vlan-id* {**add** *secondary-vlan-list* | **remove** *secondary-vlan-id*} — 無差別トランク ポートと、プライマリ VLAN および選択した関連するセカンダリ VLAN のリストをマッピングするかマッピングを削除します。 セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかとして設定できます。 トラフィックを通過させるには、プライマリ VLAN とセカンダリ VLAN の間のプライベート VLAN の関連付けが動作する必要があります。 各無差別トランク ポートに対し、最大 16 個のプライベート VLAN のプライマリとセカンダリのペアをマッピングできます。 作業しているプライマリ VLAN それぞれに対してコマンドを再入力する必要があります。	
	no switchport private-vlan mapping trunk [*primary-vlan-id* [*secondary-vlan-id*]] — インターフェイスからプライベート VLAN 無差別トランクマッピングを削除します。	

	例：
	`switch(config-if)# switchport private-vlan mapping trunk 4 add 5`
	`switch(config-if)#`	

ステップ 8	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 9	**show interface switchport** 例： `switch# show interface switchport`	（任意） スイッチポートとして設定されているすべてのインターフェイスに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 10	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、レイヤ 2 ポート 2/1 を、2 つのプライマリ VLAN とそれに関連するセカンダリ VLAN に関連付けられた無差別トランク ポートとして設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport
switch(config-if)# switchport mode private-vlan trunk promiscuous
switch(config-if)# switchport private-vlan trunk allowed vlan add 1
switch(config-if)# switchport private-vlan mapping trunk 2 add 3
switch(config-if)# switchport private-vlan mapping trunk 4 add 5
switch(config-if)# switchport private-vlan mapping trunk 1 add 20
switch(config-if)# exit
switch(config)#
```

プライベート VLAN 設定の確認

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

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

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』を参照してください。

プライベート VLAN の統計情報の表示とクリア

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

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

プライベート VLAN の設定例

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

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

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

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

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

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

プライベート VLAN の追加情報（CLI バージョン）

関連資料

関連項目	参照先
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』
VLAN インターフェイス、IP アドレス指定	『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』
スタティック MAC アドレス、セキュリティ	『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x*』
Cisco NX-OS の基礎	『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x*』
ハイ アベイラビリティ	『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』
システム管理	『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x*』
仮想デバイス コンテキスト（VDC）	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.x*』

標準

標準	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 のリンク
• CISCO-PRIVATE-VLAN-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

プライベート VLAN 設定の機能履歴（CLI バージョン）

次の表に、この機能のリリースの履歴を示します。

表 *10*：プライベート *VLAN* 設定の機能履歴

機能名	リリース	機能情報
プライベート VLAN 無差別トランク ポートと独立トランク ポート	5.0(2)	この機能では、無差別ポートから複数のプライベート VLAN および通常の VLAN のトラフィックを伝送でき、独立ポートから複数の独立 VLAN および通常の VLAN のトラフィックを伝送できます。
変更なし	4.2(1)	–
デバイス上でイネーブルになっている機能の表示	4.1(2)	次のコマンドを入力すると、デバイス上でイネーブルになっている機能を表示できます。 • **show feature**

第 7 章

Cisco NX-OS を使用した Rapid PVST+ の設定

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

この章は、次の内容で構成されています。

- Information About Rapid PVST+, 93 ページ
- Licensing Requirements for Rapid PVST+, 111 ページ
- Prerequisites for Configuring Rapid PVST+, 112 ページ
- Guidelines and Limitations for Configuring Rapid PVST+, 112 ページ
- Rapid PVST+ のデフォルト設定, 113 ページ
- Rapid PVST+ の設定, 115 ページ
- Rapid PVST+ の設定の確認, 134 ページ
- Rapid PVST+ 統計情報の表示およびクリア（CLI バージョン）, 135 ページ
- Rapid PVST+ の設定例, 135 ページ
- Rapid PVST+ の追加情報（CLI バージョン）, 136 ページ
- Rapid PVST+ の設定の機能履歴（CLI バージョン）, 137 ページ

Information About Rapid PVST+

（注） See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』, for information on creating Layer 2 interfaces.

The Spanning Tree Protocol (STP) was implemented to provide a loop-free network at Layer 2 of the network. Rapid PVST+ is an updated implementation of STP that allows you to create one spanning tree topology for each VLAN. Rapid PVST+ is the default STP mode on the device.

（注） Spanning tree is used to refer to IEEE 802.1w and IEEE 802.1s. If the IEEE 802.1D Spanning Tree Protocol is discussed in this publication, then 802.1D is stated specifically.

（注） You can run either Rapid PVST+ or MST within each virtual device context (VDC). You cannot run both STP modes simultaneously in a VDC. Rapid PVST+ is the default STP mode.

The Rapid PVST+ protocol is the IEEE 802.1w standard, Rapid Spanning Tree Protocol (RSTP), implemented on a per VLAN basis. Rapid PVST+ interoperates with the IEEE 802.1Q VLAN standard, which mandates a single STP instance for all VLANs, rather than per VLAN.

Rapid PVST+ is enabled by default on the default VLAN (VLAN1) and on all newly created VLANs on the device. Rapid PVST+ interoperates with devices that run legacy IEEE 802.1D STP.

RSTP is an improvement on the original STP standard, 802.1D, which allows faster convergence.

（注） The device supports full nondisruptive upgrades for Rapid PVST+. See the 『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』, for complete information on nondisruptive upgrades.

The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this chapter. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

（注） Beginning with Cisco NX-OS Release 5.x, when you are running virtual port channels (vPCs), you can configure STP for better performance. See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』, for more information on this feature.

STP

STP is a Layer 2 link-management protocol that provides path redundancy while preventing loops in the network.

Overview of STP

In order for a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. STP operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

When you create fault-tolerant internetworks, you must have a loop-free path between all nodes in a network. The STP algorithm calculates the best loop-free path throughout a switched Layer 2 network. Layer 2 LAN ports send and receive STP frames, which are called Bridge Protocol Data Units (BPDUs), at regular intervals. Network devices do not forward these frames but use the frames to construct a loop-free path.

Multiple active paths between end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages and network devices might learn end station MAC addresses on multiple Layer 2 LAN ports.

STP defines a tree with a root bridge and a loop-free path from the root to all network devices in the Layer 2 network. STP forces redundant data paths into a blocked state. If a network segment in the spanning tree fails and a redundant path exists, the STP algorithm recalculates the spanning tree topology and activates the blocked path.

When two Layer 2 LAN ports on a network device are part of a loop, the STP port priority and port path-cost setting determine which port on the device is put in the forwarding state and which port is put in the blocking state. The STP port priority value is the efficiency with which that location allows the port to pass traffic. The STP port path-cost value is derived from the media speed.

How a Topology is Created

All devices in a LAN that participate in a spanning tree gather information about other switches in the network by exchanging BPDUs. This exchange of BPDUs results in the following actions:

- The system elects a unique root switch for the spanning tree network topology.
- The system elects a designated switch for each LAN segment.
- The system eliminates any loops in the switched network by placing redundant switch ports in a backup state; all paths that are not needed to reach the root device from anywhere in the switched network are placed in an STP-blocked state.

The topology on an active switched network is determined by the following:

- The unique device identifier Media Access Control (MAC) address of the device that is associated with each device
- The path cost to the root that is associated with each switch port
- The port identifier that is associated with each switch port

In a switched network, the root switch is the logical center of the spanning tree topology. STP uses BPDUs to elect the root switch and root port for the switched network.

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。

Bridge Priority Value

The bridge priority is a 4-bit value when the extended system ID is enabled.

You can only specify a device bridge ID (used by the spanning tree algorithm to determine the identity of the root bridge; the lowest number is preferred) as a multiple of 4096.

（注） In this device, the extended system ID is always enabled; you cannot disable the extended system ID.

Extended System ID

The device always uses the 12-bit extended system ID.

This figure shows the 12-bit extended system ID field that is part of the bridge ID.

図 *4* : ***Bridge ID with Extended System ID***

This table shows how the system ID extension combined with the bridge ID functions as the unique identifier for a VLAN.

表 *11* : ***Bridge Priority Value and Extended System ID with the Extended System ID Enabled***

Bridge Priority Value				Extended System ID (Set Equal to the VLAN ID)											
Bit 16	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

STP MAC Address Allocation

（注） MAC address reduction is always enabled on the device.

Because MAC address reduction is always enabled on the device, you should also enable MAC address reduction on all other Layer 2 connected network devices to avoid undesirable root bridge election and spanning tree topology issues.

When MAC address reduction is enabled, the root bridge priority becomes a multiple of 4096 plus the VLAN ID. You can only specify a device bridge ID (used by the spanning tree algorithm to determine the identity of the root bridge; the lowest number is preferred) as a multiple of 4096. Only the following values are possible:

- 0
- 4096
- 8192
- 12288

- 16384
- 20480
- 24576
- 28672
- 32768
- 36864
- 40960
- 45056
- 49152
- 53248
- 57344
- 61440

STP uses the extended system ID plus a MAC address to make the bridge ID unique for each VLAN.

（注） If another bridge in the same spanning tree domain does not run the MAC address reduction feature, it could win the root bridge ownership because of the finer granularity in the selection of its bridge ID.

BPDUs

Network devices transmit BPDUs throughout the STP instance. Each network device sends configuration BPDUs to communicate and compute the spanning tree topology. Each configuration BPDU contains the following minimal information:

- The unique bridge ID of the network device that the transmitting network device believes to be the root bridge
- The STP path cost to the root
- The bridge ID of the transmitting bridge
- The message age
- The identifier of the transmitting port
- Values for the hello, forward delay, and max-age protocol timer
- Additional information for STP extension protocols

When a network device transmits a Rapid PVST+ BPDU frame, all network devices connected to the VLAN on which the frame is transmitted receive the BPDU. When a network device receives a BPDU, it does not forward the frame but instead uses the information in the frame to calculate a BPDU. If the topology changes, the device initiates a BPDU exchange.

A BPDU exchange results in the following:

- One network device is elected as the root bridge.

- The shortest distance to the root bridge is calculated for each network device based on the path cost.
- A designated bridge for each LAN segment is selected. This network device is closest to the root bridge through which frames are forwarded to the root.
- A root port is elected. This port provides the best path from the bridge to the root bridge.
- Ports included in the spanning tree are selected.

Election of the Root Bridge

For each VLAN, the network device with the highest bridge ID (that is, the lowest numerical ID value) is elected as the root bridge. If all network devices are configured with the default priority (32768), the network device with the lowest MAC address in the VLAN becomes the root bridge. The bridge priority value occupies the most significant bits of the bridge ID.

When you change the bridge priority value, you change the probability that the device will be elected as the root bridge. Configuring a lower value increases the probability; a higher value decreases the probability.

The STP root bridge is the logical center of each spanning tree topology in a Layer 2 network. All paths that are not needed to reach the root bridge from anywhere in the Layer 2 network are placed in STP blocking mode.

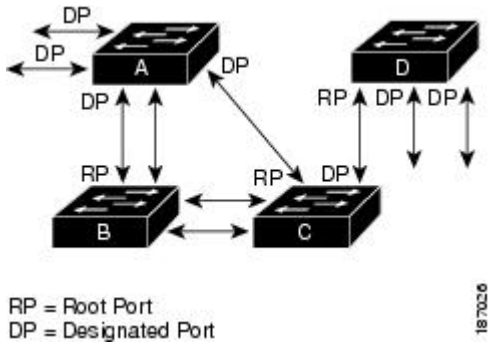
BPDUs contain information about the transmitting bridge and its ports, including bridge and MAC addresses, bridge priority, port priority, and path cost. STP uses this information to elect the root bridge for the STP instance, to elect the root port that leads to the root bridge, and to determine the designated port for each Layer 2 segment.

Creating the Spanning Tree Topology

By increasing the priority (lowering the numerical value) of the ideal network device so that it becomes the root bridge, you force an STP recalculation to form a new spanning tree topology with the ideal network device as the root.

In this figure, switch A is elected as the root bridge because the bridge priority of all the network devices is set to the default (32768) and switch A has the lowest MAC address. However, due to traffic patterns, the number of forwarding ports, or link types, switch A might not be the ideal root bridge.

図 *5* : ***Spanning Tree Topology***



When the spanning tree topology is calculated based on default parameters, the path between the source and destination end stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change. The goal is to make the fastest link the root port.

For example, assume that one port on switch B is a fiber-optic link, and another port on switch B (an unshielded twisted-pair [UTP] link) is the root port. Network traffic might be more efficient over the high-speed fiber-optic link. By changing the STP port priority on the fiber-optic port to a higher priority (lower numerical value) than the root port, the fiber-optic port becomes the new root port.

Rapid PVST+

Rapid PVST+ is the default spanning tree mode for the software and is enabled by default on the default VLAN and all newly created VLANs.

A single instance, or topology, of RSTP runs on each configured VLAN, and each Rapid PVST+ instance on a VLAN has a single root device. You can enable and disable STP on a per-VLAN basis when you are running Rapid PVST+.

Overview of Rapid PVST+

Rapid PVST+ is the IEEE 802.1w (RSTP) standard implemented per VLAN. A single instance of STP runs on each configured VLAN (if you do not manually disable STP). Each Rapid PVST+ instance on a VLAN has a single root switch. You can enable and disable STP on a per-VLAN basis when you are running Rapid PVST+.

（注） Rapid PVST+ is the default STP mode for the device.

Rapid PVST+ uses point-to-point wiring to provide rapid convergence of the spanning tree. The spanning tree reconfiguration can occur in less than 1 second with Rapid PVST+ (in contrast to 50 seconds with the default settings in the 802.1D STP). The device automatically checks the PVID.

（注） Rapid PVST+ supports one STP instance for each VLAN.

Using Rapid PVST+, STP convergence occurs rapidly. By default, each designated port in the STP sends out a BPDU every 2 seconds. On a designated port in the topology, if hello messages are missed three consecutive times, or if the maximum age expires, the port immediately flushes all protocol information in the table. A port considers that it loses connectivity to its direct neighbor designated port if it misses three BPDUs or if the maximum age expires. This rapid aging of the protocol information allows quick failure detection.

Rapid PVST+ provides for rapid recovery of connectivity following the failure of a device, a device port, or a LAN. It provides rapid convergence for edge ports, new root ports, and ports connected through point-to-point links as follows:

- Edge ports—When you configure a port as an edge port on an RSTP device, the edge port immediately transitions to the forwarding state. (This immediate transition was previously a Cisco-proprietary feature named PortFast.) You should only configure ports that connect to a single end station as edge ports. Edge ports do not generate topology changes when the link changes.

Enter the **spanning-tree port type** interface configuration command to configure a port as an STP edge port.

（注） We recommend that you configure all ports connected to a Layer 2 host as edge ports.

- Root port—If Rapid PVST+ selects a new root port, it blocks the old root port and immediately transitions the new root port to the forwarding state.
- Point-to-point links—If you connect a port to another port through a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port by using the proposal-agreement handshake to ensure a loop-free topology.

Rapid PVST+ achieves rapid transition to the forwarding state only on edge ports and point-to-point links. Although the link type is configurable, the system automatically derives the link type information from the duplex setting of the port. Full-duplex ports are assumed to be point-to-point ports, while half-duplex ports are assumed to be shared ports.

Edge ports do not generate topology changes, but all other designated and root ports generate a topology change (TC) BPDU when they either fail to receive three consecutive BPDUs from the directly connected neighbor or the maximum age times out. At this point, the designated or root port sends a BPDU with the TC flag set. The BPDUs continue to set the TC flag as long as the TC While timer runs on that port. The value of the TC While timer is the value set for the hello time plus 1 second. The initial detector of the topology change immediately floods this information throughout the entire topology.

When Rapid PVST+ detects a topology change, the protocol does the following:

- Starts the TC While timer with a value equal to twice the hello time for all the nonedge root and designated ports, if necessary.
- Flushes the MAC addresses associated with all these ports.

The topology change notification floods quickly across the entire topology. The system flushes dynamic entries immediately on a per-port basis when it receives a topology change.

（注） The TCA flag is used only when the device is interacting with devices that are running legacy 802.1D STP.

The proposal and agreement sequence then quickly propagates toward the edge of the network and quickly restores connectivity after a topology change.

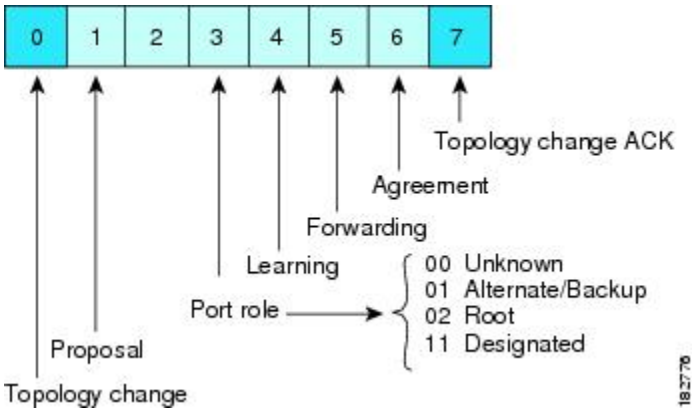
Rapid PVST+ BPDUs

Rapid PVST+ and 802.1w use all six bits of the flag byte to add the following:

- The role and state of the port that originates the BPDU
- The proposal and agreement handshake

This figure shows the use of the BPDU flags in Rapid PVST+.

図 *6* : ***Rapid PVST+ Flag Byte in BPDU***



Another important change is that the Rapid PVST+ BPDU is type 2, version 2, which makes it possible for the device to detect connected legacy (802.1D) bridges. The BPDU for 802.1D is type 0, version 0.

Proposal and Agreement Handshake

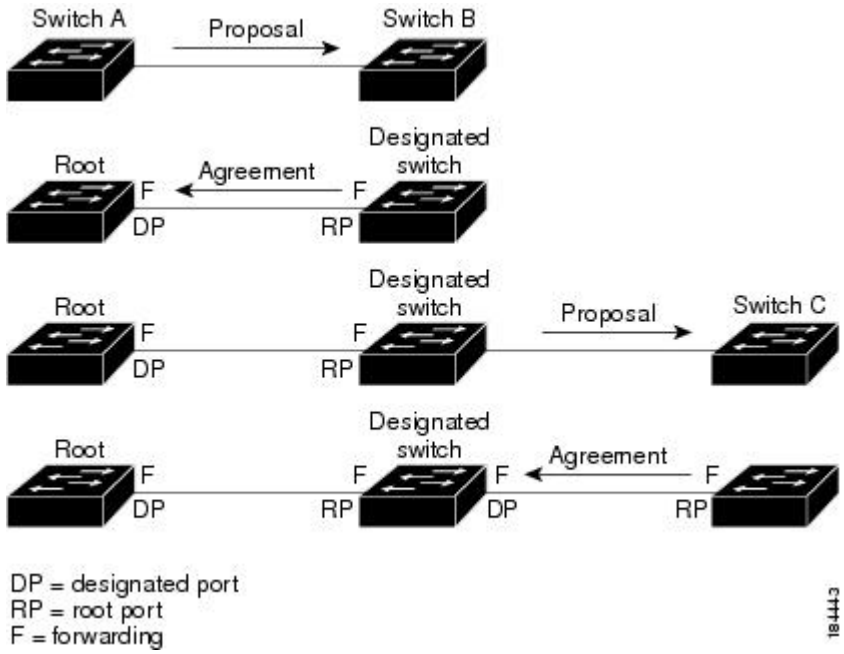
In this figure, switch A is connected to switch B through a point-to-point link, and all of the ports are in the blocking state. Assume that the priority of switch A is a smaller numerical value than the priority of switch B. Switch A sends a proposal message (a configuration BPDU with the proposal flag set) to switch B, proposing itself as the designated switch.

After receiving the proposal message, switch B selects as its new root port the port from which the proposal message was received, forces all nonedge ports to the blocking state, and sends an agreement message (a BPDU with the agreement flag set) through its new root port.

After receiving the agreement message from switch B, switch A also immediately transitions its designated port to the forwarding state. No loops in the network can form because switch B blocked all of its nonedge ports and because there is a point-to-point link between switches A and B.

When switch C connects to switch B, a similar set of handshaking messages are exchanged. Switch C selects the port connected to switch B as its root port, and both ends of the link immediately transition to the forwarding state. With each iteration of this handshaking process, one more switch joins the active topology. As the network converges, this proposal-agreement handshaking progresses from the root toward the leaves of the spanning tree as shown in this figure.

図 7： *Proposal and Agreement Handshaking for Rapid Convergence*



The switch learns the link type from the port duplex mode; a full-duplex port is considered to have a point-to-point connection and a half-duplex port is considered to have a shared connection. You can override the default setting that is controlled by the duplex setting by entering the **spanning-tree link-type** interface configuration command.

This proposal/agreement handshake is initiated only when a nonedge port moves from the blocking to the forwarding state. The handshaking process then proliferates step-by-step throughout the topology.

Protocol Timers

This table describes the protocol timers that affect the Rapid PVST+ performance.

表 12： *Rapid PVST+ Protocol Timers*

Variable	Description
Hello timer	Determines how often each device broadcasts BPDUs to other network devices. The default is 2 seconds, and the range is from 1 to 10.
Forward delay timer	Determines how long each of the listening and learning states last before the port begins forwarding. This timer is generally not used by the protocol, but it is used when interoperating with the 802.1D spanning tree. The default is 15 seconds, and the range is from 4 to 30 seconds.

Variable	Description
Maximum age timer	Determines the amount of time that protocol information received on a port is stored by the network device. This timer is generally not used by the protocol, but it is used when interoperating with the 802.1D spanning tree. The default is 20 seconds; the range is from 6 to 40 seconds.

Port Roles

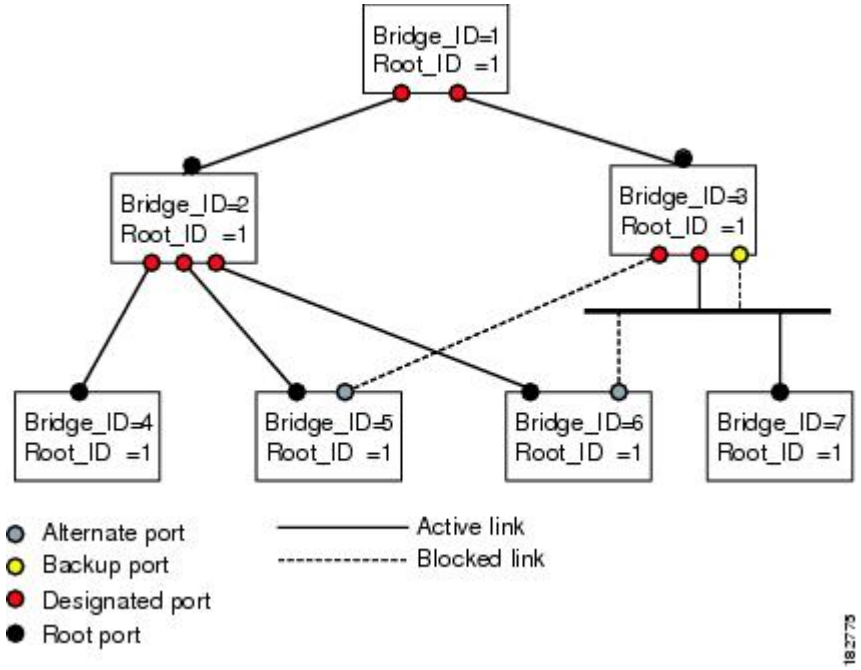
Rapid PVST+ provides rapid convergence of the spanning tree by assigning port roles and learning the active topology. Rapid PVST+ builds upon the 802.1D STP to select the device with the highest switch priority (lowest numerical priority value) as the root bridge. Rapid PVST+ assigns one of these port roles to individual ports:

- Root port—Provides the best path (lowest cost) when the device forwards packets to the root bridge.
- Designated port—Connects to the designated device that has the lowest path cost when forwarding packets from that LAN to the root bridge. The port through which the designated device is attached to the LAN is called the designated port.
- Alternate port—Offers an alternate path toward the root bridge to the path provided by the current root port. An alternate port provides a path to another device in the topology.
- Backup port—Acts as a backup for the path provided by a designated port toward the leaves of the spanning tree. A backup port can exist only when two ports are connected in a loopback by a point-to-point link or when a device has two or more connections to a shared LAN segment. A backup port provides another path in the topology to the device.
- Disabled port—Has no role within the operation of the spanning tree.

In a stable topology with consistent port roles throughout the network, Rapid PVST+ ensures that every root port and designated port immediately transition to the forwarding state while all alternate and backup ports are always in the blocking state. Designated ports start in the blocking state. The port state controls the operation of the forwarding and learning processes.

This figure shows port roles. A port with the root or a designated port role is included in the active topology. A port with the alternate or backup port role is excluded from the active topology.

図 *8* : ***Sample Topology Demonstrating Port Roles***



Rapid PVST+ Port State Overview

Propagation delays can occur when protocol information passes through a switched LAN. As a result, topology changes can take place at different times and at different places in a switched network. When a Layer 2 LAN port transitions directly from nonparticipation in the spanning tree topology to the forwarding state, it can create temporary data loops. Ports must wait for new topology information to propagate through the switched LAN before starting to forward frames.

Each Layer 2 LAN port on the device that uses Rapid PVST+ or MST exists in one of the following four states:

- Blocking—The Layer 2 LAN port does not participate in frame forwarding.
- Learning—The Layer 2 LAN port prepares to participate in frame forwarding.
- Forwarding—The Layer 2 LAN port forwards frames.
- Disabled—The Layer 2 LAN port does not participate in STP and is not forwarding frames.

When you enable Rapid PVST+, every port in the device, VLAN, and network goes through the blocking state and the transitory states of learning at power up. If properly configured, each Layer 2 LAN port stabilizes to the forwarding or blocking state.

When the STP algorithm places a Layer 2 LAN port in the forwarding state, the following process occurs:

1. The Layer 2 LAN port is put into the blocking state while it waits for protocol information that suggests it should go to the learning state.

2 The Layer 2 LAN port waits for the forward delay timer to expire, moves the Layer 2 LAN port to the learning state, and restarts the forward delay timer.

3 In the learning state, the Layer 2 LAN port continues to block frame forwarding as it learns the end station location information for the forwarding database.

4 The Layer 2 LAN port waits for the forward delay timer to expire and then moves the Layer 2 LAN port to the forwarding state, where both learning and frame forwarding are enabled.

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 ポートは、次の処理を実行します。

- 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。
- エンド ステーションの場所は、そのアドレス データベースには取り入れません （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 モジュールから受信した BPDU を、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。

Learning State

A Layer 2 LAN port in the learning state prepares to participate in frame forwarding by learning the MAC addresses for the frames. The Layer 2 LAN port enters the learning state from the blocking state.

A Layer 2 LAN port in the learning state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Incorporates the end station location into its address database.
- Receives BPDUs and directs them to the system module.
- Receives, processes, and transmits BPDUs received from the system module.
- Receives and responds to control plane messages.

Forwarding State

A Layer 2 LAN port in the forwarding state forwards frames. The Layer 2 LAN port enters the forwarding state from the learning state.

A Layer 2 LAN port in the forwarding state performs as follows:

- Forwards frames received from the attached segment.

- Forwards frames switched from another port for forwarding.
- Incorporates the end station location information into its address database.
- Receives BPDUs and directs them to the system module.
- Processes BPDUs received from the system module.
- Receives and responds to control plane messages.

Disabled State

A Layer 2 LAN port in the disabled state does not participate in frame forwarding or STP. A Layer 2 LAN port in the disabled state is virtually nonoperational.

A disabled Layer 2 LAN port performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Does not incorporate the end station location into its address database. (There is no learning, so there is no address database update.)
- Does not receive BPDUs from neighbors.
- Does not receive BPDUs for transmission from the system module.

Summary of Port States

This table lists the possible operational and Rapid PVST+ states for ports and whether the port is included in the active topology.

表 *13* : ***Port State Active Topology***

Operational Status	Port State	Is Port Included in the Active Topology?
Enabled	Blocking	No
Enabled	Learning	Yes
Enabled	Forwarding	Yes
Disabled	Disabled	No

Synchronization of Port Roles

When the device receives a proposal message on one of its ports and that port is selected as the new root port, Rapid PVST+ forces all other ports to synchronize with the new root information.

The device is synchronized with superior root information received on the root port if all other ports are synchronized. An individual port on the device is synchronized if either of the following applies:

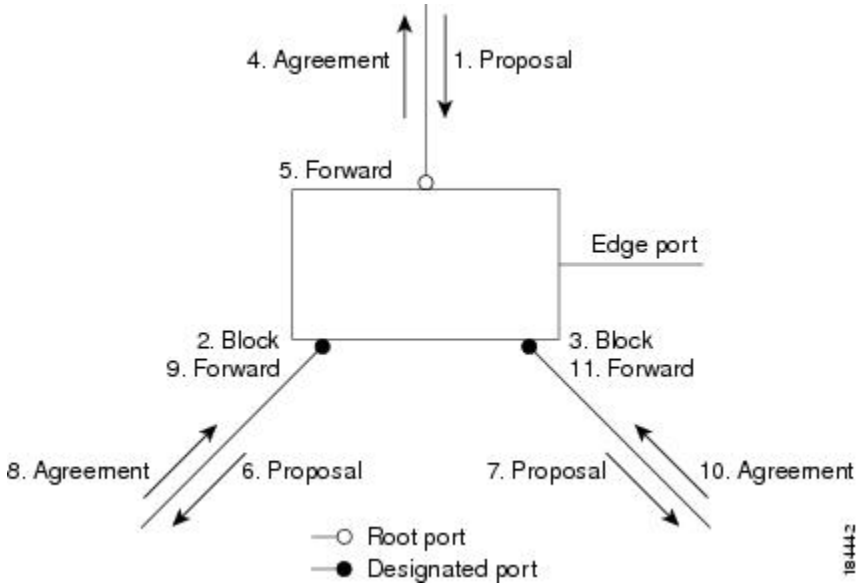
- That port is in the blocking state.
- It is an edge port (a port configured to be at the edge of the network).

If a designated port is in the forwarding state and is not configured as an edge port, it transitions to the blocking state when the Rapid PVST+ forces it to synchronize with new root information. In general, when the Rapid PVST+ forces a port to synchronize with root information and the port does not satisfy any of the above conditions, its port state is set to blocking.

After ensuring that all of the ports are synchronized, the device sends an agreement message to the designated device that corresponds to its root port. When the devices connected by a point-to-point link are in agreement about their port roles, Rapid PVST+ immediately transitions the port states to the forwarding state.

This figure shows the sequence of events during synchronization.

図 *9* : ***Sequence of Events During Rapid Convergence***



Processing Superior BPDU Information

A superior BPDU is a BPDU with root information (such as a lower switch ID or lower path cost) that is superior to what is currently stored for the port.

If a port receives a superior BPDU, Rapid PVST+ triggers a reconfiguration. If the port is proposed and is selected as the new root port, Rapid PVST+ forces all the designated, nonedge ports to synchronize.

If the received BPDU is a Rapid PVST+ BPDU with the proposal flag set, the device sends an agreement message after all of the other ports are synchronized. The new root port transitions to the forwarding state as soon as the previous port reaches the blocking state.

If the superior information received on the port causes the port to become a backup port or an alternate port, Rapid PVST+ sets the port to the blocking state and sends an agreement message. The designated port continues sending BPDUs with the proposal flag set until the forward-delay timer expires. At that time, the port transitions to the forwarding state.

Processing Inferior BPDU Information

An inferior BPDU is a BPDU with root information (such as a higher switch ID or higher path cost) that is inferior to what is currently stored for the port.

If a designated port receives an inferior BPDU, it immediately replies with its own information.

Detecting Unidirectional Link Failure:Rapid PVST+

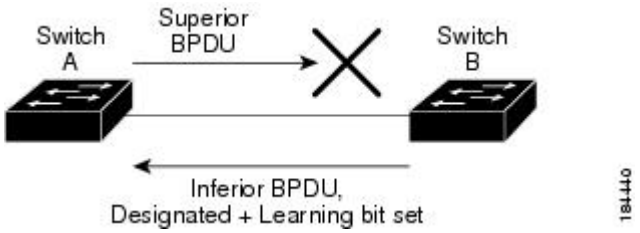
The software checks the consistency of the port role and state in the received BPDUs to detect unidirectional link failures that could cause bridging loops using the Unidirectional Link Detection (UDLD) feature. This feature is based on the dispute mechanism.

See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』, for information on UDLD.

When a designated port detects a conflict, it keeps its role, but reverts to a discarding state because disrupting connectivity in case of inconsistency is preferable to opening a bridging loop.

This figure illustrates a unidirectional link failure that typically creates a bridging loop. Switch A is the root bridge, and its BPDUs are lost on the link leading to switch B. The 802.1w-standard BPDUs include the role and state of the sending port. With this information, switch A can detect that switch B does not react to the superior BPDUs that it sends and that switch B is the designated, not root port. As a result, switch A blocks (or keeps blocking) its port, which prevents the bridging loop.

図 *10*： *Detecting Unidirectional Link Failure*



Port Cost

（注） Rapid PVST+ uses the short (16-bit) path-cost method to calculate the cost by default. With the short path-cost method, you can assign any value in the range of 1 to 65535. However, you can configure the device to use the long (32-bit) path-cost method, which allows you to assign any value in the range of 1 to 200,000,000. You configure the path-cost calculation method globally.

This table shows how the STP port path-cost default value is determined from the media speed and path-cost calculation method of a LAN interface.

表 *14* : *Default Port Cost*

Bandwidth	Short Path-Cost Method of Port Cost	Long Path-Cost Method of Port Cost
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gigabit Ethernet	4	20,000
10 Gigabit Ethernet	2	2,000

If a loop occurs, STP considers the port cost when selecting a LAN interface to put into the forwarding state.

You can assign the lower cost values to LAN interfaces that you want STP to select first and higher cost values to LAN interfaces that you want STP to select last. If all LAN interfaces have the same cost value, STP puts the LAN interface with the lowest LAN interface number in the forwarding state and blocks other LAN interfaces.

On access ports, you assign the port cost by the port. On trunk ports, you assign the port cost by the VLAN; you can configure the same port cost to all the VLANs on a trunk port.

Port Priority

If a redundant path occurs and multiple ports have the same path cost, Rapid PVST+ considers the port priority when selecting which LAN port to put into the forwarding state. You can assign lower priority values to LAN ports that you want Rapid PVST+ to select first and higher priority values to LAN ports that you want Rapid PVST+ to select last.

If all LAN ports have the same priority value, Rapid PVST+ puts the LAN port with the lowest LAN port number in the forwarding state and blocks other LAN ports. The possible priority range is from 0 through 224 (the default is 128), configurable in increments of 32. The device uses the port priority value when the LAN port is configured as an access port and uses the VLAN port priority values when the LAN port is configured as a trunk port.

Rapid PVST+ and IEEE 802.1Q Trunks

The 802.1Q trunks impose some limitations on the STP strategy for a network. In a network of Cisco network devices connected through 802.1Q trunks, the network devices maintain one instance of STP for each VLAN allowed on the trunks. However, non-Cisco 802.1Q network devices maintain only one instance of STP for all VLANs allowed on the trunks, which is the Common Spanning Tree (CST).

When you connect a Cisco network device to a non-Cisco device through an 802.1Q trunk, the Cisco network device combines the STP instance of the 802.1Q VLAN of the trunk with the STP instance of the non-Cisco 802.1Q network device. However, all per-VLAN STP information that is maintained by Cisco network devices is separated by a cloud of non-Cisco 802.1Q network devices. The non-Cisco 802.1Q cloud that separates the Cisco network devices is treated as a single trunk link between the network devices.

For more information on 802.1Q trunks, see the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』.

Rapid PVST+ Interoperation with Legacy 802.1D STP

Rapid PVST+ can interoperate with devices that are running the legacy 802.1D protocol. The device knows that it is interoperating with equipment running 802.1D when it receives a BPDU version 0. The BPDUs for Rapid PVST+ are version 2. If the BPDU received is an 802.1w BPDU version 2 with the proposal flag set, the device sends an agreement message after all of the other ports are synchronized. If the BPDU is an 802.1D BPDU version 0, the device does not set the proposal flag and starts the forward-delay timer for the port. The new root port requires twice the forward-delay time to transition to the forwarding state.

The device interoperates with legacy 802.1D devices as follows:

- Notification—Unlike 802.1D BPDUs, 802.1w does not use TCN BPDUs. However, for interoperability with 802.1D devices, the device processes and generates TCN BPDUs.
- Acknowledgment—When an 802.1w device receives a TCN message on a designated port from an 802.1D device, it replies with an 802.1D configuration BPDU with the TCA bit set. However, if the TC-while timer (the same as the TC timer in 802.1D) is active on a root port connected to an 802.1D device and a configuration BPDU with the TCA set is received, the TC-while timer is reset.

  This method of operation is required only for 802.1D devices. The 802.1w BPDUs do not have the TCA bit set.
- Protocol migration—For backward compatibility with 802.1D devices, 802.1w selectively sends 802.1D configuration BPDUs and TCN BPDUs on a per-port basis.

  When a port is initialized, the migrate-delay timer is started (specifies the minimum time during which 802.1w BPDUs are sent), and 802.1w BPDUs are sent. While this timer is active, the device processes all BPDUs received on that port and ignores the protocol type.

  If the device receives an 802.1D BPDU after the port migration-delay timer has expired, it assumes that it is connected to an 802.1D device and starts using only 802.1D BPDUs. However, if the 802.1w device is using 802.1D BPDUs on a port and receives an 802.1w BPDU after the timer has expired, it restarts the timer and starts using 802.1w BPDUs on that port.

（注） If you want all devices on the same LAN segment to reinitialize the protocol on each interface, you must reinitialize Rapid PVST+.

Rapid PVST+ Interoperation with 802.1s MST

Rapid PVST+ interoperates seamlessly with the IEEE 802.1s Multiple Spanning Tree (MST) standard. No user configuration is needed. To disable this seamless interoperation, you can use PVST Simulation.

High Availability for Rapid PVST+

The software supports high availability for Rapid PVST+. However, the statistics and timers are not restored when Rapid PVST+ restarts. The timers start again and the statistics begin from 0.

（注） See the 『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』, for complete information on high-availability features.

Virtualization Support for Rapid PVST+

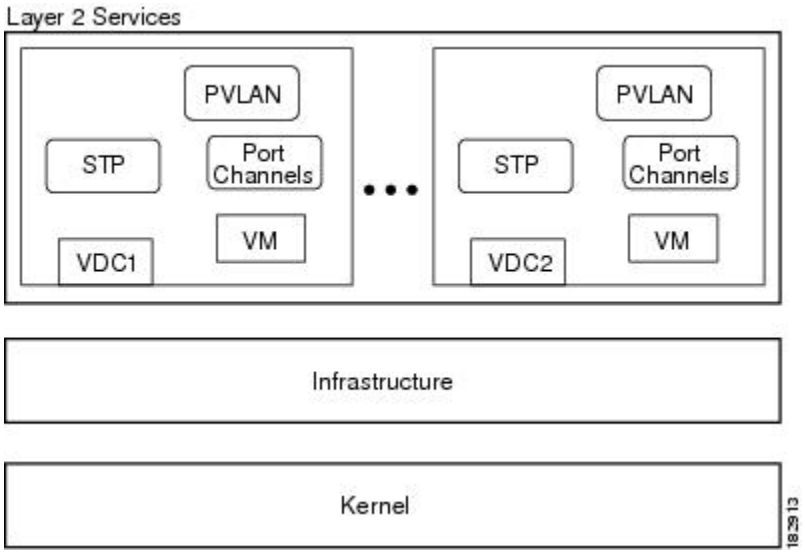
（注） See the 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』, for complete information on virtual device contexts (VDCs) and assigning resources.

This figure shows how the system provides support for VDCs. Using VDCs, you have a separate Layer 2 virtualization in each VDC, and each VDC runs a separate STP.

Each VDC will have its own Rapid PVST+. You cannot configure Rapid PVST+ across VDCs with Cisco NX-OS software. However, you can run Rapid PVST+ in one VDC and run MST in each VDC.

For example, VDC1 can run MST, VDC2 can run Rapid PVST+, and VDC3 can run MST.

図 *11*： *Separate STP in each VDC*



Ensure that you are in the correct VDC before you begin configuring either Rapid PVST+ parameters.

Licensing Requirements for Rapid PVST+

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	Rapid PVST+ requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see 『*Cisco NX-OS Licensing Guide*』.

However, using VDCs requires an Advanced Services license.

Prerequisites for Configuring Rapid PVST+

Rapid PVST+ has the following prerequisites:

- You must be logged onto the device.
- If required, install the Advanced Services license and enter the desired VDC.
- If you are working in another VDC than the default VDC, that VDC must be created already.

Guidelines and Limitations for Configuring Rapid PVST+

Rapid PVST+ has the following configuration guidelines and limitations:

- There is a total of 4000 Rapid PVST+ for each VDC.
- The maximum number of VLANs and ports is 16,000.
- Only Rapid PVST+ or MST can be active at any time for each VDC.
- Port channeling—The port-channel bundle is considered as a single port. The port cost is the aggregation of all the configured port costs assigned to that channel.
- For Private VLANs, on a normal VLAN trunk port, the primary and secondary private VLANs are two different logical ports and must have the exact STP topology. On access ports, STP sees only the primary VLAN.
- We recommend that you configure all ports connected to Layer 2 hosts as STP edge ports.
- Always leave STP enabled.
- Do not change timers because changing timers can adversely affect stability.
- Keep user traffic off the management VLAN; keep the management VLAN separate from the user data.
- Choose the distribution and core layers as the location of the primary and secondary root switches.
- When you connect two Cisco devices through 802.1Q trunks, the switches exchange spanning tree BPDUs on each VLAN allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved 802.1D spanning tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all VLANs on the trunk are sent tagged to the reserved Cisco Shared Spanning Tree Protocol (SSTP) multicast MAC address (01-00-0c-cc-cc-cd).

Rapid PVST+ のデフォルト設定

次の表に、Rapid PVST+ パラメータのデフォルト設定を示します。

表 *15*：デフォルト *Rapid PVST+* パラメータ

パラメータ	デフォルト
スパニングツリー	すべての VLAN でイネーブル
スパニングツリー モード	Rapid PVST+ **注意** スパニングツリー モードを変更すると、すべてのスパニングツリー インスタンスが前のモードで停止して新規モードで開始されるため、トラフィックが中断されます。
VLAN	VLAN 1 に割り当てられたすべてのポート
拡張システム ID	常にイネーブル
MAC アドレス リダクション	常にイネーブル
ブリッジ ID プライオリティ	32769（デフォルト VLAN 1 のデフォルト ブリッジ プライオリティに拡張システム ID を加えた値）
ポート ステート	ブロッキング（コンバージェンスが発生すると、即座に変更される）
ポート ロール	指定（コンバージェンスが発生すると、変更される）
ポート/VLAN プライオリティ	128.
パスコスト計算方式	ショート

パラメータ	デフォルト
ポート/VLAN コスト	Auto デフォルトのポート コストは、次のように、メディア速度およびパスコスト計算方式から判別されます。 • 10 Mbps： ◦ ショート：100 ◦ ロング：2,000,000 • 100 Mbps： ◦ ショート：19 ◦ ロング：200,000 • 1 ギガビット イーサネット： ◦ ショート：4 ◦ ロング：20,000 • 10 ギガビット イーサネット： ◦ ショート：2 ◦ ロング：2,000
hello タイム	2 秒
転送遅延時間	15 秒
最大エージング タイム	20 秒
リンク タイプ	Auto デフォルト リンク タイプは、次のようにデュプレックスから判別されます。 • 全二重：ポイントツーポイント リンク • 半二重：共有リンク

Rapid PVST+ の設定

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

Rapid PVST+ は VLAN ごとにイネーブルにします。 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）。 デフォルトで Rapid PVST+ は、デフォルト VLAN と、作成した各 VLAN でイネーブルになります。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

Rapid PVST+ の設定に関する注意事項

正しい VDC を開始していることを確認してください（『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照）。

Rapid PVST+ のイネーブル化（CLI バージョン）

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

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

（注） スパニングツリー モードを変更すると、すべてのスパニングツリー インスタンスが前のモードで停止して新規モードで再開されるため、トラフィックが中断されます。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree mode rapid-pvst** 例： `switch(config)# spanning-tree mode rapid-pvst`	デバイスで Rapid PVST+ をイネーブルにします。 Rapid PVST+ はデフォルトのスパニングツリー モードです。 （注） スパニングツリーモードを変更すると、変更前のモードのスパニングツリーインスタンスがすべて停止されて新しいモードで起動されるため、トラフィックが中断する場合があります。

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

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

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

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

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

Rapid PVST+ の VLAN 単位でのディセーブル化またはイネーブル化（CLI バージョン）

Rapid PVST+ は、VLAN ごとにイネーブルまたはディセーブルにできます。

（注） Rapid PVST+ は、デフォルト VLAN と、作成したすべての VLAN でデフォルトでイネーブルになります。

はじめる前に

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

手順の概要

1. **config t**
2. 次のいずれかのコマンドを入力します。
3. **exit**
4. （任意） **show spanning-tree**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。	

	コマンドまたはアクション	目的
	オプション / 説明 **spanning-tree vlan** *vlan-range*：VLAN ごとに Rapid PVST+（デフォルト STP）をイネーブルにします。*vlan-range* の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。 **no spanning-tree vlan** *vlan-range*：指定 VLAN で Rapid PVST+ をディセーブルにします。 このコマンドに関する詳細については、注意を参照してください。 例： `switch(config)# spanning-tree vlan 5`	

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

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

次に、VLAN 5 で STP をイネーブルにする例を示します。

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

（注） VLAN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ない場合は、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。 VLAN 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して、VLANのその他のスイッチおよびブリッジでイネーブルにしておくことはできません。 スパニングツリーをイネーブルにしたスイッチとブリッジに、ネットワークの物理トポロジに関する不完全な情報が含まれることになるので、この処理によって予想外の結果となることがあります。

注意 物理的なループが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しないことを推奨します。 スパニングツリーは、設定の誤りおよび配線の誤りに対する保護手段として動作します。 VLAN 内に物理的なループが存在しないことを保証できる場合以外は、VLAN でスパニングツリーをディセーブルにしないでください。

（注） STP はデフォルトでイネーブルのため、設定結果を参照するために **show running** コマンドを入力しても、STP をイネーブルするために入力したコマンドは表示されません。

ルート ブリッジ ID の設定

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

特定のVLANインスタンスがルートブリッジになるように設定するには、そのブリッジのプライオリティをデフォルト値（32768）よりかなり小さい値に変更します。

spanning-tree vlan *vlan_ID* **primary root** コマンドを入力すると、各 VLAN で現在ルートになっているブリッジのブリッジ プライオリティがデバイスによって確認されます。 24576 という値でデバイスが指定 VLAN のルートになる場合、デバイスは指定 VLAN のブリッジ プライオリティをこの値に設定します。 指定 VLAN のルート ブリッジのブリッジ プライオリティが 24576 より小さい場合、デバイスは最小ブリッジ プライオリティより 4096 小さい値に指定 VLAN のブリッジ プライオリティを設定します。

（注） ルート ブリッジになるために必要な値が 4096 より小さい場合は、**spanning-tree vlan** *vlan_ID* **primary root** コマンドはエラーになります。 ソフトウェアでブリッジ プライオリティをそれ以上低くできない場合、デバイスは次のメッセージを返します。

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

注意 STP のインスタンスごとのルート ブリッジは、バックボーンまたはディストリビューション デバイスである必要があります。 アクセス デバイスは、STP のプライマリ ルートとして設定しないでください。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間における最大ブリッジ ホップ数）を指定するには、**diameter** キーワードを入力します。ネットワーク直径を指定すると、その直径のネットワークに最適な hello タイム、転送遅延時間、最大経過時間が自動的に選択されます。これにより、STP 収束の時間が大幅に削減されます。キーワード **hello-time** を入力すると、自動的に計算された hello タイムを上書きできます。

（注） ルート ブリッジとして設定されているデバイスでは、hello タイム、転送遅延時間、最大エージング タイムは手動で設定（**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、**spanning-tree mst max-age** の各グローバル コンフィギュレーション コマンドを使用）しないでください。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree vlan** *vlan-range* **root primary** [**diameter** *dia* [**hello-time** *hello-time*]] 例： `switch(config)# spanning-tree vlan 5 root primary diameter 4`	デバイスをプライマリ ルート ブリッジとして設定します。 The *vlan-range* の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。*dia* のデフォルトは 7 です。 *hello-time* の範囲は 1 ～ 10 秒で、デフォルト値は 2 秒です。

	コマンドまたはアクション	目的

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

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

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

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

セカンダリ ルート ブリッジの設定（CLI バージョン）

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

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間における最大ブリッジ ホップ数）を指定するには、**diameter** キーワードを入力します。ネットワーク直径を指定すると、その直径のネットワークに最適な hello タイム、転送遅延時間、最大経過時間が自動的に選択されます。これにより、STP 収束の時間が大幅に削減されます。キーワード **hello-time** を入力すると、自動的に計算された hello タイムを上書きできます。

この方法で、複数のデバイスに複数のバックアップ ルート ブリッジを設定できます。 プライマリ ルート ブリッジの設定時に使用した値と同じネットワーク直径と hello タイムの値を入力します。

（注） ルート ブリッジとして設定されているデバイスでは、hello タイム、転送遅延時間、最大エージング タイムは手動で設定（**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、**spanning-tree mst max-age** の各グローバル コンフィギュレーション コマンドを使用）しないでください。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

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

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

ステップ 4	**show spanning-tree vlan** *vlan_id* 例： `switch# show spanning-tree vlan 5`	（任意） 指定された VLAN の STP コンフィギュレーションを表示します。

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

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

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

VLAN の Rapid PVST+ のブリッジ プライオリティの設定

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

（注） この設定を使用するときは注意が必要です。 ブリッジ プライオリティを変更するには、プライマリ ルートおよびセカンダリ ルートを設定することを推奨します。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree vlan** *vlan-range* **priority** *value* 例： `switch(config)# spanning-tree vlan 5 priority 8192`	VLAN のブリッジ プライオリティを設定します。 有効な値は 0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。 その他すべての値は拒否されます。 デフォルト値は 32768 です。

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

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

次の例は、ギガビット イーサネット ポート 1/4 で VLAN 5 のプライオリティを 8192 に設定する方法を示しています。

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

Rapid PVST+ ポート プライオリティの設定（CLI バージョン）

Rapid PVST+ に最初に選択させる LAN ポートには小さいプライオリティ値を割り当て、Rapid PVST+ に最後に選択させる LAN ポートには大きいプライオリティ値を割り当てます。 すべての LAN ポートに同じプライオリティ値が割り当てられている場合、Rapid PVST+ は、LAN ポート番号が最小の LAN ポートをフォワーディング ステートにし、他の 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。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**spanning-tree** [**vlan** *vlan-list*] **port-priority** *priority* 例： `switch(config-if)# spanning-tree port-priority 160`	LAN インターフェイスのポート プライオリティを設定します。 *priority* の値は 0 ～ 224 の範囲です。 値が小さいほど、プライオリティは高くなります。 プライオリティ値は、0、32、64、96、128、160、192、224 です。その他すべての値は拒否されます。 デフォルト値は 128 です。

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

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

次の例は、イーサネット アクセス ポート 1/4 のポート プライオリティを 160 に設定する方法を示しています。

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

Rapid PVST+ パスコスト方式およびポート コストの設定（CLI バージョン）

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。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree pathcost method** {**long**	**short**} 例： `switch(config)# spanning-tree pathcost method long`	Rapid PVST+ パスコスト計算に使用される方式を選択します。 デフォルト方式は short 型です。

ステップ 3	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)`
		設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

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

	コマンドまたはアクション	目的

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

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

次の例は、イーサネット アクセス ポート 1/4 のポート コストを 1000 に設定する方法を示しています。

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

VLAN の Rapid PVST+ hello タイムの設定（CLI バージョン）

VLAN の Rapid-PVST+ hello タイムを設定できます。

（注） この設定を使用する場合は、注意してください。スパニングツリーが中断されることがあります。 ほとんどの場合、プライマリ ルートとセカンダリ ルートを設定して、hello タイムを変更することを推奨します。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree vlan** *vlan-range* **hello-time** *value* 例： `switch(config)# spanning-tree vlan 5 hello-time 7`	VLAN の hello タイムを設定します。 hello タイムの値の範囲は 1 ～ 10 秒で、デフォルトは 2 秒です。

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

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

次の例は、VLAN 5 の hello タイムを 7 秒に設定する方法を示しています。

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

VLAN の Rapid PVST+ 転送遅延時間の設定（CLI バージョン）

Rapid PVST+ の使用時は、VLAN ごとに転送遅延時間を設定できます。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree vlan** *vlan-range* **forward-time** *value* 例： `switch(config)# spanning-tree vlan 5 forward-time 21`	VLAN の転送遅延時間を設定します。 転送遅延時間の値の範囲は 4 ～ 30 秒で、デフォルトは 15 秒です。

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

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

次の例は、VLAN 5 の転送遅延時間を 21 秒に設定する方法を示しています。

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

```
switch(config)# exit
switch#
```

VLAN の Rapid PVST+ 最大エージング タイムの設定（CLI バージョン）

Rapid PVST+ の使用時は、VLAN ごとに最大経過時間を設定できます。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree vlan** *vlan-range* **max-age** *value* 例： `switch(config)# spanning-tree vlan 5 max-age 36`	VLAN の最大エージング タイムを設定します。 最大経過時間の値の範囲は 6 ～ 40 秒で、デフォルトは 20 秒です。

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

ステップ 4	**show spanning-tree vlan** *vlan_id* 例： `switch# show spanning-tree vlan 5`	（任意） STP コンフィギュレーションを VLAN 単位で表示します。

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

次の例は、VLAN 5 の最大エージング タイムを 36 秒に設定する方法を示しています。

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

Rapid PVST+ のリンク タイプの指定（CLI バージョン）

Rapid の接続性（802.1w 規格）は、ポイントツーポイントのリンク上でのみ確立されます。 リンク タイプは、デフォルトでは、インターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続であると見なされ、半二重ポートは共有接続であると見なされます。

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。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**spanning-tree link-type** {*auto* | *point-to-point* | *shared*} 例： `switch(config-if)# spanning-tree link-type point-to-point`	リンク タイプを、ポイントツーポイント インクまたは共有リンクに設定します。 デフォルト値はデバイス接続から読み取られ、半二重リンクは共有、全二重リンクはポイントツーポイントです。 リンク タイプが共有の場合、STP は 802.1D にフォール バックします。 デフォルトは auto で、インターフェイスのデュプレックス設定に基づいてリンク タイプが設定されます。

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

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

次の例は、リンク タイプをポイントツーポイント リンクとして設定する方法を示しています。

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

Rapid PVST+ 用のプロトコルの再初期化

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

はじめる前に

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

手順の概要

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

手順の詳細

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

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

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

Rapid PVST+ の設定の確認

Rapid PVST+ の設定情報を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
show running-config spanning-tree [**all**]	STP 情報を表示します。
show spanning-tree summary	STP の概要を表示します。
show spanning-tree detail	STP の詳細を表示します。

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

これらのコマンドの出力フィールドについては、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』を参照してください。

Rapid PVST+ 統計情報の表示およびクリア（CLI バージョン）

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

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

Rapid PVST+ の設定例

次に、Rapid PVST+ の設定例を示します。

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

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

switch(config)# spanning-tree port type edge
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# spanning-tree guard root
switch(config-if)# exit
switch(config)#
```

Rapid PVST+ の追加情報（CLI バージョン）

関連資料

関連項目	参照先
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』
レイヤ 2 インターフェイス	『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』
NX-OS の基礎	『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x*』
ハイ アベイラビリティ	『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』
システム管理	『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x*』
仮想デバイス コンテキスト（VDC）	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.x*』

標準

標準	タイトル
IEEE 802.1Q-2006（旧称 IEEE 802.1s）、IEEE 802.1D-2004（旧称 IEEE 802.1w）、IEEE 802.1D、IEEE 802.1t	—

MIB

MIB	MIB のリンク
• CISCO-STP-EXTENSION-MIB • BRIDGE-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Rapid PVST+ の設定の機能履歴（CLI バージョン）

次の表に、この機能のリリースの履歴を示します。

表 *16*：*Rapid PVST+* 設定の機能履歴

機能名	リリース	機能情報
変更なし	4.2(1)	--
変更なし	4.1(2)	--

第 8 章

Cisco NX-OS を使用した MST の設定

この章では、Cisco NX-OS デバイス上でマルチ スパニングツリー（MST）を設定する方法について説明します。

この章は、次の内容で構成されています。

- Information About MST, 139 ページ
- Licensing Requirements for MST, 149 ページ
- Prerequisites for MST, 149 ページ
- Guidelines and Limitations for Configuring MST, 149 ページ
- MST のデフォルト設定, 151 ページ
- Configuring MST, 152 ページ
- MST 設定の確認, 184 ページ
- MST 統計情報の表示およびクリア（CLI バージョン）, 185 ページ
- MST の設定例, 185 ページ
- MST の追加情報（CLI バージョン）, 187 ページ
- MST 設定の機能履歴（CLI バージョン）, 188 ページ

Information About MST

（注） See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』, for information on creating Layer 2 interfaces.

MST, which is the IEEE 802.1s standard, allows you to assign two or more VLANs to a spanning tree instance. MST is not the default spanning tree mode; Rapid per VLAN Spanning Tree (Rapid PVST+) is the default mode. MST instances with the same name, revision number, and VLAN-to-instance mapping combine to

form an MST region. The MST region appears as a single bridge to spanning tree configurations outside the region. MST forms a boundary to that interface when it receives an IEEE 802.1D Spanning Tree Protocol (STP) message from a neighboring device.

（注） Spanning tree is used to refer to IEEE 802.1w and IEEE 802.1s. If the IEEE 802.1D Spanning Tree Protocol is discussed in this publication, 802.1D is stated specifically.

（注） Beginning with Cisco NX-OS Release 5.x, when you are running virtual port channels (vPCs), you can configure STP for better performance. See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』, for more information on this feature.

MST Overview

（注） You must enable MST; Rapid PVST+ is the default spanning tree mode.

MST maps multiple VLANs into a spanning tree instance, with each instance having a spanning tree topology independent of other spanning tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of STP instances required to support a large number of VLANs. MST improves the fault tolerance of the network because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).

MST provides rapid convergence through explicit handshaking because each MST instance uses the IEEE 802.1w standard, which eliminates the 802.1D forwarding delay and quickly transitions root bridge ports and designated ports to the forwarding state.

MAC address reduction is always enabled on the device. You cannot disable this feature.

MST improves spanning tree operation and maintains backward compatibility with these STP versions:

- Original 802.1D spanning tree
- Rapid per-VLAN spanning tree (Rapid PVST+)

（注）
- IEEE 802.1 was defined in the Rapid Spanning Tree Protocol (RSTP) and was incorporated into IEEE 802.1D.
- IEEE 802.1 was defined in MST and was incorporated into IEEE 802.1Q.

MST Regions

To allow devices to participate in MST instances, you must consistently configure the devices with the same MST configuration information.

A collection of interconnected devices that have the same MST configuration is an MST region. An MST region is a linked group of MST bridges with the same MST configuration.

The MST configuration controls the MST region to which each device belongs. The configuration includes the name of the region, the revision number, and the VLAN-to-MST instance assignment mapping.

A region can have one or multiple members with the same MST configuration. Each member must be capable of processing 802.1w bridge protocol data units (BPDUs). There is no limit to the number of MST regions in a network.

Each device can support up to 65 MST instances (MSTIs), including Instance 0, in a single MST region. Instances are identified by any number in the range from 1 to 4094. The system reserves Instance 0 for a special instance, which is the IST. You can assign a VLAN to only one MST instance at a time.

The MST region appears as a single bridge to adjacent MST regions and to other Rapid PVST+ regions and 802.1D spanning tree protocols.

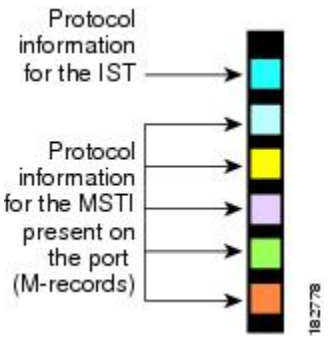
（注） We do not recommend that you partition the network into a large number of regions.

MST BPDUs

Each device has only one MST BPDU per interface, and that BPDU carries an M-record for each MSTI on the device. Only the IST sends BPDUs for the MST region; all M-records are encapsulated in that one BPDU that the IST sends. Because the MST BPDU carries information for all instances, the number of BPDUs that need to be processed to support MST is significantly reduced compared with Rapid PVST+.

Only the IST sends BPDUs for the MST region; all M-records are encapsulated in that one BPDU that the IST sends.

図 *12* : ***MST BPDU with M-Records for MSTIs***



MST Configuration Information

The MST configuration that must be identical on all devices within a single MST region is configured by the user.

You can configure the three parameters of the MST configuration as follows:

- Name—32-character string, null padded and null terminated, identifying the MST region

- Revision number—Unsigned 16-bit number that identifies the revision of the current MST configuration

（注） You must set the revision number when required as part of the MST configuration. The revision number is not incremented automatically each time that the MST configuration is committed.

- VLAN-to-MST instance mapping—4096-element table that associates each of the potential 4094 VLANs supported in each virtual device context (VDC) to a given instance with the first (0) and last element (4095) set to 0. The value of element number X represents the instance to which VLAN X is mapped.

（注） When you change the VLAN-to-MSTI mapping, the system reconverges MST.

MST BPDUs contain these three configuration parameters. An MST bridge accepts an MST BPDU into its own region only if these three configuration parameters match exactly. If one configuration attribute differs, the MST bridge considers the BPDU to be from another MST region.

IST, CIST, and CST

IST, CIST, and CST Overview

Unlike Rapid PVST+, in which all the STP instances are independent, MST establishes and maintains IST, CIST, and CST spanning trees, as follows:

- An IST is the spanning tree that runs in an MST region.

  MST establishes and maintains additional spanning trees within each MST region; these spanning trees are called multiple spanning tree instances (MSTIs).

  Instance 0 is a special instance for a region, known as the IST. The IST always exists on all ports; you cannot delete the IST, or Instance 0. By default, all VLANs are assigned to the IST. All other MST instances are numbered from 1 to 4094.

  The IST is the only STP instance that sends and receives BPDUs. All of the other MSTI information is contained in MST records (M-records), which are encapsulated within MST BPDUs.

  All MSTIs within the same region share the same protocol timers, but each MSTI has its own topology parameters, such as the root bridge ID, the root path cost, and so forth.

  An MSTI is local to the region; for example, MSTI 9 in region A is independent of MSTI 9 in region B, even if regions A and B are interconnected. Only CST information crosses region boundaries.

- The CST interconnects the MST regions and any instance of 802.1D and 802.1w STP that may be running on the network. The CST is the one STP instance for the entire bridged network and encompasses all MST regions and 802.1w and 802.1D instances.

- A CIST is a collection of the ISTs in each MST region. The CIST is the same as an IST inside an MST region, and the same as a CST outside an MST region.

The spanning tree computed in an MST region appears as a subtree in the CST that encompasses the entire switched domain. The CIST is formed by the spanning tree algorithm running among devices that support

the 802.1w, 802.1s, and 802.1D standards. The CIST inside an MST region is the same as the CST outside a region.

Spanning Tree Operation Within an MST Region

The IST connects all the MSTdevices in a region. When the IST converges, the root of the IST becomes the CIST regional root. The CIST regional root is also the CIST root if there is only one region in the network. If the CIST root is outside the region, the protocol selects one of the MST devices at the boundary of the region as the CIST regional root.

When an MST device initializes, it sends BPDUs that identify itself as the root of the CIST and the CIST regional root, with both the path costs to the CIST root and to the CIST regional root set to zero. The device also initializes all of its MSTIs and claims to be the root for all of them. If the device receives superior MSTI root information (lower switch ID, lower path cost, and so forth) than the information that is currently stored for the port, it relinquishes its claim as the CIST regional root.

During initialization, an MST region might have many subregions, each with its own CIST regional root. As devices receive superior IST information from a neighbor in the same region, they leave their old subregions and join the new subregion that contains the true CIST regional root. This action causes all subregions to shrink except for the subregion that contains the true CIST regional root.

All devices in the MST region must agree on the same CIST regional root. Any two devices in the region will only synchronize their port roles for an MSTI if they converge to a common CIST regional root.

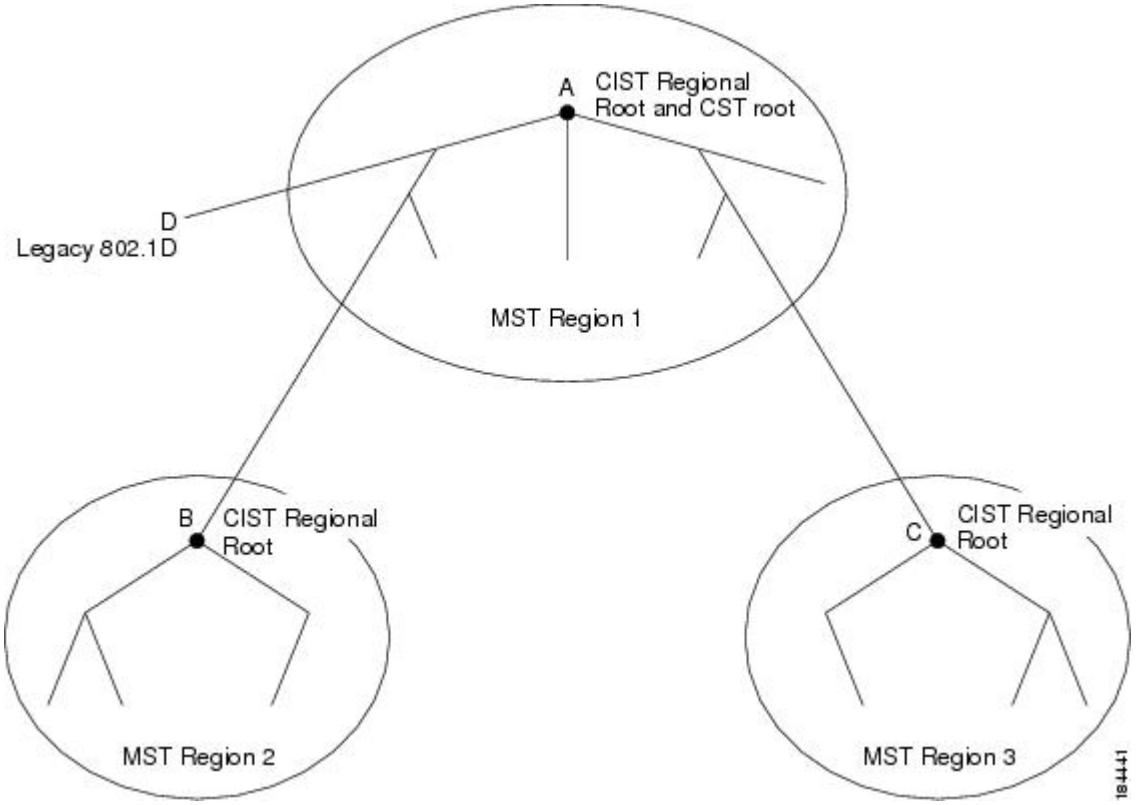
Spanning Tree Operations Between MST Regions

If you have multiple regions or 802.1 w or 802.1D STP instances within a network, MST establishes and maintains the CST, which includes all MST regions and all 802.1w and 802.1D STP devices in the network. The MSTIs combine with the IST at the boundary of the region to become the CST.

The IST connects all the MST devices in the region and appears as a subtree in the CIST that encompasses the entire switched domain. The root of the subtree is the CIST regional root. The MST region appears as a virtual device to adjacent STP devices and MST regions.

This figure shows a network with three MST regions and an 802.1D device (D). The CIST regional root for region 1 (A) is also the CIST root. The CIST regional root for region 2 (B) and the CIST regional root for region 3 (C) are the roots for their respective subtrees within the CIST.

図 *13* : ***MST Regions, CIST Regional Roots, and CST Root***



Only the CST instance sends and receives BPDUs. MSTIs add their spanning tree information into the BPDUs (as M-records) to interact with neighboring devices within the same MST region and compute the final spanning tree topology. The spanning tree parameters related to the BPDU transmission (for example, hello time, forward time, max-age, and max-hops) are configured only on the CST instance but affect all MSTIs. You can configure the parameters related to the spanning tree topology (for example, the switch priority, the port VLAN cost, and the port VLAN priority) on both the CST instance and the MSTI.

MST devices use Version 3 BPDUs. If the MST device falls back to 802.1D STP, the device uses only 802.1D BPDUs to communicate with 802.1D-only devices. MST devices use MST BPDUs to communicate with MST devices.

MST Terminology

MST naming conventions include identification of some internal or regional parameters. These parameters are used only within an MST region, compared to external parameters that are used throughout the whole network. Because the CIST is the only spanning tree instance that spans the whole network, only the CIST parameters require the external qualifiers and not the internal or regional qualifiers. The MST terminology is as follows:

- The CIST root is the root bridge for the CIST, which is the unique instance that spans the whole network.

- The CIST external root path cost is the cost to the CIST root. This cost is left unchanged within an MST region. An MST region looks like a single device to the CIST. The CIST external root path cost is the root path cost calculated between these virtual devices and devices that do not belong to any region.
- If the CIST root is in the region, the CIST regional root is the CIST root. Otherwise, the CIST regional root is the closest device to the CIST root in the region. The CIST regional root acts as a root bridge for the IST.
- The CIST internal root path cost is the cost to the CIST regional root in a region. This cost is only relevant to the IST, instance 0.

Hop Count

MST does not use the message-age and maximum-age information in the configuration BPDU to compute the STP topology inside the MST region. Instead, the protocol uses the path cost to the root and a hop-count mechanism similar to the IP time-to-live (TTL) mechanism.

By using the **spanning-tree mst max-hops** global configuration command, you can configure the maximum hops inside the region and apply it to the IST and all MST instances in that region.

The hop count achieves the same result as the message-age information (triggers a reconfiguration). The root bridge of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count set to the maximum value. When a device receives this BPDU, it decrements the received remaining hop count by one and propagates this value as the remaining hop count in the BPDUs that it generates. When the count reaches zero, the device discards the BPDU and ages the information held for the port.

The message-age and maximum-age information in the 802.1w portion of the BPDU remain the same throughout the region (only on the IST), and the same values are propagated by the region-designated ports at the boundary.

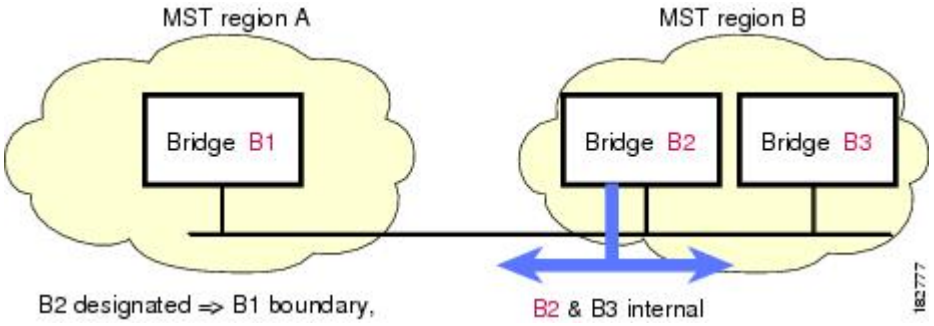
You configure a maximum aging time as the number of seconds that a device waits without receiving spanning tree configuration messages before attempting a reconfiguration.

境界ポート

境界ポートは、LAN に接続されたポートで、その代表ブリッジは、MST 設定が異なるブリッジ（つまり、別の MST 領域）、または Rapid PVST+ や 802.1D STP スイッチのいずれかです。 指定ポートは、STP ブリッジを検出するか、設定が異なる MST ブリッジまたは Rapid PVST+ ブリッジから合意提案を受信すると、境界にあることを認識します。 この定義では、領域内部の 2 つの

ポートが、別の領域に属するポートとセグメントを共有でき、そのため内部メッセージおよび外部メッセージの両方をポートで受信する可能性があります。

図 *14* : *MST* 境界ポート



境界では、MST ポートのロールは問題ではなく、その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。 境界フラグがポートに対してオンに設定されている場合、MST ポートのロールの選択処理では、ポートのロールが境界に割り当てられ、同じステートが IST ポートのステートとして割り当てられます。 境界にある IST ポートでは、バックアップ ポートのロール以外のすべてのポートのロールを引き継ぐことができます。

Detecting Unidirectional Link Failure:MST

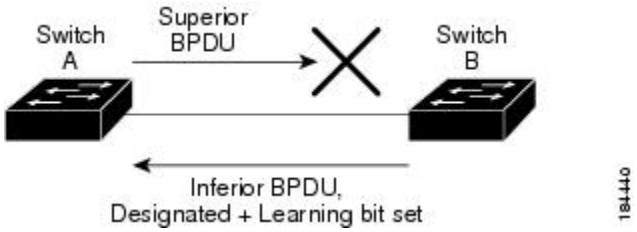
Currently, this feature is not present in the IEEE MST standard, but it is included in the standard-compliant implementation; it is based on the dispute mechanism. The software checks the consistency of the port role and state in the received BPDUs to detect unidirectional link failures that could cause bridging loops. This feature is based on the dispute mechanism.

（注） See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』, for information on Unidirectional Link Detection (UDLD).

When a designated port detects a conflict, it keeps its role, but reverts to a discarding state because disrupting connectivity in case of inconsistency is preferable to opening a bridging loop.

This figure shows a unidirectional link failure that typically creates a bridging loop. Switch A is the root bridge, and its BPDUs are lost on the link leading to switch B. Rapid PVST+ (802.1w) and MST BPDUs include the role and state of the sending port. With this information, switch A can detect that switch B does not react to the superior BPDUs that it sends and that switch B is the designated, not root port. As a result, switch A blocks (or keeps blocking) its port, which prevents the bridging loop.

図 *15* : *Detecting a Unidirectional Link Failure*



Port Cost and Port Priority

Spanning tree uses port costs to break a tie for the designated port. Lower values indicate lower port costs, and spanning tree chooses the least costly path. Default port costs are taken from the bandwidth of the interface, as follows:

- 10 Mbps—2,000,000
- 100 Mbps—200,000
- 1 Gigabit Ethernet—20,000
- 10 Gigabit Ethernet—2,000

You can configure the port costs in order to influence which port is chosen.

（注） MST always uses the long path-cost calculation method, so the range of valid values is between 1 and 200,000,000.

The system uses port priorities to break ties among ports with the same cost. A lower number indicates a higher priority. The default port priority is 128. You can configure the priority to values between 0 and 224, in increments of 32.

Interoperability with IEEE 802.1D

A device that runs MST supports a built-in protocol migration feature that enables it to interoperate with 802.1D STP devices. If this devoce receives an 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only 802.1D BPDUs on that port. In addition, an MST device can detect that a port is at the boundary of a region when it receives an 802.1D BPDU, an MST BPDU (Version 3) associated with a different region, or an 802.1w BPDU (Version 2).

However, the device does not automatically revert to the MST mode if it no longer receives 802.1D BPDUs because it cannot detect whether the 802.1D device has been removed from the link unless the 802.1D device is the designated device. A device might also continue to assign a boundary role to a port when the device to which this device is connected has joined the region.

To restart the protocol migration process (force the renegotiation with neighboring devices), enter the **clear spanning-tree detected-protocols** command.

All Rapid PVST+ switches (and all 8021.D STP switches) on the link can process MST BPDUs as if they are 802.1w BPDUs. MST devices can send either Version 0 configuration and topology change notification (TCN)

BPDUs or Version 3 MST BPDUs on a boundary port. A boundary port connects to a LAN, the designated device of which is either a single spanning tree device or a device with a different MST configuration.

MST interoperates with the Cisco prestandard MSTP whenever it receives prestandard MSTP on an MST port; no explicit configuration is necessary. In Cisco NX-OS Release 4.0(2) and later releases, you can configure specified interfaces to send prestandard MSTP messages all the time; it does not have to wait to receive a prestandard MST message to begin sending prestandard MST messages.

You can also configure the interface to proactively send prestandard MSTP messages.

High Availability for MST

The software supports high availability for MST. However, the statistics and timers are not restored when MST restarts. The timers start again and the statistics begin from 0.

The device supports full nondisruptive upgrades for MST. See the 『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』, for complete information on nondisruptive upgrades and high-availability features.

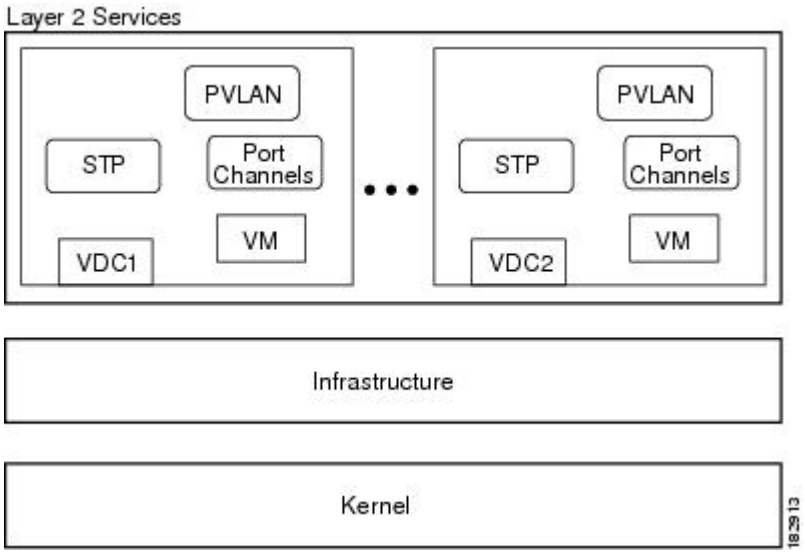
Virtualization Support for MST

The system provides support for virtual device contexts (VDCs), and each VDC runs a separate STP.

You can run Rapid PVST+ in one VDC and run MST in another VDC as shown in this figure. Each VDC will have its own MST. Ensure that you are in the correct VDC.

For example, VDC1 can run MST, VDC2 can run Rapid PVST+, and VDC 3 can run MST.

図 *16*： *Separate STP in each VDC*



（注） MSTs in different VDCs are distinct, so you must perform MST region configuration for each VDC.

（注） See the 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』, for complete information on VDCs and assigning resources.

Licensing Requirements for MST

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	MST requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the 『*Cisco NX-OS Licensing Guide*』.

However, using VDCs requires an Advanced Services license.

Prerequisites for MST

MST has the following prerequisites:

- You must be logged onto the device.
- If necessary, install the Advanced Services license and enter the desired VDC.
- If you are working in another VDC than the default VDC, that VDC must be created.

Guidelines and Limitations for Configuring MST

（注） When you change the VLAN-to-MSTI mapping, the system reconverges MST.

MST has the following configuration guidelines and limitations:

- You must enable MST; Rapid PVST+ is the default spanning tree mode.
- You can assign a VLAN to only one MST instance at a time.
- You cannot map VLANs 3968 to 4047 or 4094 to an MST instance. These VLANs are reserved for internal use by the device.
- You can have up to 65 MST instances on one device.
- The maximum number of VLANs and ports is 75,000.

- By default, all VLANs are mapped to MSTI 0 or the IST.
- When you are working with private VLANs on the system, ensure that all secondary VLANs are mapped to the same MSTI as the primary VLAN.
- You can load balance only within the MST region.
- Ensure that trunks carry all of the VLANs that are mapped to an MSTI or exclude all those VLANs that are mapped to an MSTI.
- Always leave STP enabled.
- Do not change timers because you can adversely affect your network stability.
- Keep user traffic off the management VLAN; keep the management VLAN separate from user data.
- Choose the distribution and core layers as the location of the primary and secondary root switches.
- Port channeling—The port channel bundle is considered as a single port. The port cost is the aggregation of all the configured port costs assigned to that channel.
- When you map a VLAN to an MSTI, the system automatically removes that VLAN from its previous MSTI.
- You can map any number of VLANs to an MSTI.
- All MST boundary ports must be forwarding for load balancing between Rapid PVST+ and an MST cloud or between a PVST+ and an MST cloud. The CIST regional root of the MST cloud must be the root of the CST. If the MST cloud consists of multiple MST regions, one of the MST regions must contain the CST root and all of the other MST regions must have a better path to the root contained within the MST cloud than a path through the Rapid PVST+ or PVST+ cloud.
- Do not partition the network into a large number of regions. However, if this situation is unavoidable, we recommend that you partition the switched LAN into smaller LANs interconnected by non-Layer 2 devices.
- When you work with private VLANs, enter the **private-vlan synchronize** command to map the secondary VLANs to the same MST instance as the primary VLAN.
- When you are in the MST configuration submode, the following guidelines apply:
  - Each command reference line creates its pending regional configuration.
  - The pending region configuration starts with the current region configuration.
  - To leave the MST configuration submode without committing any changes, enter the **abort** command.
  - To leave the MST configuration submode and commit all the changes that you made before you left the submode, enter the **exit** or **end** commands, or press **Ctrl + Z**.

（注） The software supports full nondisruptive upgrades for MST. See 『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』, for complete information about nondisruptive upgrades.

MST のデフォルト設定

次の表に、MST パラメータのデフォルト設定を示します。

表 *17*：デフォルトの *MST* パラメータ

パラメータ	デフォルト
スパニングツリー	イネーブル
スパニングツリー モード	Rapid PVST+ がデフォルトでイネーブル **注意** スパニングツリー モードを変更すると、すべてのスパニングツリー インスタンスが前のモードで停止して新規モードで開始されるため、トラフィックが中断されます。
名前	空の文字列
VLAN マッピング	すべての VLAN を CIST インスタンスにマッピング
リビジョン	0
インスタンス ID	インスタンス 0。VLAN 1 ～ 4094 はデフォルトでインスタンス 0 にマッピングされます。
MST 領域あたりの MSTI 数	65
ブリッジ プライオリティ（CIST ポート単位で設定可能）	32768
スパニングツリー ポート プライオリティ（CIST ポート単位で設定可能）	128
スパニングツリー ポート コスト（CIST ポート単位で設定可能）	Auto デフォルトのポート コストは、次のように、ポート速度から判別されます。 • 10 Mbps：2,000,000 • 100 Mbps：200,000 • 1 ギガビット イーサネット：20,000 • 10 ギガビット イーサネット：2,000

パラメータ	デフォルト
hello タイム	2 秒
転送遅延時間	15 秒
最大エージング タイム	20 秒
最大ホップ カウント	20 ホップ
リンク タイプ	Auto デフォルト リンク タイプは、次のようにデュプレックスから判別されます。 • 全二重：ポイントツーポイント リンク • 半二重：共有リンク

Configuring MST

（注） If you are familiar with the Cisco IOS CLI, be aware that the Cisco software commands for this feature might differ from the Cisco IOS commands that you would use.

MST のイネーブル化（CLI バージョン）

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

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

（注） スパニングツリー モードを変更すると、すべてのスパニングツリー インスタンスが前のモードで停止して新規モードで再開されるため、トラフィックが中断されます。

はじめる前に

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

手順の概要

1. **config t**
2. 次のいずれかのコマンドを入力します。
3. **exit**
4. （任意） **show running-config spanning-tree all**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーションモードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。 **spanning-tree mode mst** — デバイスの MST をイネーブルにします。 **no spanning-tree mode mst** — デバイス上で MST をディセーブルにして、Rapid PVST+ に戻します。 例： `switch(config)# spanning-tree mode mst`	

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

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

次に、デバイス上で MST をイネーブルにする例を示します。

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

MST コンフィギュレーション モードの開始

デバイスに MST 名、VLAN/インスタンス マッピング、および MST リビジョン番号を設定するには、MST コンフィギュレーション モードを開始します。

複数のデバイスが同じ MST 領域内にある場合は、これらのデバイスの MST 名、VLAN/インスタンス マッピング、および MST リビジョン番号を同一にする必要があります。

（注） 各コマンド参照行により、MST コンフィギュレーション モードで保留中の領域設定が作成されます。 さたに、保留中の領域設定により、現在の領域設定が開始されます。

はじめる前に

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

手順の概要

1. **config t**
2. 次のいずれかのコマンドを入力します。
3. 次のいずれかのコマンドを入力します。
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。	

	コマンドまたはアクション	目的

	オプション / **説明**
	spanning-tree mst configuration — システム上で、MST設定サブモードを開始します。次の MST 設定パラメータを割り当てるには、MST 設定サブモードを開始しておく必要があります。
	• MST 名
	• VLAN/MST インスタンス マッピング
	• MST リビジョン番号
	• プライベート VLAN でのプライマリ VLAN とセカンダリ VLAN との同期
	no spanning-tree mst configuration — MST 領域設定を次のデフォルト値に戻します。
	• 領域名は空の文字列になります。
	• VLAN は MSTI にマッピングされません（すべての VLAN は CIST インスタンスにマッピングされます）。
	• リビジョン番号は 0 です。
	例：
	`switch(config)# spanning-tree mst configuration`
	`switch(config-mst)#`	

ステップ 3	次のいずれかのコマンドを入力します。
	オプション / **説明**
	exit — すべての変更をコミットし、MST設定サブモードを終了します。
	abort — いずれの変更もコミットすることなく、MST設定サブモードを終了します。
	例：
	`switch(config-mst)# exit`
	`switch(config)#`	

ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コン

	コマンドまたはアクション	目的
		フィギュレーションにコピーします。

次に、デバイスで MST コンフィギュレーション サブモードを開始する例を示します。

```
switch# spanning-tree mst configuration
switch(config-mst)#
```

MST の名前の指定

ブリッジに領域名を設定できます。 複数のブリッジが同じ MST 領域内にある場合は、これらのブリッジの MST 名、VLAN/インスタンス 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。

はじめる前に

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

手順の概要

1. **config t**
2. **spanning-tree mst configuration**
3. **name** *name*
4. 次のいずれかのコマンドを入力します。
5. （任意） **show spanning-tree mst**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree mst configuration**
	
	例：
	`switch(config)# spanning-tree mst configuration`
	`switch(config-mst)#`
		MST コンフィギュレーション サブモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**name** *name* 例： `switch(config-mst)# name accounting`	MST 領域の名前を指定します。 *name* ストリングには最大 32 文字まで使用でき、大文字と小文字が区別されます。 デフォルトは空の文字列です。

ステップ 4	次のいずれかのコマンドを入力します。
	exit：すべての変更をコミットし、MST 設定サブモードを終了します。
	abort：いずれの変更もコミットすることなく、MST 設定サブモードを終了します。
	
	例：
	`switch(config-mst)# exit`
	`switch(config)#`	

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

次の例は、MST 領域の名前の設定方法を示しています。

```
switch# spanning-tree mst configuration
switch(config-mst)# name accounting
switch(config-mst)#
```

MST 設定のリビジョン番号の指定

リビジョン番号は、ブリッジ上に設定します。 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 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。

はじめる前に

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

手順の概要

1. **config t**
2. **spanning-tree mst configuration**
3. **revision** *version*
4. 次のいずれかのコマンドを入力します。
5. （任意） **show spanning-tree mst**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーションモードを開始します。

ステップ 2	**spanning-tree mst configuration**
	
	例：
	`switch(config)# spanning-tree mst configuration`
	`switch(config-mst)#`
		MST コンフィギュレーション サブモードを開始します。

ステップ 3	**revision** *version* 例： `switch(config-mst)# revision 5`	MST領域のリビジョン番号を指定します。範囲は 0 ～ 65535 で、デフォルト値は 0 です。

ステップ 4	次のいずれかのコマンドを入力します。
	exit：すべての変更をコミットし、MST 設定サブモードを終了します。
	abort：いずれの変更もコミットすることなく、MST 設定サブモードを終了します。
	
	例：
	`switch(config-mst)# exit`
	`switch(config)#`	

ステップ 5	**show spanning-tree mst** 例： `switch# show spanning-tree mst`	（任意） MST 設定を表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、MSTI 領域のリビジョン番号を 5 に設定する例を示します。

```
switch# spanning-tree mst configuration
switch(config-mst)# revision 5
switch(config-mst)#
```

MST 領域での設定の指定

2 台以上のデバイスを同一 MST 領域内に存在させるには、同じ VLAN からインスタンスへのマッピング、同じ構成リビジョン番号、および同じ MST の名前が設定されている必要があります。

領域には、同じ MST 設定の 1 つのメンバーまたは複数のメンバーを存在させることができます。各メンバーでは、IEEE 802.1w RSTP BPDU を処理できる必要があります。 ネットワーク内の MST 領域には、数の制限はありませんが、各領域では、最大 65 までのインスタンスをサポートできます。 VLAN は、一度に 1 つの MST インスタンスに対してのみ割り当てることができます。

はじめる前に

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

手順の概要

1. **config t**
2. **spanning-tree mst configuration**
3. **instance** *instance-id* **vlan** *vlan-range*
4. **name** *name*
5. **revision** *version*
6. 次のいずれかのコマンドを入力します。
7. **show spanning-tree mst**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree mst configuration**
	
	例：
	`switch(config)# spanning-tree mst configuration`
	`switch(config-mst)#`
		MST コンフィギュレーション サブモードを開始します。

ステップ 3	**instance** *instance-id* **vlan** *vlan-range* 例： `switch(config-mst)# instance 1 vlan 10-20`	VLAN を MST インスタンスにマッピングする手順は、次のとおりです。 • *instance-id* の範囲は 1 ～ 4094 です。 • **vlan** *vlan-range* の範囲は 1 ～ 4094 です。 MST インスタンスに VLAN をマッピングする場合、マッピングはインクリメンタルに行われ、コマンドで指定された VLAN がすでにマッピング済みの VLAN に対して追加または削除されます。 VLAN 範囲を指定する場合は、ハイフンを使用します。たとえば、**instance 1 vlan 1-63** とコマンドを入力すると、MST インスタンス 1 に VLAN 1 ～ 63 がマッピングされます。 複数の VLAN を指定する場合はカンマで区切ります。たとえば、**instance 1 vlan 10, 20, 30** と指定すると、MST インスタンス 1 に VLAN 10、20、および 30 がマッピングされます。
ステップ 4	**name** *name* 例： `switch(config-mst)# name region1`	インスタンス名を指定します。 name ストリングには最大 32 文字まで使用でき、大文字と小文字が区別されます。
ステップ 5	**revision** *version* 例： `switch(config-mst)# revision 1`	設定リビジョン番号を指定します。 指定できる範囲は 0 ～ 65535 です。
ステップ 6	次のいずれかのコマンドを入力します。	

	コマンドまたはアクション	目的

	オプション / 説明
	exit / すべての変更をコミットし、MST設定サブモードを終了します。
	abort / いずれの変更もコミットすることなく、MST設定サブモードを終了します。
	
	例：
	`switch(config-mst)# exit`
	`switch(config)#`	

ステップ 7	**show spanning-tree mst** 例： `switch# show spanning-tree mst`	（任意）MST 設定を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例では、MST コンフィギュレーション モードを開始して VLAN 10 ～ 20 を MST インスタンス 1 にマッピングし、リージョンに *region1* と名前を付けて、コンフィギュレーション リビジョンを 1 に設定します。その後、変更確認前の設定を表示して変更を適用し、グローバル コンフィギュレーション モードに戻る方法を示します。

```
switch# spanning-tree mst configuration
switch(config-mst)# instance 1 vlan 10-20
switch(config-mst)# name region1
switch(config-mst)# revision 1
switch(config-mst#) show pending
Pending MST configuration
Name      [region1]
Revision  1
Instances configured 2
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------
switch(config-mst)# exit
switch(config)#
```

VLAN と MST インスタンスのマッピングおよびマッピング解除（CLI バージョン）

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 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 は MST インスタンスにマッピングできません。 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。

はじめる前に

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

手順の概要

1. **config t**
2. **spanning-tree mst configuration**
3. 次のいずれかのコマンドを入力します。
4. 次のいずれかのコマンドを入力します。
5. （任意） **show spanning-tree mst**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree mst configuration**
	
	例：
	`switch(config)# spanning-tree mst configuration`
	`switch(config-mst)#`
		MST コンフィギュレーション サブモードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。	

<table>
<tr><th></th><th>コマンドまたはアクション</th><th>目的</th></tr>
<tr><td></td><td>
<table>
<tr><th>オプション</th><th>説明</th></tr>
<tr><td>instance
instance-id vlan
vlan-range</td><td>VLAN を MST インスタンスにマッピングする手順は、次のとおりです。
• instance_id の範囲は 1 ～ 4094 です。インスタンス 0 は、各 MST 領域での IST 用に予約されています。
• vlan-range の範囲は 1 ～ 4094 です。
VLAN を MSTI にマッピングすると、マッピングは差分で実行され、コマンドで指定された VLAN が、以前マッピングされた VLAN に追加または VLAN から削除されます。</td></tr>
<tr><td>no instance
instance-id vlan
vlan-range</td><td>指定したインスタンスを削除し、VLAN を、デフォルト MSTI である CIST に戻します。</td></tr>
</table>
例：
<pre>switch(config-mst)# instance 3 vlan 200</pre>
</td><td></td></tr>
<tr><td>ステップ 4</td><td>次のいずれかのコマンドを入力します。
<table>
<tr><th>オプション</th><th>説明</th></tr>
<tr><td>exit</td><td>すべての変更をコミットし、MST設定サブモードを終了します。</td></tr>
<tr><td>abort</td><td>いずれの変更もコミットすることなく、MST設定サブモードを終了します。</td></tr>
</table>
例：
<pre>switch(config-mst)# exit
switch(config)#</pre>
</td><td></td></tr>
<tr><td>ステップ 5</td><td>show spanning-tree mst
例：
<pre>switch# show spanning-tree mst</pre></td><td>（任意）
MST 設定を表示します。</td></tr>
<tr><td>ステップ 6</td><td>copy running-config startup-config
例：
<pre>switch(config)# copy running-config startup-config</pre></td><td>（任意）
実行コンフィギュレーションを、スタートアップ コンフィ</td></tr>
</table>

	コマンドまたはアクション	目的
		ギュレーションにコピーします。

次の例は、VLAN 200 を MSTI 3 にマッピングする方法を示しています。

```
switch# config t
switch(config)# spanning-tree mst configuration
switch(config-mst)# instance 3 vlan 200
switch(config-mst)#
```

プライベート VLAN でセカンダリ VLAN をプライマリ VLAN として同じ MSTI にマッピングするには

システムのプライベート VLAN で作業しているときは、関連プライマリ VLAN と同じ MSTI にすべてのセカンダリ VLAN を配置する必要があります。 この同期を自動的に実現するには、**private-vlan synchronize** コマンドを入力します。

はじめる前に

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

手順の概要

1. **config t**
2. **spanning-tree mst configuration**
3. **private-vlan synchronize**
4. 次のいずれかのコマンドを入力します。
5. （任意） **show spanning-tree mst**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**spanning-tree mst configuration**
	
	例：
	`switch(config)# spanning-tree mst configuration`
	`switch(config-mst)#`
		MST コンフィギュレーション サブモードを開始します。

ステップ 3	**private-vlan synchronize** 例： `g-mst)# private-vlan synchronize`	すべてのプライベート VLAN について、関連プライマリ VLAN と同じ MSTI にすべてのセカンダリ VLAN を自動的にマッピングします。

ステップ 4	次のいずれかのコマンドを入力します。
	exit：すべての変更をコミットし、MST 設定サブモードを終了します。
	abort：いずれの変更もコミットすることなく、MST 設定サブモードを終了します。
	
	例：
	`switch(config-mst)# exit`
	`switch(config)#`	

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

次の例は、すべてのプライベート VLAN と同じ MSTI および関連プライマリ VLAN にすべてのセカンダリ VLAN を自動的にマッピングする方法を示しています。

```
switch# config t
switch(conf9g)# spanning-tree mst configuration
switch(config-mst)# private-vlan synchronize
switch(config-mst)#
```

ルート ブリッジの設定

MST ルート ブリッジになるデバイスを設定できます。

ルート ブリッジになるために必要な値が 4096 より小さい場合は、**spanning-tree vlan** *vlan_ID* **primary root** コマンドはエラーになります。 ソフトウェアでブリッジ プライオリティをそれ以上低くできない場合、デバイスは次のメッセージを返します。

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

（注） 各 MSTI のルート ブリッジは、バックボーンまたはディストリビューション デバイスである必要があります。 アクセス デバイスは、スパニングツリーのプライマリ ルート ブリッジとして設定しないでください。

レイヤ 2 ネットワークの直径（レイヤ 2 ネットワーク上の任意の 2 台のエンド ステーション間における最大レイヤ 2 ホップ カウント）を指定するには、MSTI 0（IST）専用の **diameter** キーワードを入力します。 ネットワーク直径を指定すると、デバイスは、その直径のネットワークで最適な hello タイム、転送遅延時間、最大エージング タイムを自動的に設定し、これによって収束時間が大幅に短縮されます。 **hello** キーワードを入力すると、自動的に計算された hello タイムを上書きできます。

（注） ルート ブリッジとして設定されているデバイスでは、hello タイム、転送遅延時間、最大エージング タイムは手動で設定（**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、**spanning-tree mst max-age** の各グローバル コンフィギュレーション コマンドを使用）しないでください。

はじめる前に

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

手順の概要

1. **config t**
2. 次のいずれかのコマンドを入力します。
3. 次のいずれかのコマンドを入力します。
4. （任意） **show spanning-tree mst**
5. （任意） **copy running-config startup-config**

手順の詳細

<table>
<tr><th></th><th>コマンドまたはアクション</th><th>目的</th></tr>
<tr><td>ステップ 1</td><td>config t

例：
<pre>switch# config t
switch(config)#</pre></td><td>コンフィギュレーション モードを開始します。</td></tr>
<tr><td>ステップ 2</td><td>次のいずれかのコマンドを入力します。
<table>
<tr><th>オプション</th><th>説明</th></tr>
<tr><td>spanning-tree mst instance-id root {primary | secondary} [diameter dia [hello-time hello-time]]</td><td>次のようにルート ブリッジとしてデバイスを設定します。
• instance-id には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定します。 有効な範囲は 1 ～ 4094 です。
• diameter net-diameter には、任意の 2 つのエンド ステーション間にレイヤ 2 ホップの最大数を指定します。 デフォルトは 7 です。このキーワードは、MST インスタンス 0 にだけ使用できます。
• hello-time seconds には、ルート ブリッジによって生成された設定メッセージの間隔を秒単位で指定します。 有効な範囲は 1 ～ 10 秒で、デフォルトは 2 秒です。</td></tr>
<tr><td>no spanning-tree mst instance-id root</td><td>スイッチのプライオリティ、範囲、hello タイムをデフォルト値に戻します。</td></tr>
</table>
例：
<pre>switch(config)# spanning-tree mst 5 root primary</pre></td><td></td></tr>
<tr><td>ステップ 3</td><td>次のいずれかのコマンドを入力します。
<table>
<tr><th>オプション</th><th>説明</th></tr>
<tr><td>exit</td><td>すべての変更をコミットし、MST設定サブモードを終了します。</td></tr>
<tr><td>abort</td><td>いずれの変更もコミットすることなく、MST設定サブモードを終了します。</td></tr>
</table></td><td></td></tr>
</table>

	コマンドまたはアクション	目的

	例：
	`switch(config)# exit`
	`switch#`	

ステップ 4	**show spanning-tree mst** 例： `switch# show spanning-tree mst`	（任意） MST 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、デバイスを MSTI 5 のルート スイッチに設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst 5 root primary
switch(config)#
```

MST セカンダリ ルート ブリッジの設定

複数のバックアップルートブリッジを設定するには、複数のデバイスでこのコマンドを使用します。 **spanning-tree mst root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート ブリッジを設定したときに使用したのと同じネットワーク直径と hello タイムの値を入力します。

はじめる前に

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

手順の概要

1. **config t**
2. 次のいずれかのコマンドを入力します。
3. **exit**
4. （任意） **show spanning-tree mst**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。 **オプション** / **説明** **spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia*[**hello-time** *hello-time*]] 次のようにセカンダリ ルート ブリッジとしてデバイスを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 有効な範囲は 1 ～ 4094 です。 • **diameter** *net-diameter* には、任意の 2 つのエンド ステーション間にレイヤ 2 ホップの最大数を指定します。 デフォルトは 7 です。 このキーワードは、MSTインスタンス 0 にだけ使用できます。 • **hello-time** *seconds* には、ルート ブリッジによって生成された設定メッセージの間隔を秒単位で指定します。 有効な範囲は 1 ～ 10 秒で、デフォルトは 2 秒です。 **no spanning-tree mst** *instance-id* **root** スイッチのプライオリティ、範囲、hello タイムをデフォルト値に戻します。 例： `switch(config)# spanning-tree mst 5 root secondary`	

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

ステップ 4	**show spanning-tree mst** 例： `switch# show spanning-tree mst`	（任意） MST 設定を表示します。

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

次に、デバイスを MSTI 5 のセカンダリ ルートスイッチに設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst 5 root secondary
switch(config)#
```

MST スイッチ プライオリティの設定

MST インスタンスのスイッチ プライオリティを設定し、指定デバイスがルート ブリッジとして選択される可能性を高めることができます。

（注） **spanning-tree mst priority** コマンドを使用するときは注意してください。 ほとんどの場合、スイッチのプライオリティを変更するには、**spanning-tree mst root primary** および **spanning-tree mst root secondary** のグローバル コンフィギュレーション コマンドの使用を推奨します。

はじめる前に

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

手順の概要

1. **config t**
2. **spanning-tree mst** *instance-id* **priority** *priority-value*
3. **exit**
4. （任意） **show spanning-tree mst**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree mst** *instance-id* **priority** *priority-value* 例： `switch(config)# spanning-tree mst 5 priority 4096`	次のようにデバイス プライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 有効な範囲は 1 ～ 4094 です。 • *priority-valu* の範囲は 0 ～ 61440 で、4096 ずつ増加します。 デフォルト値は 32768 です。 数値を小さくすると、ルート ブリッジとしてデバイスが選択される可能性が高くなります。 プライオリティ値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。 システムでは、他のすべての値が拒否されます。

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

ステップ 4	**show spanning-tree mst** 例： `switch# show spanning-tree mst`	（任意） MST 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、MSTI 5 のブリッジのプライオリティを 4096 に設定する方法を示しています。

```
switch# config t
switch(config)# spanning-tree mst 5 priority 4096
switch(config)#
```

MST ポート プライオリティの設定

ループが発生する場合、MSTは、フォワーディング ステートにするインターフェイスを選択するとき、ポートプライオリティを使用します。最初に選択させるインターフェイスには低いプライオリティの値を割り当て、最後に選択させるインターフェイスには高いプライオリティの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のプライオリティ値が同一である場合、MSTはインターフェイス番号が最も低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、その他のインターフェイスをブロックします。

はじめる前に

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

手順の概要

1. **config t**
2. **interface** {{*type slot/port*} | {**port-channel** *number*}}
3. **spanning-tree mst** *instance-id* **port-priority** *priority*
4. **exit**
5. （任意） **show spanning-tree mst**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** {{*type slot/port*}	{**port-channel** *number*}}
		
		例：
		`switch(config)# interface ethernet 3/1`
		`switch(config-if)#`
			設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**spanning-tree mst** *instance-id* **port-priority** *priority* 例： `switch(config-if)# spanning-tree mst 3 port-priority 64`	次のように、ポートのプライオリティを設定します。 • *instance-id* には、1 つの MSTI、それぞれをハイフンで区切った MSTI の範囲、またはカンマで区切った一連の MSTI を指定できます。 有効な範囲は 1 ～ 4094 です。

	コマンドまたはアクション	目的
		• *priority* の範囲は 0 ～ 224 で、32 ずつ増加します。 デフォルトは 128 です。 値が小さいほど、プライオリティが高いことを示します。 プライオリティ値は、0、32、64、96、128、160、192、224 です。 システムでは、他のすべての値が拒否されます。

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

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

次の例は、イーサネット ポート 3/1 で MSTI 3 の MST インターフェイス ポート プライオリティを 64 に設定する方法を示しています。

```
switch# config t
switch(config)# interface ethernet 3/1
switch(config-if)# spanning-tree mst 3 port-priority 64
switch(config-if)# exit
switch(config)#
```

MST ポート コストの設定

MST ポート コストのデフォルト値は、インターフェイスのメディア速度から抽出されます。ループが発生した場合、MST は、コストを使用して、フォワーディング ステートにするインターフェイスを選択します。 最初に選択させるインターフェイスには小さいコストの値を割り当て、最後に選択させるインターフェイスの値には大きいコスト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のコスト値が同一である場合、MST はインターフェイス番号が最も低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、その他のインターフェイスをブロックします。

（注） MST はロング パスコスト計算方式を使用します。

はじめる前に

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

手順の概要

1. **config t**
2. **interface** {{*type slot/port*} | {**port-channel** *number*}}
3. **spanning-tree mst** *instance-id* **cost** {*cost* | *auto*}
4. **exit**
5. （任意） **show spanning-tree mst**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** {{*type slot/port*}	{**port-channel** *number*}}
		
		例：
		`switch# config t`
		`switch(config)# interface ethernet 3/1`
		`switch(config-if)#`
			設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**spanning-tree mst** *instance-id* **cost** {*cost*	*auto*} 例： `switch(config-if)# spanning-tree mst 4 cost 17031970`	コストを設定します。 ループが発生する場合、MST は、フォワーディング ステートにするインターフェイスを選択するとき、パス コストを使用します。パス コストが小さいほど、送信速度が速いことを示します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。有効な範囲は 1 ～ 4094 です。 • *cost* の範囲は 1 ～ 200000000 です。デフォルト値は **auto** で、インターフェイスのメディア速度から取得されるものです。

	コマンドまたはアクション	目的

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

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

次の例は、イーサネット ポート 3/1 で MSTI 4 の MST インターフェイス ポート コストを設定する方法を示しています。

```
switch# config t
switch(config)# interface ethernet 3/1
switch(config-if)# spanning-tree mst 4 cost 17031970
switch(config-if)# exit
switch(config)#
```

MST hello タイムの設定

デバイス上のすべてのインスタンスに対してルート ブリッジが作成する設定メッセージの間隔を設定するには、hello タイムを変更します。

（注） **spanning-tree mst hello-time** コマンドを使用するときは注意してください。 ほとんどの場合、hello タイムを変更するには、**spanning-tree mst** *instance-id* **root primary** および **spanning-tree mst** *instance-id* **root secondary** のグローバル コンフィギュレーション コマンドの使用を推奨します。

はじめる前に

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

手順の概要

1. **config t**
2. **spanning-tree mst hello-time** *seconds*
3. **exit**
4. （任意） **show spanning-tree mst**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree mst hello-time** *seconds* 例： `switch(config)# spanning-tree mst hello-time 1`	すべての MST インスタンスについて、hello タイムを設定します。 hello タイムは、ルート ブリッジが設定メッセージを生成する時間です。 これらのメッセージは、デバイスが動作していることを示します。 *seconds* の範囲は 1 ～ 10 で、デフォルトは 2 秒です。

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

ステップ 4	**show spanning-tree mst** 例： `switch# show spanning-tree mst`	（任意） MST 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、デバイスの hello タイムを 1 秒に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst hello-time 1
switch(config)#
```

MST 転送遅延時間の設定

デバイスのすべての MST インスタンスの転送遅延時間を 1 つのコマンドで設定できます。

はじめる前に

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

手順の概要

1. **config t**
2. **spanning-tree mst forward-time** *seconds*
3. **exit**
4. （任意） **show spanning-tree mst**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree mst forward-time** *seconds* 例： `switch(config)# spanning-tree mst forward-time 10`	すべての MST インスタンスについて、転送時間を設定します。 転送遅延は、スパニングツリー ブロッキング ステートとラーニング ステートからフォワーディング ステートに変更する前に、ポートが待つ秒数です。 *seconds* の範囲は 4 ～ 30 で、デフォルトは 15 秒です。

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

ステップ 4	**show spanning-tree mst** 例： `switch# show spanning-tree mst`	（任意） MST 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、デバイスの転送遅延時間を 10 秒に設定する例を示します。

```
switch# config t
switch(config)# spanning-time mst forward-time 10
switch(config)#
```

MST 最大エージング タイムの設定

デバイスのすべての MST インスタンスの最大エージング タイマーを 1 つのコマンドで設定できます（最大エージング タイムが適用されるのは IST のみです）。

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

はじめる前に

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

手順の概要

1. **config t**
2. **spanning-tree mst max-age** *seconds*
3. **exit**
4. （任意） **show spanning-tree mst**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree mst max-age** *seconds* 例： `switch(config)# spanning-tree mst max-age 40`	すべての MST インスタンスについて、最大経過時間を設定します。 最大エージング タイムは、デバイスがスパニングツリー設定メッセージを受信せずに再設定を試行するまで待機する秒数です。 *seconds* の範囲は 6 ～ 40 で、デフォルトは 20 秒です。

	コマンドまたはアクション	目的

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

ステップ 4	**show spanning-tree mst** 例： `switch# show spanning-tree mst`	（任意） MST 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、デバイスの最大エージング タイマーを 40 秒に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst max-age 40
switch(config)#
```

MST 最大ホップ カウントの設定

領域内の最大ホップを設定し、それをその領域内にある IST およびすべての MST インスタンスに適用できます。 MST では、IST リージョナル ルートへのパス コストと、IP の存続可能時間（TTL）メカニズムに類似したホップ カウント メカニズムが、使用されます。 ホップ カウントを設定すると、メッセージ エージ情報を設定するのと同様の結果が得られます（再構成の開始時期を決定します）。

はじめる前に

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

手順の概要

1. **config t**
2. **spanning-tree mst max-hops** *hop-count*
3. **exit**
4. （任意） **show spanning-tree mst**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree mst max-hops** *hop-count* 例： `switch(config)# spanning-tree mst max-hops 40`	BPDUが廃棄され、ポートに維持されていた情報が期限切れになるまでの、領域内でのホップ カウントを指定します。 *hop-count* の範囲は 1 ～ 255 で、デフォルト値は 20 ホップです。

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

ステップ 4	**show spanning-tree mst** 例： `switch# show spanning-tree mst`	（任意） MST 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、最大ホップ カウントを 40 に設定する方法を示しています。

```
switch# config t
switch(config)# spanning-tree mst max-hops 40
switch(config)#
```

先行標準 MSTP メッセージを事前に送信するインターフェイスの設定（CLI バージョン）

デフォルトで、MST を実行中のデバイス上のインターフェイスは、別のインターフェイスから先行標準 MSTP メッセージを受信したあと、標準ではなく先行標準の MSTP メッセージを送信します。 Cisco NX-OS Release 4.0(2) 以降のリリースでは、先行標準 MSTP メッセージを事前に送信するインターフェイスを設定できるようになりました。 つまり、指定されたインターフェイスは、先行標準 MSTP メッセージの受信を待機する必要がなく、この設定のインターフェイスは常に先行標準 MSTP メッセージを送信します。

はじめる前に

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

手順の概要

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree mst pre-standard** [**interface** {{ *type slot/port*} | {**port-channel** *number*}}] [**detail**]
4. **exit**
5. （任意） **show spanning-tree mst**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**spanning-tree mst pre-standard** [**interface** {{ *type slot/port*}	{**port-channel** *number*}}] [**detail**] 例： `switch(config-if)# spanning-tree mst pre-standard`	インターフェイスが MSTP 標準形式ではなく、先行標準形式の MSTP メッセージを常に送信するように指定します。

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

ステップ 5	**show spanning-tree mst** 例： `switch# show spanning-tree mst`	（任意） MST 設定を表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、MSTP メッセージを常に先行標準形式で送信するように、MST インターフェイスを設定する例を示します。

```
switch# config t
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree mst pre-standard
switch(config-if)# exit
switch(config)#
```

MST のリンク タイプの指定（CLI バージョン）

Rapid の接続性（802.1w 規格）は、ポイントツーポイントのリンク上でのみ確立されます。 リンク タイプは、デフォルトでは、インターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続であると見なされ、半二重ポートは共有接続であると見なされます。

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。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**spanning-tree link-type** {*auto* | *point-to-point* | *shared*} 例： `switch(config-if)# spanning-tree link-type point-to-point`	リンク タイプを、ポイントツーポイント インクまたは共有リンクに設定します。 デフォルト値はデバイス接続から読み取られ、半二重リンクは共有、全二重リンクはポイントツーポイントです。 リンク タイプが共有の場合、STP は 802.1D にフォール バックします。 デフォルトは auto で、インターフェイスのデュプレックス設定に基づいてリンク タイプが設定されます。

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

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

次の例は、リンク タイプをポイントツーポイント リンクとして設定する方法を示しています。

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

MST 用のプロトコルの再初期化

MST ブリッジでは、レガシー BPDU または異なる領域にアソシエートされている MST BPDU 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、STP プロトコルを移行しても、レガシー デバイス（IEEE 802.1D だけが稼働するデバイス）が代表スイッチでないかぎり、レガシーデバイスがリンクから削除されたかどうかを判別することはできません。デバイス全体で、または指定されたインターフェイスでプロトコル ネゴシエーションを再初期化する（ネイバー デバイスとの再ネゴシエーションを強制的に行う）には、次のコマンドを入力します。

はじめる前に

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

手順の概要

1. **clear spanning-tree detected-protocol** [**interface** *interface* [*interface-num* | *port-channel*]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear spanning-tree detected-protocol** [**interface** *interface* [*interface-num* | *port-channel*]] 例： `switch# clear spanning-tree detected-protocol`	デバイス全体または指定されたインターフェイスで、MST を再初期化します。

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

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

MST 設定の確認

MST の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config spanning-tree [**all**]	STP 情報を表示します。
show spanning-tree mst configuration	MST 情報を表示します。
show spanning-tree mst [**detail**]	MST インスタンスの情報を表示します。

コマンド	目的
show spanning-tree mst *instance-id* [**detail**]	指定された MST インスタンスに関する情報を表示します。
show spanning-tree mst *instance-id* **interface** {**ethernet** *slot/port* | **port-channel** *channel-number*} [**detail**]	指定したインターフェイスおよびインスタンスの MST 情報を表示します。
show spanning-tree summary	STP の概要を表示します。
show spanning-tree detail	STP の詳細を表示します。
show spanning-tree {**vlan** *vlan-id* | **interface** {[**ethernet** *slot/port*] | [**port-channel** *channel-number*]}} [**detail**]	VLAN またはインターフェイス単位の STP 情報を表示します。
show spanning-tree vlan *vlan-id* **bridge**	STP ブリッジの情報を表示します。

これらのコマンド出力の詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』を参照してください。

MST 統計情報の表示およびクリア（CLI バージョン）

MST の設定情報を表示するには、次のいずれかの作業を行います。

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

MST の設定例

次に、MST を設定する例を示します。

```
switch# configure terminal
switch(config)# spanning-tree mode mst
switch(config)# spanning-tree port type edge bpduguard default
switch(config)# spanning-tree port type edge bpdufilter default
switch(config)# spanning-tree port type network default
switch(config)# spanning-tree mst 0-64 priority 24576
switch(config)# spanning-tree mst configuration
switch(config-mst)# name cisco_region_1
```

```
switch(config-mst)# revision 2
switch(config-mst)# instance 1 vlan 1-21
switch(config-mst)# instance 2 vlan 22-42
switch(config-mst)# instance 3 vlan 43-63
switch(config-mst)# instance 4 vlan 64-84
switch(config-mst)# instance 5 vlan 85-105
switch(config-mst)# instance 6 vlan 106-126
switch(config-mst)# instance 6 vlan 106-126
switch(config-mst)# instance 7 vlan 127-147
switch(config-mst)# instance 8 vlan 148-168
switch(config-mst)# instance 9 vlan 169-189
switch(config-mst)# instance 10 vlan 190-210
switch(config-mst)# instance 11 vlan 211-231
switch(config-mst)# instance 12 vlan 232-252
switch(config-mst)# instance 13 vlan 253-273
switch(config-mst)# instance 14 vlan 274-294
switch(config-mst)# instance 15 vlan 295-315
switch(config-mst)# instance 16 vlan 316-336
switch(config-mst)# instance 17 vlan 337-357
switch(config-mst)# instance 18 vlan 358-378
switch(config-mst)# instance 19 vlan 379-399
switch(config-mst)# instance 20 vlan 400-420
switch(config-mst)# instance 21 vlan 421-441
switch(config-mst)# instance 22 vlan 442-462
switch(config-mst)# instance 23 vlan 463-483
switch(config-mst)# instance 24 vlan 484-504
switch(config-mst)# instance 25 vlan 505-525
switch(config-mst)# instance 26 vlan 526-546
switch(config-mst)# instance 27 vlan 547-567
switch(config-mst)# instance 28 vlan 568-588
switch(config-mst)# instance 29 vlan 589-609
switch(config-mst)# instance 30 vlan 610-630
switch(config-mst)# instance 31 vlan 631-651
switch(config-mst)# instance 32 vlan 652-672
switch(config-mst)# instance 33 vlan 673-693
switch(config-mst)# instance 34 vlan 694-714
switch(config-mst)# instance 35 vlan 715-735
switch(config-mst)# instance 36 vlan 736-756
switch(config-mst)# instance 37 vlan 757-777
switch(config-mst)# instance 38 vlan 778-798
switch(config-mst)# instance 39 vlan 799-819
switch(config-mst)# instance 40 vlan 820-840
switch(config-mst)# instance 41 vlan 841-861
switch(config-mst)# instance 42 vlan 862-882
switch(config-mst)# instance 43 vlan 883-903
switch(config-mst)# instance 44 vlan 904-924
switch(config-mst)# instance 45 vlan 925-945
switch(config-mst)# instance 46 vlan 946-966
switch(config-mst)# instance 47 vlan 967-987
switch(config-mst)# instance 48 vlan 988-1008
switch(config-mst)# instance 49 vlan 1009-1029
switch(config-mst)# instance 50 vlan 1030-1050
switch(config-mst)# instance 51 vlan 1051-1071
switch(config-mst)# instance 52 vlan 1072-1092
switch(config-mst)# instance 53 vlan 1093-1113
switch(config-mst)# instance 54 vlan 1114-1134
switch(config-mst)# instance 55 vlan 1135-1155
switch(config-mst)# instance 56 vlan 1156-1176
switch(config-mst)# instance 57 vlan 1177-1197
switch(config-mst)# instance 58 vlan 1198-1218
switch(config-mst)# instance 59 vlan 1219-1239
switch(config-mst)# instance 60 vlan 1240-1260
switch(config-mst)# instance 61 vlan 1261-1281
switch(config-mst)# instance 62 vlan 1282-1302
switch(config-mst)# instance 63 vlan 1303-1323
switch(config-mst)# instance 64 vlan 1324-1344
switch(config-mst)# exit

switch(config)# interface ethernet 3/1
switch(config-if)# switchport
```

```
switch(config-if)# no shutdown
switch(config-if)# spanning-tree port type edge
switch(congig-if)# exit

switch(config)# interface ethernet 3/2
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# no shutdown
switch(config-if)# spanning-tree guard root
switch(config-if)# exit
switch(config)#
```

MST の追加情報（CLI バージョン）

関連資料

関連項目	参照先
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』
レイヤ 2 インターフェイス	『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』
NX-OS の基礎	『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x*』
ハイ アベイラビリティ	『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』
システム管理	『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x*』
仮想デバイス コンテキスト（VDC）	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.x*』

標準

標準	タイトル
IEEE 802.1Q-2006（旧称 IEEE 802.1s）、IEEE 802.1D-2004（旧称 IEEE 802.1w）、IEEE 802.1D、IEEE 802.1t	—

MIB

MIB	MIB のリンク
• CISCO-STP-EXTENSION-MIB • BRIDGE-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

MST 設定の機能履歴（CLI バージョン）

次の表に、この機能のリリースの履歴を示します。

表 *18* : *MST* 設定の機能履歴

機能名	リリース	機能情報
変更なし	4.2(1)	--
変更なし	4.1(2)	--

第 9 章

Cisco NX-OS を使用した STP 拡張の設定

この章では、Cisco NX-OS デバイスでスパニングツリー プロトコル（STP）拡張機能を設定する方法について説明します。

この章は、次の内容で構成されています。

- Information About STP Extensions, 189 ページ
- Licensing Requirements for STP Extensions, 196 ページ
- Prerequisites for STP Extensions, 197 ページ
- Guidelines and Limitations for Configuring STP Extensions, 197 ページ
- STP 拡張機能のデフォルト設定, 198 ページ
- Configuring STP Extensions Steps, 199 ページ
- STP 拡張機能の設定の確認, 221 ページ
- STP 拡張機能の設定例, 221 ページ
- STP 拡張機能の追加情報（CLI バージョン）, 221 ページ
- STP 拡張機能の設定の機能履歴（CLI バージョン）, 222 ページ

Information About STP Extensions

（注） See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』, for information on creating Layer 2 interfaces.

Cisco has added extensions to STP that enhances loop prevention, protects against some possible user misconfigurations, and provides better control over the protocol parameters. Although, in some cases, similar functionality may be incorporated into the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) standard, we recommend using these extensions. All of these extensions, except PVST Simulation, can be used with both Rapid PVST+ and MST. You use PVST Simulation only with MST.

The available extensions are spanning tree edge ports (which supply the functionality previously known as PortFast), Bridge Assurance, BPDU Guard, BPDU Filtering, Loop Guard, Root Guard, and PVT Simulation. Many of these features can be applied either globally or on specified interfaces.

（注） Spanning tree is used to refer to IEEE 802.1w and IEEE 802.1s. If the text is discussing the IEEE 802.1D Spanning Tree Protocol, 802.1D is stated specifically.

STP Port Types

You can configure a spanning tree port as an edge port, a network port, or a normal port. A port can be in only one of these states at a given time. The default spanning tree port type is normal.

Edge ports, which are connected to Layer 2 hosts, can be either an access port or a trunk port.

（注） If you configure a port connected to a Layer 2 switch or bridge as an edge port, you might create a bridging loop.

Network ports are connected only to Layer 2 switches or bridges.

（注） If you mistakenly configure ports that are connected to Layer 2 hosts, or edge devices, as spanning tree network ports, those ports will automatically move into the blocking state.

STP Edge Ports

You connect STP edge ports only to Layer 2 hosts. The edge port interface immediately transitions to the forwarding state, without moving through the blocking or learning states. (This immediate transition was previously configured as the Cisco-proprietary feature PortFast.)

Interfaces that are connected to Layer 2 hosts should not receive STP bridge protocol data units (BPDUs).

Bridge Assurance

You can use Bridge Assurance to protect against certain problems that can cause bridging loops in the network. Specifically, you use Bridge Assurance to protect against a unidirectional link failure or other software failure and a device that continues to forward data traffic when it is no longer running the spanning tree algorithm.

（注） Bridge Assurance is supported only by Rapid PVST+ and MST.

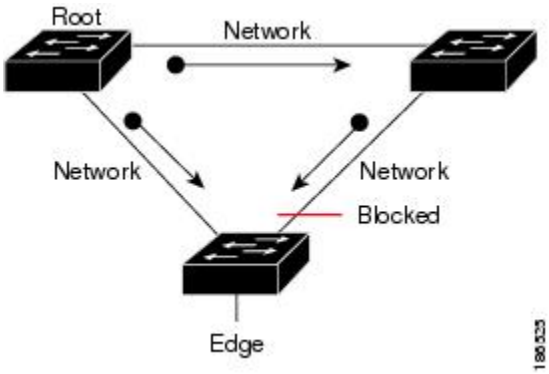
Bridge Assurance is enabled by default and can only be disabled globally. Also, Bridge Assurance can be enabled only on spanning tree network ports that are point-to-point links. Finally, both ends of the link must have Bridge Assurance enabled. If the device on one side of the link has Bridge Assurance enabled and the

device on the other side either does not support Bridge Assurance or does not have this feature enabled, the connecting port is blocked.

With Bridge Assurance enabled, BPDUs are sent out on all operational network ports, including alternate and backup ports, for each hello time period. If the port does not receive a BPDU for a specified period, the port moves into the blocking state and is not used in the root port calculation. Once that port receives a BPDU, it resumes the normal spanning tree transitions.

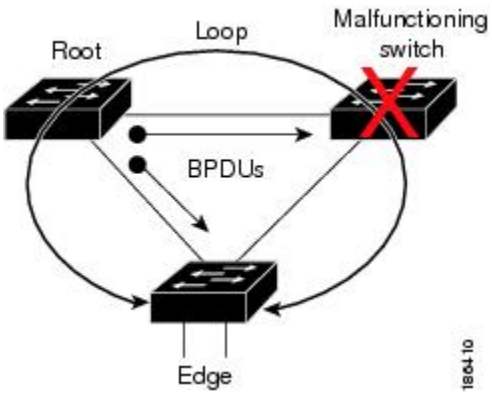
This figure shows a normal STP topology.

図 *17*： *Network with Normal STP Topology*



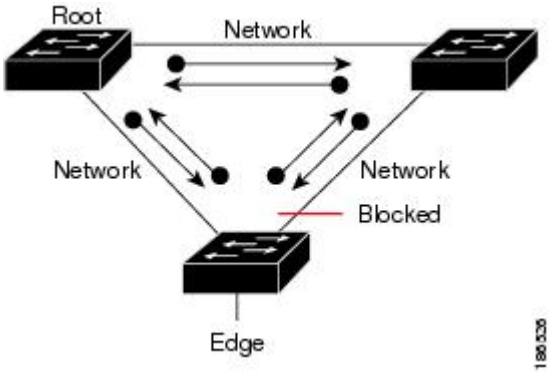
This figure demonstrates a potential network problem when the device fails and you are not running Bridge Assurance.

図 *18*： *Network Problem without Running Bridge Assurance*



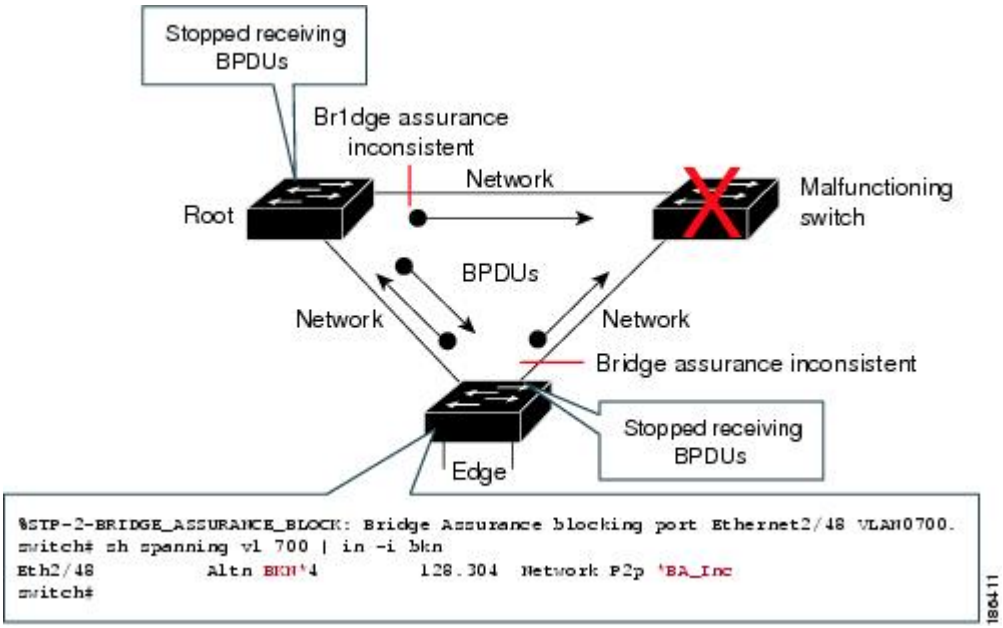
This figure shows the network with Bridge Assurance enabled, and the STP topology progressing normally with bidirectional BPDUs issuing from every STP network port.

図 *19* : ***Network STP Topology Running Bridge Assurance***



This figure shows how the potential network problem does not happen when you have Bridge Assurance enabled on your network.

図 *20* : ***Network Problem Averted with Bridge Assurance Enabled***



BPDU ガード

BPDU ガードをイネーブルにすると、BPDU を受信したときにそのインターフェイスがシャットダウンされます。

BPDU ガードはインターフェイス レベルで設定できます。 BPDU ガードをインターフェイス レベルで設定すると、そのポートはポート タイプ設定にかかわらず BPDU を受信するとすぐにシャットダウンされます。

BPDU ガードをグローバル単位で設定すると、動作中のスパニング ツリー エッジ ポート上だけで有効となります。 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単位でイネーブルにすると、BPDU を受信したすべてのスパニング ツリー エッジ ポートがシャットダウンされます。

BPDU ガードでは、無効な設定が通知された場合、レイヤ 2 LAN インターフェイスを手動で再起動させる必要があるので、無効な設定に対して安全に対応できます。

（注） BPDU ガードをグローバル単位でイネーブルにすると、動作中のすべてのスパニング ツリー エッジ インターフェイスに適用されます。

BPDU フィルタリング

BPDU フィルタリングを使用すると、デバイスの特定のポート上で BPDU が送信されないように、または BPDU を受信しないように設定できます。

グローバルに設定された BPDU フィルタリングは、動作中のすべてのスパニング ツリー エッジ ポートに適用されます。エッジポートはホストだけに接続してください。ホストでは通常、BPDU は破棄されます。 動作中のスパニング ツリー エッジ ポートが BPDU を受信すると、ただちに標準のスパニング ツリー ポート タイプに戻り、通常のポート状態遷移が行われます。 その場合、当該ポートで BPDU フィルタリングはディセーブルとなり、スパニング ツリーによって、同ポートでの BPDU の送信が再開されます。

BPDU フィルタリングは、インターフェイスごとに設定することもできます。 BPDU フィルタリングを特定のポートに明示的に設定すると、そのポートは BPDU を送出しなくなり、受信した BPDU をすべてドロップします。 特定のインターフェイスを設定することによって、個々のポート上のグローバルな BPDU フィルタリングの設定を実質的に上書きできます。 このようにインターフェイスに対して実行された BPDU フィルタリングは、そのインターフェイスがトランキングであるか否かに関係なく、インターフェイス全体に適用されます。

注意 BPDU フィルタリングをインターフェイスごとに設定するときは注意が必要です。 ホストに接続されていないポートに BPDU フィルタリングを明示的に設定すると、ブリッジング ループに陥る可能性があります。このようなポートは受信した BPDU をすべて無視して、フォワーディング ステートに移行するからです。

次の表に、すべての BPDU フィルタリングの組み合わせを示します。

表 *19* : *BPDU* フィルタリングの設定

ポート単位の BPDU フィルタリングの設定	グローバルな BPDU フィルタリングの設定	STP エッジ ポート設定	BPDU フィルタリングの状態
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	N/A	ディセーブル
ディセーブル	N/A	N/A	ディセーブル
イネーブル	N/A	N/A	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 10 以上の BPDU を送信します。 このポートは、BPDU を受信すると、スパニング ツリー標準ポート状態に戻り、BPDU フィルタリングはディセーブルになります。

Loop Guard

Loop Guard helps prevent bridging loops that could occur because of a unidirectional link failure on a point-to-point link.

An STP loop occurs when a blocking port in a redundant topology erroneously transitions to the forwarding state. Transitions are usually caused by a port in a physically redundant topology (not necessarily the blocking port) that stops receiving BPDUs.

When you enable Loop Guard globally, it is useful only in switched networks where devices are connected by point-to-point links. On a point-to-point link, a designated bridge cannot disappear unless it sends an inferior BPDU or brings the link down. However, you can enable Loop Guard on shared links per interface,

You can use Loop Guard to determine if a root port or an alternate/backup root port receives BPDUs. If the port that was previously receiving BPDUs is no longer receiving BPDUs, Loop Guard puts the port into an inconsistent state (blocking) until the port starts to receive BPDUs again. If such a port receives BPDUs again, the port—and link—is deemed viable again. The protocol removes the loop-inconsistent condition from the port, and the STP determines the port state because the recovery is automatic.

Loop Guard isolates the failure and allows STP to converge to a stable topology without the failed link or bridge. Disabling Loop Guard moves all loop-inconsistent ports to the listening state.

You can enable Loop Guard on a per-port basis. When you enable Loop Guard on a port, it is automatically applied to all of the active instances or VLANs to which that port belongs. When you disable Loop Guard, it is disabled for the specified ports.

Enabling Loop Guard on a root device has no effect but provides protection when a root device becomes a nonroot device.

Root Guard

When you enable Root Guard on a port, Root Guard does not allow that port to become a root port. If a received BPDU triggers an STP convergence that makes that designated port become a root port, that port is put into a root-inconsistent (blocked) state. After the port stops sending superior BPDUs, the port is unblocked again. Through STP, the port moves to the forwarding state. Recovery is automatic.

When you enable Root Guard on an interface, this functionality applies to all VLANs to which that interface belongs.

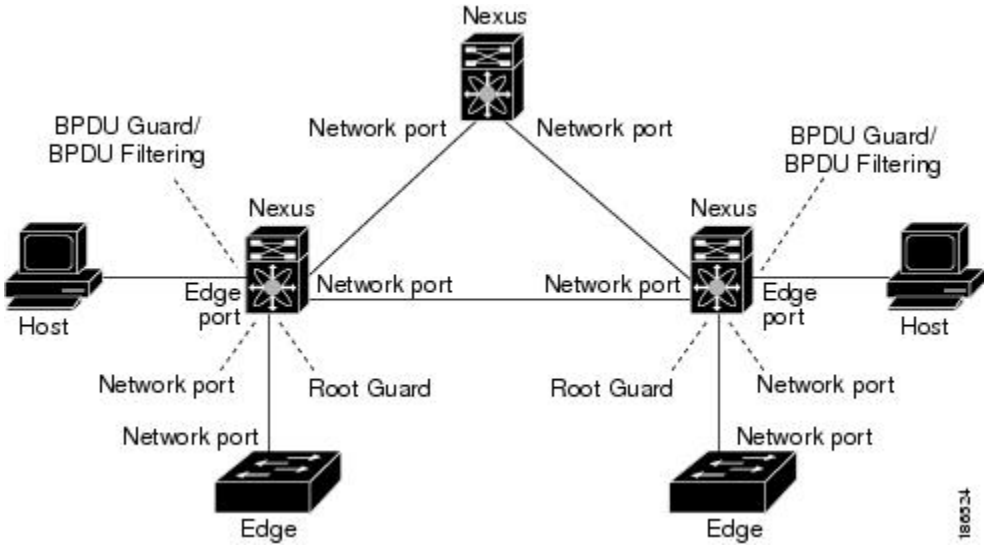
You can use Root Guard to enforce the root bridge placement in the network. Root Guard ensures that the port on which Root Guard is enabled is the designated port. Normally, root bridge ports are all designated ports, unless two or more of the ports of the root bridge are connected. If the bridge receives superior BPDUs on a Root Guard-enabled port, the bridge moves this port to a root-inconsistent STP state. In this way, Root Guard enforces the position of the root bridge.

You cannot configure Root Guard globally.

STP 拡張機能の適用

この図に示すように、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。 Bridge Assurance 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上で、BPDU ガードと BPDU フィルタリングのいずれかをイネーブルにすることをお勧めします。

図 *21*： *STP* 拡張機能を適正に展開したネットワーク



PVST Simulation

MST interoperates with Rapid PVST+ with no need for user configuration. The PVST simulation feature enables this interoperability.

（注） PVST simulation is enabled by default when you enable MST. By default, all interfaces on the device interoperate between MST and Rapid PVST+.

However, you may want to control the connection between MST and Rapid PVST+ to protect against accidentally connecting an MST-enabled port to a port enabled to run Rapid PVST+. Because Rapid PVST+ is the default STP mode, you may encounter many Rapid PVST+ connections.

Disabling Rapid PVST+ simulation, which can be done per port or globally for the entire device, moves the MST-enabled port to the blocking state once it detects it is connected to a Rapid PVST+-enabled port. This port remains in the inconsistent state until the port stops receiving Rapid PVST+/SSTP BPDUs, and then the port resumes the normal STP transition process.

The root bridge for all STP instances must all be in either the MST region or the Rapid PVST+ side. If the root bridge for all STP instances are not on one side or the other, the software moves the port into a PVST simulation-inconsistent state.

（注） We recommend that you put the root bridge for all STP instances in the MST region.

High Availability for STP

The software supports high availability for STP. However, the statistics and timers are not restored when STP restarts. The timers start again and the statistics begin from 0.

（注） See the 『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』, for complete information on high-availability features.

Virtualization Support for STP Extensions

The system provides support for virtual device contexts (VDCs), and each VDC runs a separate STP. You can run Rapid PVST+ in one VDC and MST in another VDC.

（注） See the 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』, for complete information on VDCs and assigning resources.

Licensing Requirements for STP Extensions

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	STP extensions require no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see 『*Cisco NX-OS Licensing Guide*』.

However, using VDCs requires an Advanced Services license.

Prerequisites for STP Extensions

STP has the following prerequisites:

- You must be logged onto the device.
- You must have STP configured already.
- If necessary, install the Advanced Services license and enter the desired VDC.

Guidelines and Limitations for Configuring STP Extensions

STP extensions have the following configuration guidelines and limitations:

- Connect STP network ports only to switches.
- You should configure host ports as STP edge ports and not as network ports.
- If you enable STP network port types globally, ensure that you manually configure all ports connected to hosts as STP edge ports.
- You should configure all access and trunk ports connected to Layer 2 hosts as edge ports.
- Bridge Assurance runs only on point-to-point spanning tree network ports. You must configure each side of the link for this feature.
- We recommend that you enable Bridge Assurance throughout your network.
- We recommend that you enable BPDU Guard on all edge ports.
- Enabling Loop Guard globally works only on point-to-point links.
- Enabling Loop Guard per interface works on both shared and point-to-point links.
- Root Guard forces a port to always be a designated port; it does not allow a port to become a root port. Loop Guard is effective only if the port is a root port or an alternate port. You cannot enable Loop Guard and Root Guard on a port at the same time.
- Loop Guard has no effect on a disabled spanning tree instance or a VLAN.

- Spanning tree always chooses the first operational port in the channel to send the BPDUs. If that link becomes unidirectional, Loop Guard blocks the channel, even if other links in the channel are functioning properly.
- If you group together a set of ports that are already blocked by Loop Guard to form a channel, spanning tree loses all the state information for those ports and the new channel port may obtain the forwarding state with a designated role.
- If a channel is blocked by Loop Guard and the channel members go back to an individual link status, spanning tree loses all the state information. The individual physical ports may obtain the forwarding state with the designated role, even if one or more of the links that formed the channel are unidirectional.

（注） You can enable UniDirectional Link Detection (UDLD) aggressive mode to isolate the link failure. A loop may occur until UDLD detects the failure, but Loop Guard will not be able to detect it. See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』, for information on UDLD.

- You should enable Loop Guard globally on a switch network with physical loops.
- You should enable Root Guard on ports that connect to network devices that are not under direct administrative control.

STP 拡張機能のデフォルト設定

次の表に、STP 拡張機能のデフォルト設定を示します。

表 *20*：*STP* 拡張機能パラメータのデフォルト設定

パラメータ	デフォルト
ポート タイプ	標準
Bridge Assurance	イネーブル（STP ネットワーク ポートのみ）
グローバル BPDU ガード	ディセーブル
インターフェイス単位の BPDU ガード	ディセーブル
グローバル BPDU フィルタリング	ディセーブル
インターフェイス単位の BPDU フィルタリング	ディセーブル
グローバル ループ ガード	ディセーブル
インターフェイス単位のループ ガード	ディセーブル
インターフェイス単位のルート ガード	ディセーブル

パラメータ	デフォルト
PVST シミュレーション	イネーブル

Configuring STP Extensions Steps

（注） If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

You can enable Loop Guard per interface on either shared or point-to-point links.

スパニングツリー ポート タイプのグローバルな設定

スパニングツリーポートタイプの指定は、次のように、ポートの接続先デバイスによって異なります。

- エッジ：エッジ ポートは、レイヤ 2 ホストに接続するアクセス ポートです。
- ネットワーク：ネットワーク ポートは、レイヤ 2 スイッチまたはブリッジだけに接続し、アクセス ポートまたはトランク ポートのいずれかになります。
- 標準：標準ポートはエッジ ポートでもネットワーク ポートでもない、標準のスパニングツリー ポートです。 これらのポートは、どのデバイスにも接続できます。

ポートタイプは、グローバル単位でもインターフェイス単位でも設定できます。デフォルトのスパニングツリー ポート タイプは「標準」です。

はじめる前に

スパニングツリー ポート タイプを設定する前に、次の点を確認してください。

- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。
- STP が設定されていること。
- ポートの接続先デバイスに応じて、ポートを正しく設定していること。

手順の概要

1. **config t**
2. 次の 2 つのコマンドのいずれかを入力します。
3. **exit**
4. （任意） **show spanning-tree**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	次の 2 つのコマンドのいずれかを入力します。 **オプション** / **説明** **spanning-tree port type edge default** — レイヤ 2 ホストに接続しているすべてのアクセス ポートをエッジポートとして設定します。エッジポートは、リンクアップすると、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。 デフォルトのスパニングツリー ポート タイプは「標準」です。 **spanning-tree port type network default** — レイヤ 2 スイッチおよびブリッジに接続しているすべてのインターフェイスを、スパニングツリー ネットワーク ポートとして設定します。 Bridge Assurance をイネーブルにすると、各ネットワーク ポート上で Bridge Assurance が自動的に実行されます。 デフォルトのスパニングツリー ポート タイプは「標準」です。 （注） レイヤ 2 ホストに接続しているインターフェイスをネットワーク ポートとして設定すると、これらのポートは自動的にブロッキング ステートに移行します。 例： `switch(config)# spanning-tree port type edge default`	

	コマンドまたはアクション	目的

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

ステップ 4	**show spanning-tree** 例： `switch# show spanning-tree`	（任意） 設定した STP ポート タイプを含む STP コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、レイヤ 2 ホストに接続しているすべてのアクセス ポートをスパニングツリー エッジ ポートとして設定する例を示します。

```
switch# config t
switch(config)# spanning-tree port type edge default
switch(config)# exit
switch#
```

次に、レイヤ 2 スイッチまたはブリッジに接続しているすべてのポートを、スパニングツリー ネットワーク ポートとして設定する例を示します。

```
switch# config t
switch(config)# spanning-tree port type network default
switch(config)#
```

指定インターフェイスでのスパニングツリー エッジ ポートの設定

指定インターフェイスにスパニングツリーエッジポートを設定できます。スパニングツリーエッジ ポートとして設定されたインターフェイスは、リンク アップ時に、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。

このコマンドには次の 4 つの状態があります。

- **spanning-tree port type edge**：このコマンドはアクセス ポートのエッジ動作を明示的にイネーブルにします。
- **spanning-tree port type edge trunk**：このコマンドはトランク ポートのエッジ動作を明示的にイネーブルにします。

（注） **spanning-tree port type edge trunk** コマンドを入力すると、そのポートは、アクセス モードであってもエッジ ポートとして設定されます。

- **spanning-tree port type normal**：このコマンドは、ポートを標準スパニングツリー ポートとして明示的に設定しますが、フォワーディング ステートへの直接移行はイネーブルにしません。
- **no spanning-tree port type**：このコマンドは、**spanning-tree port type edge default** コマンドをグローバル コンフィギュレーション モードで定義した場合に、エッジ動作を暗黙的にイネーブルにします。エッジ ポートをグローバルに設定していない場合、**no spanning-tree port type** コマンドは、**spanning-tree port type normal** コマンドと同じです。

はじめる前に

スパニングツリー ポート タイプを設定する前に、次の点を確認してください。

- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。
- STP が設定されていること。
- ポートの接続先デバイスに応じて、ポートを正しく設定していること。

手順の概要

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree port type edge**
4. **exit**
5. （任意） **show spanning-tree**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**spanning-tree port type edge** 例： `switch(config-if)# spanning-tree port type edge`	指定したアクセス インターフェイスをスパニング エッジ ポートに設定します。エッジ ポートは、リンク アップすると、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。デフォルトのスパニングツリー ポート タイプは「標準」です。

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

ステップ 5	**show spanning-tree** 例： `switch# show spanning-tree`	（任意） 設定した STP ポート タイプを含む STP コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、アクセス インターフェイス Ethernet 1/4 をスパニングツリー エッジ ポートとして設定する例を示します。

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

指定インターフェイスでのスパニングツリー ネットワーク ポートの設定

指定インターフェイスにスパニングツリー ネットワーク ポートを設定できます。

Bridge Assurance は、スパニングツリー ネットワーク ポート上だけで実行されます。

このコマンドには次の 3 つの状態があります。

- **spanning-tree port type network**：このコマンドは指定したポートを明示的にネットワーク ポートとして設定します。 Bridge Assurance をグローバルにイネーブルにすると、スパニングツリー ネットワーク ポート上で Bridge Assurance が自動的に実行されます。
- **spanning-tree port type normal**：このコマンドは、ポートを明示的に標準スパニングツリー ポートとして設定します。このインターフェイス上では Bridge Assurance は動作しません。
- **no spanning-tree port type**：このコマンドは、**spanning-tree port type network default** コマンドをグローバル コンフィギュレーション モードで定義した場合に、ポートを暗黙的にスパニングツリー ネットワーク ポートとしてイネーブルにします。 Bridge Assurance をイネーブルにすると、このポート上で Bridge Assurance が自動的に実行されます。

（注） レイヤ 2 ホストに接続しているポートをネットワーク ポートとして設定すると、自動的にブロッキング ステートに移行します。

はじめる前に

スパニングツリー ポート タイプを設定する前に、次の点を確認してください。

- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。
- STP が設定されていること。
- ポートの接続先デバイスに応じて、ポートを正しく設定していること。

手順の概要

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree port type network**
4. **exit**
5. （任意） **show spanning-tree**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**spanning-tree port type network** 例： `switch(config-if)# spanning-tree port type network`	指定したインターフェイスをスパニング ネットワーク ポートに設定します。 Bridge Assurance をイネーブルにすると、各ネットワーク ポート上で Bridge Assurance が自動的に実行されます。デフォルトのスパニングツリー ポート タイプは「標準」です。

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

ステップ 5	**show spanning-tree** 例： `switch# show spanning-tree`	（任意） 設定した STP ポート タイプを含む STP コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、Ethernet インターフェイス 1/4 をスパニングツリー ネットワーク ポートとして設定する例を示します。

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

BPDU ガードのグローバルなイネーブル化

BPDU ガードをデフォルトでグローバルにイネーブルにできます。 BPDU ガードがグローバルにイネーブルにされると、システムは、BPDU を受信したエッジ ポートをシャット ダウンします。

（注） すべてのエッジ ポートで BPDU ガードをイネーブルにすることを推奨します。

はじめる前に

スパニングツリー ポート タイプを設定する前に、次の点を確認してください。

- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。
- STP が設定されていること。
- ポートの接続先デバイスに応じて、ポートを正しく設定していること。

手順の概要

1. **config t**
2. **spanning-tree port type edge bpduguard default**
3. **exit**
4. （任意） **show spanning-tree summary**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree port type edge bpduguard default** 例： `switch(config)# spanning-tree port type edge bpduguard default`	すべてのスパニングツリーエッジポートで、BPDU ガードを、デフォルトでイネーブルにします。 デフォルトでは、グローバルな BPDU ガードはディセーブルです。

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

ステップ 4	**show spanning-tree summary** 例： `switch# show spanning-tree summary`	（任意） STP の概要を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、すべてのスパニングツリー エッジ ポートで BPDU ガードをイネーブルにする例を示します。

```
switch# config t
switch(confiig)# spanning-tree port type edge bpduguard default
switch(config)# exit
switch#
```

指定インターフェイスでの BPDU ガードのイネーブル化

指定インターフェイスで、BPDU ガードをイネーブルにできます。 BPDU ガードがイネーブルにされたポートは、BPDU を受信すると、シャットダウンされます。

BPDU ガードは、指定インターフェイスで次のように設定にできます。

- **spanning-tree bpduguard enable**：指定インターフェイスで BPDU ガードを無条件にイネーブルにします。
- **spanning-tree bpduguard disable**：指定インターフェイスで BPDU ガードを無条件にディセーブルにします。
- **no spanning-tree bpduguard**：動作中のエッジ ポート インターフェイスに spanning-tree port type edge bpduguard default コマンドが設定されている場合、そのインターフェイスで BPDU ガードをイネーブルにします。

はじめる前に

この機能を設定する前に、次の点を確認してください。

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

手順の概要

1. **config t**
2. **interface** *type slot/port*
3. 次のいずれかのコマンドを入力します。
4. **exit**
5. （任意） **show spanning-tree summary**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。 **spanning-tree bpduguard {enable | disable}** — 指定したスパニングツリーエッジインターフェイスの BPDU ガードをイネーブルまたはディセーブルにします。デフォルトでは、インターフェイス上の BPDU ガードはディセーブルです。 **no spanning-tree bpduguard** — **spanning-tree port type edge bpduguard default** コマンドの入力により、インターフェイスに設定されたデフォルトのグローバル BPDU ガード設定に戻します。 例： `switch(config-if)# spanning-tree bpduguard enable`	

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

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

次に、エッジ ポート Ethernet 1/4 で BPDU ガードを明示的にイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpduguard enable
switch(config-if)# exit
switch(config)#
```

BPDU フィルタリングのグローバルなイネーブル化

スパニングツリー エッジ ポートで、BPDU フィルタリングをデフォルトでグローバルにイネーブルにできます。

BPDU フィルタリングがイネーブルであるエッジ ポートは、BPDU を受信するとエッジ ポートとしての稼働ステータスが失われ、通常の STP ステート移行を再開します。 ただし、このポートは、エッジ ポートとしての設定は保持したままです。

注意 このコマンドは、慎重に使用してください。 このコマンドを誤って使用すると、ブリッジング ループに陥る可能性があります。

はじめる前に

この機能を設定する前に、次の点を確認してください。

- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。
- STP が設定されていること。
- 少なくとも一部のスパニングツリー エッジ ポートが設定済みであること。

（注） グローバルにイネーブルにされた BPDU フィルタリングは、動作中のエッジ ポートだけに適用されます。 ポートは数個の BPDU をリンクアップ時に送出してから、実際に、発信 BPDU のフィルタリングを開始します。エッジポートは、BPDUを受信すると、動作中のエッジポート ステータスを失い、BPDU フィルタリングはディセーブルになります。

手順の概要

1. **config t**
2. **spanning-tree port type edge bpdufilter default**
3. **exit**
4. （任意） **show spanning-tree summary**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree port type edge bpdufilter default** 例： `switch(config)# spanning-tree port type edge bpdufilter default`	すべてのスパニングツリーエッジポートで、BPDU フィルタリングを、デフォルトでイネーブルにします。 デフォルトでは、グローバルな BPDU フィルタリングはディセーブルです。

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

ステップ 4	**show spanning-tree summary** 例： `switch# show spanning-tree summary`	（任意） STP の概要を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、すべての動作中のスパニングツリーエッジポートでBPDUフィルタリングをイネーブルにする例を示します。

```
switch# config t
switch(config)# spanning-tree port type edge bpdufilter default
switch(config)# exit
switch#
```

指定インターフェイスでの BPDU フィルタリングのイネーブル化

指定インターフェイスに BPDU フィルタリングを適用できます。 BPDU フィルタリングを特定のインターフェイス上でイネーブルにすると、そのインターフェイスは BPDU を送信しなくなり、受信した BPDU をすべてドロップするようになります。 この BPDU フィルタリング機能は、トランキング インターフェイスであるかどうかに関係なく、すべてのインターフェイスに適用されます。

注意 指定インターフェイスで **spanning-tree bpdufilter enable** コマンドを入力するときは注意してください。 ホストに接続していないポートに BPDU フィルタリングを設定すると、そのポートは受信した BPDU をすべて無視してフォワーディングに移行するので、ブリッジング ループが発生することがあります。

このコマンドを入力すると、指定インターフェイスのポート設定が上書きされます。

このコマンドには次の 3 つの状態があります。

- **spanning-tree bpdufilter enable**：インターフェイス上で BPDU フィルタリングが無条件にイネーブルになります。
- **spanning-tree bpdufilter disable**：インターフェイス上で BPDU フィルタリングが無条件にディセーブルになります。
- **no spanning-tree bpdufilter**：動作中のエッジ ポート インターフェイスに **spanning-tree port type edge bpdufilter default** コマンドが設定されている場合、そのインターフェイスで BPDU フィルタリングをイネーブルにします。

はじめる前に

この機能を設定する前に、次の点を確認してください。

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

（注） 特定のポートだけで BPDU フィルタリングをイネーブルにすると、そのポートでの BPDU の送受信が禁止されます。

手順の概要

1. **config t**
2. **interface** *type slot/port*
3. 次のいずれかのコマンドを入力します。
4. **exit**
5. （任意） **show spanning-tree summary**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。 **オプション** / **説明** **spanning-tree bpdufilter** {**enable** | **disable**} — 指定したスパニングツリー エッジ インターフェイスのBPDUフィルタリングをイネーブルまたはディセーブルにします。デフォルトでは、BPDUフィルタリングはディセーブルです。 **no spanning-tree bpdufilter** — 動作中のスパニングツリー エッジ ポート インターフェイスに **spanning-tree port type edge bpdufilter default** コマンドが設定されている場合、そのインターフェイスでBPDUフィルタリングをイネーブルにします。 例： `switch(config-if)# spanning-tree bpdufilter enable`	

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

ステップ 5	**show spanning-tree summary** 例： `switch# show spanning-tree summary`	（任意） STP の概要を表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、スパニングツリー エッジ ポート Ethernet 1/4 で BPDU フィルタリングを明示的にイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpdufilter enable
switch(config-if)# exit
switch(config)#
```

ループ ガードのグローバルなイネーブル化

ループ ガードは、デフォルトの設定により、すべてのポイントツーポイント スパニングツリーの標準およびネットワーク ポートで、グローバルにイネーブルにできます。ループ ガードは、エッジ ポートでは動作しません。

ループ ガードを使用すると、ブリッジ ネットワークのセキュリティを高めることができます。ループ ガードは、単方向リンクを引き起こす可能性のある障害が原因で、代替ポートまたはルート ポートが指定ポートになるのを防ぎます。

（注） 指定インターフェイスでループ ガード コマンドを入力すると、グローバルなループ ガード コマンドが上書きされます。

はじめる前に

この機能を設定する前に、次の点を確認してください。

- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。
- STP が設定されていること。
- スパニングツリー標準ポートが存在し、少なくとも一部のネットワーク ポートが設定済みであること。

手順の概要

1. **config t**
2. **spanning-tree loopguard default**
3. **exit**
4. （任意） **show spanning-tree summary**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**spanning-tree loopguard default** 例： `switch(config)# spanning-tree loopguard default`	スパニングツリーのすべての標準およびネットワーク ポートで、ループ ガードを、デフォルトでイネーブルにします。 デフォルトでは、グローバルなループ ガードはディセーブルです。

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

ステップ 4	**show spanning-tree summary** 例： `switch# show spanning-tree summary`	（任意） STP の概要を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、スパニングツリーのすべての標準およびネットワーク ポートでループ ガードをイネーブルにする例を示します。

```
switch# config t
switch(config)# spanning-tree loopguard default
switch(config)# exit
switch#
```

指定インターフェイスでのループガードまたはルートガードのイネーブル化

（注） ループ ガードは、スパニングツリーの標準またはネットワーク ポート上で実行できます。ルート ガードは、すべてのスパニングツリー ポート（標準、エッジ、ネットワーク）上で実行できます。

ループ ガードまたはルート ガードは、指定インターフェイスでイネーブルにできます。

ポート上でルート ガードをイネーブルにすることは、そのポートをルート ポートにできないことを意味します。ループ ガードは、単方向リンクの障害発生時に、代替ポートまたはルート ポートが指定ポートになるのを防止します。

特定のインターフェイスでループ ガードおよびルート ガードの両機能をイネーブルにすると、そのインターフェイスが属するすべての VLAN に両機能が適用されます。

（注） 指定インターフェイスでループ ガード コマンドを入力すると、グローバルなループ ガード コマンドが上書きされます。

はじめる前に

この機能を設定する前に、次の点を確認してください。

- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。
- STP が設定されていること。
- ループ ガードが、スパニングツリーの標準またはネットワーク ポート上で設定されていること。

手順の概要

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree guard** {**loop** | **root** | **none**}
4. **exit**
5. **interface** *type slot/port*
6. **spanning-tree guard** {**loop** | **root** | **none**}
7. **exit**
8. （任意） **show spanning-tree summary**
9. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**spanning-tree guard** {**loop** | **root** | **none**} 例： `switch(config-if)# spanning-tree guard loop`	ループ ガードまたはルート ガードを、指定インターフェイスでイネーブルまたはディセーブルにします。ルート ガードはデフォルトでディセーブル、ループ ガードも指定ポートでディセーブルになります。 （注） ループ ガードは、スパニングツリーの標準およびネットワーク インターフェイスだけで動作します。 この例では、指定したインターフェイス上でループ ガードをイネーブルにしています。

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

ステップ 5	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 1/10`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 6	**spanning-tree guard** {**loop** | **root** | **none**} 例： `switch(config-if)# spanning-tree guard root`	ループ ガードまたはルート ガードを、指定インターフェイスでイネーブルまたはディセーブルにします。ルート ガードはデフォルトでディセーブル、ループ ガードも指定ポートでディセーブルになります。 この例では、別のインターフェイス上でルート ガードをイネーブルにしています。

ステップ 7	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

	コマンドまたはアクション	目的
ステップ 8	**show spanning-tree summary** 例： `switch# show spanning-tree summary`	（任意） STP の概要を表示します。
ステップ 9	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、Ethernet ポート 1/4 で、ルート ガードをイネーブルにする例を示します。

```
switch# config t
switch(config)# interface etherent 1/4
switch(config-if)# spanning-tree guard root
switch(config-if)# exit
switch(config)#
```

PVST シミュレーションのグローバル設定（CLI バージョン）

（注） PVST シミュレーションは、デフォルトでイネーブルになっています。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。

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。Rapid PVST+ シミュレーションをディセーブルにした場合、MST がイネーブルなポートが Rapid PVST+ がイネーブルなポートに接続されていることが検出されると、MST がイネーブルなポートは、ブロッキング ステートに移行します。 このポートは、BPDU の受信が停止されるまで、一貫性のないステートのままになり、それから、ポートは、通常の STP 送信プロセスに戻ります。

この自動機能は、グローバルまたはポートごとにブロックできます。グローバル コマンドを入力し、インターフェイス コマンド モードでデバイス全体の PVST シミュレーション設定を変更できます。

はじめる前に

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

手順の概要

1. **config t**
2. **no spanning-tree mst simulate pvst global**
3. **exit**
4. （任意） **show spanning-tree detail**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**no spanning-tree mst simulate pvst global** 例： `switch(config)# no spanning-tree mst simulate pvst global`	スイッチ上のすべてのインターフェイスで、Rapid PVST+ モードを実行している接続先デバイスとの自動的な相互運用をディセーブルにします。この機能はデフォルトではイネーブルです。デフォルトでは、デバイス上のすべてのインターフェイスが、Rapid PVST+ と MST の間で運用されます。

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

ステップ 4	**show spanning-tree detail** 例： `switch# show spanning-tree detail`	（任意） STP の詳細を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、Rapid PVST+ を実行している接続先デバイスとの自動的な相互運用を回避する例を示します。

```
switch# config t
switch(config)# no spanning-tree mst simulate pvst global
switch(config)#
```

ポートごとの PVST シミュレーションの設定

（注） PVST シミュレーションは、デフォルトでイネーブルになっています。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。

PVST シミュレーションを設定できるのは、デバイス上で MST を実行している場合だけです（Rapid PVST+ がデフォルトの STP モードです）。 MST は、Rapid PVST+ と相互運用します。 ただし、デフォルトの STP モードで、MST を実行していないデバイスに接続する可能性を防ぐには、この自動機能をディセーブルに設定できます。PVST シミュレーションをディセーブルにすると、Rapid PVST+ イネーブル ポートに接続したことが検出された時点で、MST イネーブル ポートはブロッキング ステートに移行します。 このポートは、Rapid PVST+ BPDU を受信しなくなるまで不整合ステートのままですが、そのあとは標準 STP のステート移行を再開します。

この自動機能は、グローバルまたはポートごとにブロックできます。

はじめる前に

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

手順の概要

1. **config t**
2. **interface** {{*type slot/port*} |{**port-channel** *number*}}
3. 次のいずれかのコマンドを入力します。
4. **exit**
5. （任意） **show spanning-tree detail**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**interface** {{*type slot/port*} |{**port-channel** *number*}}
	
	例：
	`switch(config)# interface ethernet 3/1`
	`switch(config-if)#`
		設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。	

	コマンドまたはアクション	目的
	オプション / 説明 **spanning-tree mst simulate pvst disable**：指定したインターフェイスで、Rapid PVST+ モードを実行している接続先デバイスとの自動的な相互運用をディセーブルにします。デフォルトでは、デバイス上のすべてのインターフェイスで Rapid PVST+ と MST が相互運用されます。 **spanning-tree mst simulate pvst**：指定したインターフェイスで、MST と Rapid PVST+ のシームレスな相互運用を再びイネーブルにします。 **no spanning-tree mst simulate pvst**：インターフェイスを、**spanning-tree mst simulate pvst global** コマンドを使用して設定したデバイス全体で MST と Rapid PVST+ との間で相互動作するよう設定します。 例： `switch(config-if)# spanning-tree mst simulate pvst`	

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

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

次に、指定したインターフェイスで、MST を実行していない接続先デバイスとの自動的な相互運用を回避する例を示します。

```
switch(config-if)# spanning-tree mst simulate pvst
switch(config-if)#
```

STP 拡張機能の設定の確認

STP 拡張機能の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config spanning-tree [**all**]	STP に関する情報を表示します。
show spanning-tree summary	STP 情報の要約を表示します。
show spanning-tree mst *instance-id* **interface** {**ethernet** *slot/port* | **port-channel** *channel-number*} [**detail**]	指定したインターフェイスおよびインスタンスの MST 情報を表示します。

これらのコマンド出力の詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』を参照してください。

STP 拡張機能の設定例

次に、STP 拡張機能を設定する例を示します。

```
switch# configure terminal
switch(config)# spanning-tree port type network default
switch(config)# spanning-tree port type edge bpduguard default
switch(config)# spanning-tree port type edge bpdufilter default

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

switch(config)# interface ethernet 1/2
switch(config-if)# spanning-tree port type edge
switch(config-if)# exit
switch(config)#
```

STP 拡張機能の追加情報（CLI バージョン）

関連資料

関連項目	参照先
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』
レイヤ 2 インターフェイス	『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』

関連項目	参照先
NX-OS の基礎	『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x*』
ハイ アベイラビリティ	『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』
システム管理	『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x*』
仮想デバイス コンテキスト（VDC）	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.x*』

標準

標準	タイトル
IEEE 802.1Q-2006（旧称 IEEE 802.1s）、IEEE 802.1D-2004（旧称 IEEE 802.1w）、IEEE 802.1D、IEEE 802.1t	—

MIB

MIB	MIB のリンク
• CISCO-STP-EXTENSION-MIB • BRIDGE-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

STP 拡張機能の設定の機能履歴（CLI バージョン）

次の表に、この機能のリリースの履歴を示します。

表 *21* : *STP* 拡張機能設定の機能履歴

機能名	リリース	機能情報
変更なし	4.2(1)	--
変更なし	4.1(2)	--

付 録 A

レイヤ 2 スイッチングの設定の制限

- レイヤ 2 スイッチングの設定の制限，225 ページ

レイヤ 2 スイッチングの設定の制限

設定の制限は、『*Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*』に記載されています。

レイヤ 2 スイッチングの設定の制限

索 引

A

alternate port 103
  description 103

B

backup port 103
  description 103
blocking port state 104
  description 104
BPDU Guard 65
  private VLAN ports 65
BPDUs 97, 99, 100, 141, 143, 145, 147, 190, 195, 197
  Bridge Assurance 190
  description 97
  edge ports 190
  exchange result 97
  hop count 145
  M-records 141
  MST 141
  MST regions 141
  port channels 197
  Rapid PVST+ 97, 100
  superior 195
  TC While timer 99
  version 100, 143, 147
BPDU ガード 192, 198, 205, 207
  インターフェイス単位のイネーブル化 207
  グローバルなイネーブル化 205
  説明 192
  デフォルト設定 198
BPDU フィルタリング 193, 198, 209, 210
  インターフェイス単位のイネーブル化 210
  エッジ ポート 193
  グローバル 193
  グローバルなイネーブル化 209
  説明 193
  デフォルト設定 198
BPDU フィルタリング *(続き)*
  ポート単位 193
Bridge Assurance 190, 198
  description 190
  network ports 190
  supported protocols and link types 190
  デフォルト設定 198
bridge ID 95
  extended system ID 95
Bridge Protocol Data Units.。参照先： BPDUs
bridging loops 94, 194
  Loop Guard 194
  STP 94
broadcast traffic 28, 63
  private VLANs 63
  VLANs 28

C

CIST 142
  description 142
CIST regional root 143
common and internal spanning tree.。参照先： CIST
common spanning tree.。参照先： CST
community ports 59
  private VLANs 59
community VLANs 60
  description 60
  private VLANs 60
creating VLANs 31
  default state 31
CST 142
  description 142

D

default settings 93
  STP 93

designated bridge 97
description 97
designated ports 99, 103
BPDUs 99
description 103
Rapid PVST+ 99
designated switch 103
description 103

E

edge ports 99, 190
description 190
PortFast 190
Rapid PVST+ 99
extended system IDs 29
VLANs 29

F

forward delay time 102
description 102
forwarding port state 104
description 104

G

guidelines 33, 65, 112, 149, 197
MST 149
private VLANs 65
Rapid PVST+ 112
STP extensions 197
VLANs 33

H

hello time 102
description 102
hello タイム 128, 175
MST 175
Rapid PVST+ の VLAN 単位の設定 128
host ports 59, 99, 190
edge ports 99, 190
private VLANs 59

I

IEEE 802.1D 93
terminology 93
IEEE 802.1s 93
terminology 93
IEEE 802.1w 93
terminology 93
instance 140
MST 140
internal spanning tree.。参照先： IST
isolated ports 59
private VLANs 59
isolated VLANs 58, 60
defined 60
primary VLANs 60
secondary private VLANs 58
ISSU 14
スイッチング 14
IST 140, 141, 142
BPDUs 141
description 142
MST 140

L

learning port state 104
description 104
licenses 32, 64, 111, 149, 196
MST 149
private VLANs 64
Rapid PVST+ 111
STP extensions 196
VLANs 32
limitations 65, 112, 149, 197
MST 149
private VLANs 65
Rapid PVST+ 112
STP extensions 197
link failure 108, 146
detecting unidirectional 108, 146
link type 99
point to point 99
Rapid PVST+ 99
Loop Guard 194
description 194
link type 194

M

MAC address reduction 96, 140
  MST 140
  Rapid PVST+ 96
MAC アドレス 12, 13, 14, 15, 17, 19
  vPC 12
  一貫性 13
  エージング タイム 12
  エージング タイムの設定 19
  スタティック レイヤ 3 17
  制限事項 15
  設定 14
  注意事項 15
  テーブルの説明 12
  レイヤ 3 スタティック 13
MAC アドレス テーブル 12, 16, 17, 21, 22, 23
  確認 23
  クリア 22
  スタティック アドレス 12, 16, 17
  ダイナミックな構築 12
  フォワーディングの整合性 21
  モジュールの一致 21
mapping 63
  private VLANs 63
maximum age time 102
  description 102
modifying VLANs 31
  allowed parameters 31
MST 139, 140, 141, 143, 145, 147, 148, 149, 151, 152, 154, 156, 157, 159, 162, 164, 166, 168, 170, 172, 173, 175, 177, 178, 179, 180, 184, 185, 195
  BPDUs 141, 143, 145
  configuration information 140
  description 139
  guidelines 149
  hello タイム 175
  IEEE802.1w 140
  instance 140
  interoperation with IEEE 802.1D 147
  interoperation with other features 149
  interoperation with prestandard MSTP 147
  interoperation with Rapid PVST+ 195
  licenses 149
  limitations 149
  logging level 139
  maximum hop count 145
  maximum-aging time 145
  MST コンフィギュレーション モード 154
  name 141
  pre-provisioning 152
MST (続き)
  protocol migration 147
  revision number 140, 141
  root bridge 195
  troubleshooting 139
  VDCs 148
  VLAN-to-MST mapping 140, 141
  イネーブル化 152
  確認 184
  境界ポート 145
  最大エージング タイム 178
  最大ホップ カウント 179
  スイッチ プライオリティの設定 170
  セカンダリ ルート ブリッジ 168
  設定例 185
  先行標準 MSTP メッセージ 180
  デフォルト設定 151
  転送遅延時間 177
  統計情報 185
  トラブルシューティング 166
  パスコスト方式 173
  プライベート VLAN 164
  プロトコルの再初期化 184
  ポート コスト 173
  ポート プライオリティ 172
  リビジョン番号の設定 157
  領域の指定 159
  領域名の設定 154, 156
  ルート ブリッジの設定 166
MST instances 140
  numbering 140
MST regions 140
  description 140
  supported spanning-tree instances 140
multicast traffic 28
  VLANs 28
Multiple Spanning Tree Protocol.。参照先： MST

N

network ports 190
  Bridge Assurance 190
  description 190

P

path cost 97
  description 97

path-cost method 108, 147
MST 147
Rapid PVST+ 108
port channels 197
and STP 197
BPDUs 197
port cost 108, 147
values 108, 147
port priority 109
Rapid PVST+ 109
port roles 103
STP 103
PortFast 190
edge ports 190
ports 57, 59, 67, 99, 190
Layer 2 57, 59, 67, 99, 190
primary VLANs 58, 60
associating with secondary VLANs 60
private VLANs 58, 60
promiscuous ports 60
traffic distribution 60
private VLAN ports 59, 60, 63, 65, 67
BPDU Guard 65
broadcast traffic 63
community ports 59
isolated ports 59
isolated trunk ports 59
limitations 67
promiscuous ports 59
promiscuous trunk ports 59
traffic distribution 60
trunk ports 59
private VLANs 57, 58, 59, 60, 63, 64, 65, 67
across multiple devices 64
benefits of 58
broadcast domain 57
broadcast traffic 63
communication 57, 63
communication outside private VLANs 60
community VLANs 58, 60
configuration guidelines 67
description 57
enabling 57
end station access to 63
guidelines 65
isolated VLANs 58, 60
licenses 64
limitations 65
mapping 63
ports 59, 67
community 59
configuration guidelines 67
isolated 59
promiscuous 59
private VLANs *(続き)*
primary VLANs 58
routing 57
secondary VLANs 58
STP 65
SVIs 63
troubleshooting 57
virtualization 64
VLAN interface 57
VLAN interfaces 57, 60, 63
promiscuous ports 59, 60
community VLANs 60
isolated VLANs 60
numbers in primary VLANs 60
primary VLANs 60
proposal and agreement handshake 100, 101
BPDUs 100
Rapid PVST+ 101
PVST simulation 195
description 195
root bridge 195
PVST シミュレーション 198, 217, 219
インターフェイス単位の設定 219
グローバルに設定 217
デフォルト設定 198

R

Rapid per VLAN Spanning Tree +。参照先： Rapid PVST+
Rapid PVST+ 93, 99, 100, 102, 103, 109, 110, 111, 112, 113, 115, 117, 119, 121, 123, 134, 135, 195
aging out 99
BPDUs 100
description 93, 99
designated port 99
guidelines 112
interactions with other features 112
interoperation with IEEE 802.1D 93, 99, 110
interoperation with IEEE 802.1Q 93, 109
interoperation with IEEE 802.1s 110
interoperation with MST 110, 195
licenses 111
limitations 112
per VLAN 93
port transitions 103
protocol timers 102
rapid convergence 99
root switch 99
topology change 99
VDCs 111
VLAN プライオリティ 123

Rapid PVST+ *(続き)*
イネーブル化 **115, 117**
確認 **134**
セカンダリ ルート **121**
設定例 **135**
デフォルト設定 **113**
統計情報 **135**
トラブルシューティング **119**
プロトコルの再初期化 **134**
ルート ブリッジの設定 **119**
root bridge **98, 195**
election **98**
MST **195**
PVST simulation **195**
Root Guard **195**
Root Guard **195**
description **195**
root ports **97, 99, 103**
BPDUs **99**
description **97, 103**
RSTP **99, 103, 107**
active topology **103**
BPDUs **107**
rapid convergence **99**

S

secondary VLANs **58, 60**
associating with primary VLANs **60**
community **58**
isolated **58**
private VLANs **58**
Spanning Tree Protocol.。参照先： STP
STP **6, 65, 93, 94, 95, 96, 97, 98, 99, 103, 108, 110, 111, 115, 117, 139, 140, 146, 148, 152, 190, 195**
and vPCs **93, 139**
BPDUs **95**
bridging loops **94**
default mode **93**
dispute mechanism **108, 146**
edge ports **99, 190**
MAC address reduction **96**
MST **140**
multiple instances **111, 148**
network ports **190**
overview **6**
path cost **97**
per VLAN **93**
port roles **103**
PortFast **99, 190**
private VLANs **65**
STP *(続き)*
protocol migration **110**
root bridge **98**
root ports **97**
terminology **93**
topology **95, 98**
troubleshooting **195**
virtualization **93, 111, 148**
デフォルト モード **115, 117, 152**
トラブルシューティング **117**
STP extensions **189, 190, 196, 197**
description **189, 190**
guidelines **197**
licenses **196**
limitations **197**
virtualization **196**
STP port types **190**
description **190**
STP topology **194**
troubleshooting **194**
STP 拡張機能 **195, 198, 221**
確認 **221**
設定例 **221**
デフォルト設定 **198**
ベスト プラクティス **195**
STP ポート タイプ **198**
デフォルト設定 **198**
SVIs **28**
VLAN interfaces **28**

T

timers **102**
STP **102**

U

UDLD **108, 146, 197**
Loop Guard **197**
MST **146**
Rapid PVST+ **108**
Unidirectional Link Detection.。参照先： UDLD

V

VDCs **8, 32, 64, 111, 148, 196**
fault isolation **8**
Layer 2 switching features **8**
MST **148**

VDCs *(続き)*
private VLANs 64
Rapid PVST+ 111
resources 8
STP extensions 196
user roles 8
virtualization 8
VLANs 32
virtual device contexts。参照先： VDCs
virtual LANs。参照先： VLANs
virtualization 8, 32, 64, 93, 111, 148, 196
private VLANs 64
STP 93, 111, 148
STP extensions 196
VDCs 8
VLANs 32
VLAN 6, 33, 34, 36, 40, 41, 43
削除 34
作成 34, 36, 41
作成前の設定 41
設定 41
設定の確認 43
デフォルト設定 33
変更 36, 40
VLAN configuration submode 31
executing commands 31
VLAN interface 60
enabling 60
VLAN interfaces 28, 60, 63
communicating between VLANs 28
enabling 60
private VLANs 63
troubleshooting 63
VLAN numbers 29, 32
allowed numbers 29
reserved range 29
reusing 32
VLAN ranges 29
description 29
VLAN traffic 28
and routing 28
distribution 28
VLAN/MST マッピング 162
VLANs 27, 28, 29, 31, 32, 33, 47, 93
assigning ports 31
deleting 31
description 27, 28
extended system ID 29
guidelines 33
licenses 32
limitations 33
Rapid PVST+ 93
VLANs *(続き)*
reserved ranges 29
SVIs 28
usable VLANs 29
virtualization 32
VTP 47
VLAN コンフィギュレーション 44
例 44
VLAN コンフィギュレーション サブモード 36
使用 36
VLAN 状態 37
設定 37
VLAN 統計情報 44
クリア 44
表示 44
VLAN の予約された範囲 40
変更 40
VLAN プライオリティ 123
設定 123
VLAN 名 37
設定 37
vPC 12
MAC アドレス 12
vPCs 93, 139
and STP 93, 139
VTP 28, 47, 51
mode 28
トランスペアレント モード 51

い

イネーブル化 42
VLAN のロングねーむ 42

え

エッジ ポート 199, 201
インターフェイス単位の設定 201
グローバルに設定 199

か

学習モード 20
学習モードの設定 20
確認 23, 43, 89, 134, 184, 221
MAC アドレス テーブル 23

確認 *(続き)*
MST 184
Rapid PVST+ 134
STP 拡張機能 221
VLAN 43
プライベート VLAN 89
仮想デバイス コンテキスト（VDC） 14
MAC アドレス テーブル 14
ライセンス 14
関連資料 xiv

き

境界ポート 145
STP 145

さ

最大エージング タイム 131, 178
MST 178
Rapid PVST+ で VLAN 単位の設定 131

す

スイッチ プライオリティ 170
MST 170
スイッチング 14
ハイ アベイラビリティ 14
スタティック MAC アドレス 12, 16, 17, 23
追加 12, 16, 17
例 23

せ

セカンダリ VLAN 62, 72, 75
VLAN インターフェイスへのマッピング 75
プライマリ VLAN とのアソシエーション 62
プライマリ VLAN との関連付け 72
セカンダリ ルート ブリッジ 168
MST 168
設定 126
説明 119

た

ダイナミック MAC アドレス 12, 22
クリア 22
追加 12

ち

注意事項 15
MAC アドレス 15
直径 119

て

デフォルト設定 15, 33, 68, 113, 151, 198
MST 151
Rapid PVST+ 113
STP 拡張機能 198
VLAN 33
プライベート VLAN 68
レイヤ 2 スイッチング 15
転送遅延時間 129, 177
MST 177
Rapid PVST+ の VLAN 単位の設定 129

と

統計情報 44, 90, 135, 185
MST 185
Rapid PVST+ 135
VLAN 44
プライベート VLAN 90
トランク ポート 201
エッジ ポートとしての設定 201

ね

ネットワーク ポート 199, 203
インターフェイス単位の設定 203
グローバルに設定 199

は

パスコスト方式 126, 173
MST 173

ふ

プライベート VLAN 58, 62, 68, 69, 70, 72, 75, 77, 83, 89, 90, 164
MST マッピング 164
アソシエーション 62
動作中 62
変更 62
イネーブル化 69
確認 89
関連付け 72, 77, 83, 90
コミュニティ VLAN 70
設定 70
設定例 90
ディセーブル化 58
デフォルト設定 68
統計情報 90
独立 VLAN 70
トラフィック分散 75
トラブルシューティング 58
プライマリ VLAN 70
プライマリ VLAN のアソシエーション 62
マッピング 90
プライベート VLAN ポート 77, 79, 83, 85
コミュニティ ポート 77
独立トランク ポート 79
独立ポート 77
無差別トランク ポート 85
無差別ポート 83
プライマリ VLAN 62, 72, 75
セカンダリ VLAN とのアソシエーション 62
セカンダリ VLAN との関連付け 72
マッピング 75
プロトコルの再初期化 134, 184
MST 184
Rapid PVST+ 134

ほ

ポート 199
エッジ ポート 199
ネットワーク ポート 199
ポート *(続き)*
標準ポート 199
ポート コスト 126, 173
MST の設定 173
設定 126
ポート プライオリティ 124, 172
MST 172
Rapid PVST+ の設定 124
ホスト ポート 62, 77, 79
設定 77
独立トランク ポート 79
プライベート VLAN 62, 77

ま

マニュアル xiv
追加資料 xiv

む

無差別ポート 83, 85
設定 83
無差別トランク ポート 85

ら

ライセンス 14
仮想デバイス コンテキスト（VDC） 14
レイヤ 2 スイッチング 14

る

ルート ガード 198, 215
イネーブル化 215
デフォルト設定 198
ルート ブリッジ 119, 121, 166
MST の設定 166
Rapid PVST+ の設定 119
複数のバックアップ 121
ループ ガード 198, 213, 215
インターフェイス単位のイネーブル化 215
グローバルなイネーブル化 213
デフォルト設定 198

れ

例 23, 44, 90, 135, 185, 221
MST 185
Rapid PVST+ 135
STP 拡張機能 221
VLAN コンフィギュレーション 44
スタティック MAC アドレス 23
プライベート VLAN 90
レイヤ 2 スイッチング 5, 12, 14, 15
イーサネット スイッチング 5, 12
レイヤ 2 スイッチング *(続き)*
仮想デバイス コンテキスト（VDC） 14
デフォルト値 15
レイヤ 3 13, 17
スタティック MAC アドレス 13, 17

ろ

ロング ネームのイネーブル化 42
VLAN 42