Cisco Nexus 9000 シリーズ NX-OS レイヤ 2 スイッチング構成ガイド、リリース 10.3(x)

最終更新：2025 年 7 月 14 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/

【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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html. Cisco product warranty information is available at https://www.cisco.com/c/en/us/products/warranty-listing.html. US Federal Communications Commission Notices are found here https://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2022–2024 Cisco Systems, Inc. All rights reserved.

目 次

Trademarks ?

はじめに：

はじめに xiii

対象読者 xiii

表記法 xiii

Cisco Nexus 9000 シリーズ スイッチの関連資料 xiv

マニュアルに関するフィードバック xiv

Communications, services, and additional information xv

Cisco Bug Search Tool xv

Documentation feedback xv

第 1 章

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

第 2 章

概要 3

ライセンス要件 3

サポートされるプラットフォーム 3

レイヤ 2 イーサネット スイッチングの概要 3

VLANs 4

スパニングツリー 4

STP の概要 4

Rapid PVST+ 5

MST 5

STP 拡張機能 6

トラフィック ストーム制御 6

関連項目 7

第 3 章

レイヤ 2 スイッチングの設定 9

レイヤ 2 スイッチングについて 9

レイヤ 2 イーサネット スイッチングの概要 10

セグメント間のフレーム スイッチング 10

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 10

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 11

スイッチングのハイ アベイラビリティ 11

MAC アドレス設定の前提条件 12

レイヤ 2 スイッチングのデフォルト設定 12

レイヤ 2 スイッチングの設定手順 12

スタティック MAC アドレスの設定 12

システムでの MAC アドレス学習の無効化 14

レイヤ 2 インターフェイスでの MAC アドレス学習の無効化 14

MAC テーブルのエージング タイムの設定 16

MAC アドレス テーブルの整合性検査 17

MAC テーブルからのダイナミック アドレスのクリア 18

MAC アドレス制限の設定 18

L2 ヘビー モードの設定 19

レイヤ 2 スイッチング設定の確認 20

レイヤ 2 スイッチングの設定例 21

レイヤ 2 スイッチングの追加情報（CLI バージョン） 22

第 4 章

Flex Link の設定 23

Flex Link について 23

Flex Link 23

プリエンプション 24

マルチキャスト 24

注意事項と制約事項 25

デフォルト設定 26

Flex Link の設定 27
FlexLink の設定 27
Flex Link プリエンプションの設定 29
設定の確認 31

第 5 章 VLAN の設定 37
VLAN について 37
VLAN の概要 37
VLAN の範囲 38
予約済み VLAN について 39
VLAN 予約の例 40
VLAN の作成、削除、変更 41
VLAN のハイ アベイラビリティ 42
VLAN 設定の前提条件 42
VLAN の設定に関するガイドラインおよび制約事項 42
VLAN のデフォルト設定 43
VLAN の設定 44
VLAN の作成と削除（CLI バージョン） 44
VLAN コンフィギュレーション サブモードの開始 46
VLAN の設定 47
VLAN 作成前の VLAN 設定 49
VLAN の長い名前のイネーブル化 50
トランク ポートでの内部 VLAN および外部 VLAN マッピングの設定 51
VLAN の設定の確認 54
VLAN 統計情報の表示とクリア 54
VLAN の設定例 54
VLAN に関する追加情報 55

第 6 章 VTP の設定 57
VTP の概要 57
VTP 57

VTP の概要 58
VTP モード 58
インターフェイス単位の VTP 59
VTP の設定に関する注意事項および制約事項 59
デフォルト設定 59
VTP の設定 60

第 7 章 NX-OS を使用したプライベート VLAN の設定 63
プライベート VLAN について 63
プライベート VLAN の概要 64
プライベート VLAN のプライマリ VLAN とセカンダリ VLAN 64
プライベート VLAN ポート 65
プライマリ、独立、およびコミュニティ プライベート VLAN 66
プライマリ VLAN とセカンダリ VLAN の関連付け 68
プライベート VLAN 内のブロードキャスト トラフィック 69
プライベート VLAN ポートの分離 70
プライベート VLAN および VLAN インターフェイス 70
複数のデバイスにまたがるプライベート VLAN 70
内部 VLAN タグを保持するプライベート VLAN 71
FEXホストインターフェイスポート上のプライベートVLAN 72
プライベート VLAN のハイ アベイラビリティ 72
プライベート VLAN の前提条件 72
プライベート VLAN の設定に関するガイドラインおよび制約事項 73
プライベート VLAN のデフォルト設定 76
プライベート VLAN の設定 77
プライベート VLAN のイネーブル化（CLI バージョン） 77
プライベート VLAN としての VLAN の設定（CLI バージョン） 78
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） 80
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） 82
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 84

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 86
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 89
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 91
FEX トランクでの PVLAN の有効化 94
プライベート VLAN ホスト ポートとしてのレイヤ 2 FEX インターフェイスの設定 94
プライベート VLAN 独立トランク ポートとしてのレイヤ 2 FEX インターフェイスの設定 95
プライベート VLAN 設定の確認 98
プライベート VLAN の統計情報の表示とクリア 98
プライベート VLAN の設定例 98
プライベート VLAN の追加情報（CLI バージョン） 99

第 8 章 スイッチング モードの設定 101
スイッチング モードに関する情報 101
スイッチング モードに関するガイドラインと制限事項 102
スイッチング モードのデフォルト設定 102
スイッチング モードの設定 103
Store-and-Forward スイッチングのイネーブル化 103
カットスルー スイッチングの再イネーブル化 104

第 9 章 Cisco NX-OS を使用した Rapid PVST+ の設定 105
Rapid PVST+ について 105
STP 106
STP の概要 106
トポロジの作成方法 107
ブリッジ ID 108
BPDU 109
ルート ブリッジの選定 110
スパニングツリー トポロジの作成 111
Rapid PVST+ 111
Rapid PVST+ の概要 111
Rapid PVST+ BPDU 113

提案と合意のハンドシェイク 114
プロトコル タイマー 115
ポート ロール 115
Rapid PVST+ ポート ステートの概要 116
ポート ロールの同期 119
単方向リンク障害の検出：Rapid PVST+ 120
ポートコスト 121
ポートプライオリティ 122
Rapid PVST+ と IEEE 802.1Q トランク 122
Rapid PVST+ のレガシー 802.1D STP との相互運用 123
Rapid PVST+ の 802.1s MST との相互運用 124
Rapid PVST+ のハイ アベイラビリティ 124
Rapid PVST+ を設定するための前提条件 124
Rapid PVST+ の設定に関するガイドラインおよび制約事項 124
Rapid PVST+ のデフォルト設定 125
Rapid PVST+ の設定 126
Rapid PVST+ のイネーブル化（CLI バージョン） 127
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） 128
ルート ブリッジ ID の設定 130
セカンダリ ルート ブリッジの設定（CLI バージョン） 132
VLAN の Rapid PVST+ のブリッジ プライオリティの設定 133
Rapid PVST+ ポート プライオリティの設定（CLI バージョン） 135
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） 136
VLAN の Rapid PVST+ hello タイムの設定（CLI バージョン） 138
VLAN の Rapid PVST+ 転送遅延時間の設定（CLI バージョン） 139
VLAN の Rapid PVST+ 最大エージング タイムの設定（CLI バージョン） 140
Rapid PVST+ のリンク タイプの指定（CLI バージョン） 141
Rapid PVST+ 用のプロトコルの再初期化 143
Rapid PVST+ の設定の確認 144
Rapid PVST+ 統計情報の表示およびクリア（CLI バージョン） 144

Rapid PVST+ の設定例 144
Rapid PVST+ の追加情報（CLI バージョン） 145

第 10 章 Cisco NX-OS を使用した MST の設定 147
MST について 147
MST の概要 148
MST 領域 148
MST BPDU 149
MST 設定情報 149
IST、CIST、CST 150
IST、CIST、CST の概要 150
MST 領域内でのスパニングツリーの動作 151
MST 領域間のスパニングツリー動作 151
MST 用語 152
ホップ カウント 153
境界ポート 153
単方向リンク障害の検出：MST 154
ポート コストとポート プライオリティ 155
IEEE 802.1D との相互運用性 155
MST のハイ アベイラビリティ 156
MST の前提条件 156
MST の設定に関するガイドラインおよび制約事項 156
MST のデフォルト設定 158
MST の設定 159
MST のイネーブル化（CLI バージョン） 159
MST コンフィギュレーション モードの開始 160
MST の名前の指定 162
MST 設定のリビジョン番号の指定 163
MST リージョンでの設定の指定 165
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） 167
ルート ブリッジの設定 169

MST セカンダリ ルート ブリッジの設定 171
MST スイッチ プライオリティの設定 173
MST ポート プライオリティの設定 174
MST ポート コストの設定 176
MST hello タイムの設定 178
MST 転送遅延時間の設定 179
MST 最大エージング タイムの設定 180
MST 最大ホップ カウントの設定 181
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） 183
MST のリンク タイプの指定（CLI バージョン） 184
MST 用のプロトコルの再初期化 185
MST の設定の確認 186
MST 統計情報の表示およびクリア（CLI バージョン） 187
MST の設定例 187
MST の追加情報（CLI バージョン） 189

第 11 章 **Cisco NX-OS を使用した STP 拡張の設定 191**
STP 拡張機能について 191
STP ポート タイプ 192
STP エッジ ポート 192
Bridge Assurance 192
BPDU ガード 194
BPDU フィルタリング 194
ループ ガード 195
ルート ガード 196
STP 拡張機能の適用 197
PVST シミュレーション 197
STP のハイ アベイラビリティ 198
STP 拡張機能の前提条件 198
STP 拡張機能の設定に関するガイドラインおよび制約事項 198

STP 拡張機能のデフォルト設定 200
STP 拡張機能の設定手順 200
スパニングツリー ポート タイプのグローバルな設定 200
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 203
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 205
BPDU ガードのグローバルなイネーブル化 207
指定インターフェイスでの BPDU ガードのイネーブル化 208
BPDU フィルタリングのグローバルなイネーブル化 210
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 212
ループ ガードのグローバルなイネーブル化 214
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） 218
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） 222

第 12 章 レイヤ 2 スイッチングのリフレクティブ リレーの設定 223
リフレクティブリレー802.1Qbgについて 223
リフレクティブ リレーのサポート 223
リフレクティブ リレーのガイドラインと制約事項 224
NX-OS CLI を使用したリフレクティブ リレーの設定 224

第 13 章 トラフィック ストーム制御の設定 227
トラフィック ストーム制御について 227
トラフィック ストーム制御のガイドラインと制約事項 229
トラフィック ストーム制御のデフォルト設定 233
ワンレベルのしきい値のトラフィック ストーム制御の設定 233
ツーレベルのしきい値のトラフィック ストーム制御の設定 235
トラフィック ストーム制御の設定の確認 236
トラフィック ストーム制御カウンタのモニタリング 237

トラフィック ストーム制御の設定例 237
トラフィック ストーム制御のシステム ログの例 238

はじめに

この前書きは、次の項で構成されています。

- 対象読者 （xiii ページ）
- 表記法 （xiii ページ）
- Cisco Nexus 9000 シリーズ スイッチの関連資料 （xiv ページ）
- マニュアルに関するフィードバック （xiv ページ）
- Communications, services, and additional information （xv ページ）

対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

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、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[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、角かっこで囲み、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、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y | z}]	角かっこまたは波かっこ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。角かっこ内の波かっこと縦棒は、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。
`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ないでください。引用符を使用すると、その引用符も含めて string と見なされます。

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、スクリーン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。

Cisco Nexus 9000 シリーズ スイッチの関連資料

Cisco Nexus 9000 シリーズ スイッチ全体のマニュアル セットは、次の URL にあります。

https://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

Communications, services, and additional information

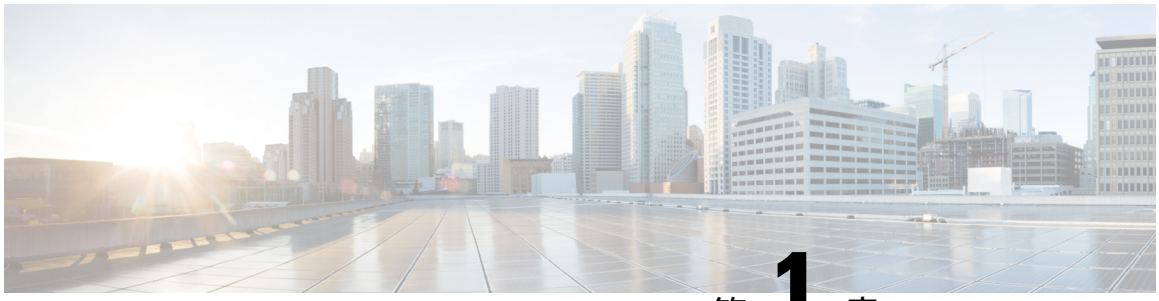
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



第 1 章

新機能および変更された機能に関する情報

この章では、「*Cisco Nexus 9000* シリーズ *NX-OS* レイヤー *2* コンフィギュレーション ガイド」に記載されている新機能および変更された機能に関するリリース固有の情報について説明します。

- 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

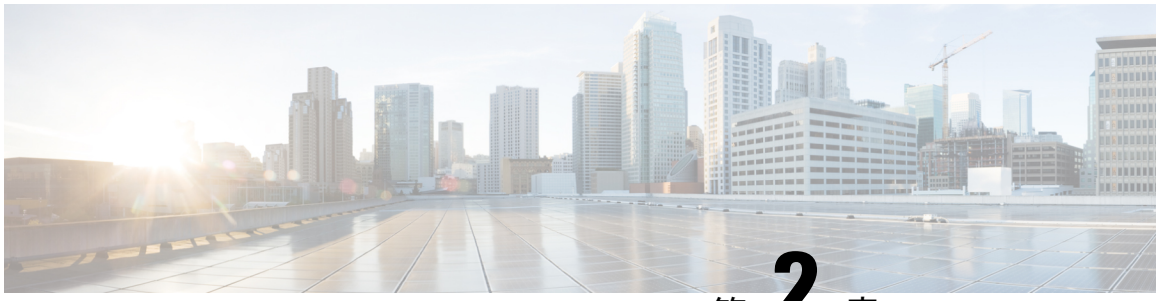
次の表は、『*Cisco Nexus 9000* シリーズ *NX-OS* レイヤ *2* スイッチング構成ガイド、リリース *10.3(x)*』に記載されている新機能および変更機能をまとめたものです。それぞれの説明が記載されている箇所も併記されています。

表 *1*: 新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
NA	このリリースで追加された新機能はありません。	10.3(1)F	該当なし

（注） Cisco NX-OS リリース 10.3(x) 以降、トラフィック ストーム制御 セクションは、『*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*』でのみ使用できます。詳細については、Cisco.com でこのガイドの適切なバージョンを選択してください。

新機能および変更された機能に関する情報



第 2 章

概要

- ライセンス要件 （3 ページ）
- サポートされるプラットフォーム （3 ページ）
- レイヤ 2 イーサネット スイッチングの概要, on page 3
- VLANs, on page 4
- スパニングツリー , on page 4
- トラフィック ストーム制御, on page 6
- 関連項目, on page 7

ライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS* ライセンス ガイド』および『*Cisco NX-OS* ライセンス オプション ガイド』を参照してください。

サポートされるプラットフォーム

Cisco NX-OS リリース 7.0(3)I7(1) 以降では、Nexus スイッチ プラットフォーム サポート マトリクスに基づいて、選択した機能をさまざまな Cisco Nexus 9000 および 3000 スイッチで使用するために、どの Cisco NX-OS リリースが必要かを確認してください。

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 コネクションは、パケットが伝送されている間だけ維持されます。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。

デバイスは、高帯域のデバイスおよび多数のユーザに起因する輻輳問題を解決するために、デバイス（サーバなど）ごとに専用のコリジョン ドメインを割り当てます。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。

イーサネット ネットワークではコリジョンによって深刻な輻輳が発生するため、全二重通信を使用することが有効な対処法の 1 つとなります。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。パケットを双方向へ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。

VLANs

VLANは、ユーザの物理的な位置に関係なく、機能、プロジェクトチーム、またはアプリケーションなどで論理的に分割されたスイッチド ネットワークです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンド ステーションもグループ化できます。

どのようなスイッチポートでもVLANに属すことができ、ユニキャスト、ブロードキャスト、マルチキャストのパケットは、その VLAN に属する端末だけに転送またはフラッディングされます。各 VLAN は 1 つの論理ネットワークであると見なされます。VLAN に属していないステーション宛てのパケットは、ブリッジまたはルータを経由して転送する必要があります。

デバイスの初回の起動時にすべてのポートがデフォルトの VLAN（VLAN1）に割り当てられます。VLAN インターフェイスまたはスイッチ仮想インターフェイス（SVI）は、VLAN 間の通信用として作成されるレイヤ 3 インターフェイスです。

このデバイスは、IEEE 802.1Q 規格に基づき、4095 の VLAN をサポートします。これらの VLAN はいくつかの範囲に分かれています。各範囲の使用法は少しずつ異なります。一部の VLAN はデバイスの内部使用のために予約されているため、設定には使用できません。

Note Cisco NX-OS では、スイッチ間リンク（ISL）はサポートされません。

スパニングツリー

ここでは、ソフトウェア上でのスパニングツリープロトコル（STP）の実装について説明します。このマニュアルでは、IEEE 802.1w および IEEE 802.1s を指す用語として、「スパニングツリー」を使用します。このマニュアルで IEEE 802.1D 規格のスパニングツリープロトコルについて記す場合は、802.1D であることを明記します。

STP の概要

STP は、レイヤ 2 レベルで、ループのないネットワークを実現します。レイヤ 2 LAN ポートは STP フレーム（ブリッジ プロトコル データ ユニット（BPDU））を一定の時間間隔で送受

信します。ネットワーク デバイスは、これらのフレームを転送せずに、フレームを使用してループフリー パスを構築します。

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

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

ソフトウェアは、従来の 802.1D システムで相互運用できますが、システムでは Rapid PVST+ および MST が実行されます。Rapid PVST+ は、Cisco Nexus デバイス用のデフォルトの STP プロトコルです。

Note Cisco NX-OS では、拡張システム ID と MAC アドレス リダクションが使用されます。これらの機能はディセーブルにできません。

また、シスコはスパニングツリーの動作を拡張するための独自の機能をいくつか作成しました。

Rapid PVST+

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

設定された各 VLAN 上で RSTP の単一インスタンスまたはトポロジが実行され、VLAN 上の各 Rapid PVST+ インスタンスに 1 つのルート デバイスが設定されます。Rapid PVST+ の実行中には、VLAN ベースで STP をイネーブルまたはディセーブルにできます。

MST

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

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

Note 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。

コマンドライン インターフェイスを使用すると、先行標準（標準ではない）の MST メッセージを指定インターフェイスで強制的に送信できます。

STP 拡張機能

このソフトウェアは、次に示すシスコ独自の機能をサポートしています。

- スパニングツリー ポート タイプ：デフォルトのスパニングツリー ポート タイプは、標準（normal）です。レイヤ 2 ホストに接続するインターフェイスをエッジ ポートとして、また、レイヤ 2 スイッチまたはブリッジに接続するインターフェイスをネットワーク ポートとして設定できます。
- ブリッジ保証：ポートをネットワーク ポートとして設定すると、ブリッジ保証によりすべてのポート上に BPDU が送信され、BPDU を受信しないポートはブロッキング ステートに移行します。この拡張機能を使用できるのは、Rapid PVST+ または MST を実行する場合だけです。
- BPDU ガード：BPDU ガードは、BPDU を受信したポートをシャットダウンします。
- BPDU フィルタ：BPDU フィルタは、ポート上での BPDU の送受信を抑制します。
- ループ ガード：ループ ガードを使用すると、ポイントツーポイント リンク上の単方向リンク障害によって発生するブリッジング ループを防止できます。
- ルート ガード：STP ルート ガードを使用すると、ポートがルート ポートまたはブロッキングされたポートになることが防止されます。ルート ガードに設定されたポートが上位 BPDU を受信すると、このポートはただちにルートとして一貫性のない（ブロックされた）ステートになります。

トラフィック ストーム制御

トラフィック ストーム制御（トラフィック抑制ともいいます）を使用すると、着信トラフィックのレベルを 1 秒より大きなインターバルでモニタできます。この間、トラフィック レベル（ポートの使用可能合計帯域幅に対するパーセンテージ）が、設定したトラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。

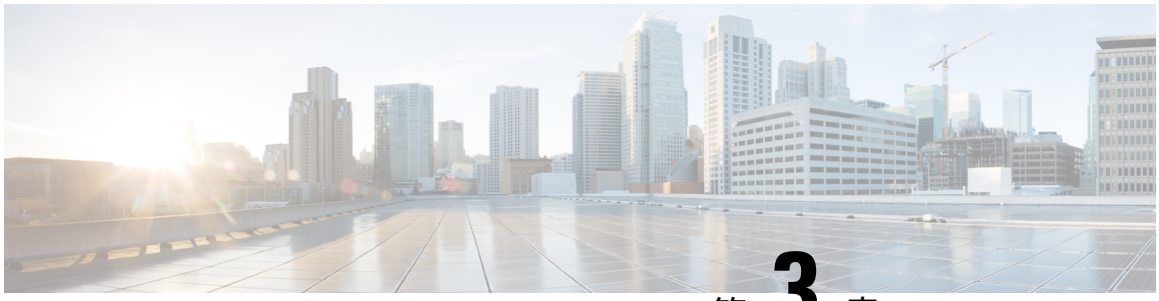
詳細については、トラフィック ストーム制御の設定, on page 227の章を参照してください。

関連項目

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 9000 Series NX-OS Interfaces Configuration Guide*』
- 『*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*』
- 『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』
- 『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』

関連項目



第 3 章

レイヤ 2 スイッチングの設定

- レイヤ 2 スイッチングについて （9 ページ）
- スイッチングのハイ アベイラビリティ, on page 11
- MAC アドレス設定の前提条件 （12 ページ）
- レイヤ 2 スイッチングのデフォルト設定 （12 ページ）
- レイヤ 2 スイッチングの設定手順 （12 ページ）
- レイヤ 2 スイッチング設定の確認 （20 ページ）
- レイヤ 2 スイッチングの設定例 （21 ページ）
- レイヤ 2 スイッチングの追加情報（CLI バージョン） （22 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については、『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』を参照してください。https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/92x/interfaces/configuration/guide/b-cisco-nexus-9000-nx-os-interfaces-configuration-guide-92x.htmlhttps://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/interfaces/configuration/guide/b-cisco-nexus-9000-nx-os-interfaces-configuration-guide-93x.html

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

（注） 『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』高可用性機能の詳細については、を参照してください。 https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/92x/High_Availability_and_Redundancy_Guide/configuration/guide/b-cisco-nexus-9000-nx-os-High-availability-and-redundancy-guide-92x.htmlhttps://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/high-availability-and-redundancy/configuration/guide/b-cisco-nexus-9000-nx-os-High-availability-and-redundancy-guide-93x.html

レイヤ 2 イーサネット スイッチングの概要

このデバイスは、レイヤ2イーサネットセグメント間の同時パラレル接続をサポートします。イーサネット セグメント間のスイッチド コネクションは、パケットが伝送されている間だけ維持されます。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。

デバイスは、高帯域のデバイスおよび多数のユーザに起因する輻輳問題を解決するために、デバイス（サーバなど）ごとに専用のコリジョン ドメインを割り当てます。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。

イーサネット ネットワークではコリジョンによって深刻な輻輳が発生するため、全二重通信を使用することが有効な対処法の 1 つとなります。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。パケットを双方向へ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。

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 デバイスのメディア アクセス コントロール（MAC）アドレスを関連付けます。

アドレス テーブルの構築およびアドレス テーブルの変更

デバイスは、受信したフレームの送信元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。

仮想ポート チャネル（vPC）ピア リンクにより接続されている両方のデバイスに、同一のスタティック 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の詳細については、『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』を参照してください。https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/92x/interfaces/configuration/guide/b-cisco-nexus-9000-nx-os-interfaces-configuration-guide-92x.htmlhttps://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/interfaces/configuration/guide/b-cisco-nexus-9000-nx-os-interfaces-configuration-guide-93x.html

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。

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。**show forwarding consistency l2** コマンドまたは **show consistency-checker l2** コマンドを入力すると、不一致、欠落、および余分の MAC アドレス エントリが表示されます。

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。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。

Note ハイ アベイラビリティ機能の詳細については、次を参照してください。*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy GuideCisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide

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、アドバンスド サービスのライセンスをインストールします。

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

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、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

スタティック MAC アドレスの設定

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

SUMMARY STEPS

1. **config t**

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

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**mac address-table static** *mac-address* **vlan** *vlan-id* {[**drop** | **interface** {*type slot/port*} | **port-channel** *number*]} **Example:** `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。 **Note** **drop** オプションを使用すると、指定した VLAN で構成されたMAC アドレスに向かうすべてのトラフィックがドロップされます。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show mac address-table static** **Example:** `switch# show mac address-table static`	スタティック MAC アドレスを表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

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)#
```

システムでの MAC アドレス学習の無効化

システムで MAC アドレス学習を無効にしてから、再度有効にできるようになりました。

手順の概要

1. switch# **configure terminal**
2. switch(config-if)# **[no] mac-learn disable**
3. switch(config-if)# **clear mac address-table dynamic**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config-if)# **[no] mac-learn disable**	スイッチでの MAC アドレス学習を無効にします。 このコマンドの **no** 形式を使用すると、スイッチでの MAC アドレス学習が再度有効になります。
ステップ 3	switch(config-if)# **clear mac address-table dynamic**	スイッチの MAC アドレステーブルをクリアします。 **重要** スイッチで MAC アドレス学習を無効化した後には、MAC アドレステーブルを必ずクリアしてください。

レイヤ 2 インターフェイスでの MAC アドレス学習の無効化

レイヤ 2 インターフェイスで MAC アドレス ラーニングを無効にしてから再度有効にできるようになりました。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. switch(config-if)# **[no] switchport mac-learn disable**
4. switch(config-if)# **clear mac address-table dynamic interface** *type slot/port*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	指定したインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **[no] switchport mac-learn disable**	レイヤ 2 インターフェイスでの MAC アドレス学習の無効化 **no** フォームのコマンドは、レイヤ2インターフェイスでのMACアドレス学習の再イネーブル化します。 （注） ワープ モードでは、Cisco Nexus 3500 スイッチは、**switchport mac-learn disable**を使用して構成されたポートが存在する VLAN にレイヤ 3 トラフィックをフラッディングせず、トラフィックはドロップされます。通常モードでは、スイッチはレイヤ3トラフィックをこの VLAN にフラッディングする必要があります。
ステップ 4	switch(config-if)# **clear mac address-table dynamic interface** *type slot/port*	指定されたインターフェイスの MAC アドレス テーブルをクリアします。 **重要** インターフェイスでMACアドレス ラーニングを無効化した後、MAC アドレス テーブルを必ずクリアしてください。

例

次の例では、レイヤ 2 インターフェイスで MAC アドレス ラーニングをディセーブルにする方法を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# switchport mac-learn disable
switch(config-if)# clear mac address-table dynamic interface ethernet 1/4
```

次の例では、レイヤ 2 インターフェイスで MAC アドレス ラーニングを再イネーブル化する方法を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# no switchport mac-learn disable
```

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。

Note MAC アドレスのエージング タイムアウトの最大時間は、設定された MAC アドレス テーブルのエージング タイムアウトの 2 倍です。

Note 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。

SUMMARY STEPS

1. **config t**
2. **mac address-table aging-time** *seconds*
3. **exit**
4. (Optional) **show mac address-table aging-time**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**mac address-table aging-time** *seconds* **Example:** `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** **Example:**	コンフィギュレーション モードを終了します。

	Command or Action	Purpose
	`switch(config)# exit` `switch#`	
ステップ 4	(Optional) **show mac address-table aging-time** **Example:** `switch# show mac address-table aging-time`	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	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

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

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

MAC アドレス テーブルの整合性検査

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。

SUMMARY STEPS

1. **show consistency-checker l2 module** <*slot_number*>

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**show consistency-checker l2 module** <*slot_number*>
	Example:
	`switch# show consistency-checker l2 module 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。

Example

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 consistency-checker l2 module 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。（指定したインターフェイスまたは VLAN によりエントリをクリアすることもできます。）

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**clear mac address-table dynamic** {**address** *mac_addr*} {**interface** [**ethernet** *slot/port* | **port-channel** *channel-number*]} {**vlan** *vlan_id*} **Example:** `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。
ステップ 2	(Optional) **show mac address-table** **Example:** `switch# show mac address-table`	MAC Address Table を表示します。

Example

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#
```

MAC アドレス制限の設定

SUMMARY STEPS

1. **config t**
2. **mac address-table limit vlan** *vlan-id limit -value*
3. **exit**

4. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**mac address-table limit vlan** *vlan-id limit -value* **Example:** `switch(config-vlan)# mac address-table limit vlan 40 108`	VLAN を適用すべき MAC アドレス制限に指定します。

ステップ 3	**exit**
	Example:
	`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	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

L2 ヘビー モードの設定

この機能の目的は、新規の L2 ヘビー テンプレートを分類し、FP タイル ハードウェア リソースの割り当てを変更し、必要な制御プレーンの変更を行うことで現在の 92k MAC アドレスのスケールを 200k に増加させ、ISSU の復元が新しいスケールへの適合をサポートできるようにすることです。

コマンド	目的
sh system routing mode	設定済みおよび適用済みモードを表示します

コマンド	目的
system routing template-l2-heavy	200K MAC をイネーブルにします。200K MAC は、このモードが設定され、システムがリロードされた場合にのみ有効になります。 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。 （注） Cisco NX-OS リリース 10.2(2)F 以降、MAC は Cisco N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。
sh run | i system	適用済みのモードを実行します。

ガイドラインおよび制約事項:

- この機能はレイヤ 2 の 1 次元スケールのみサポートします。
- SVI、レイヤ 3 インターフェイス、および VXLAN VLAN はサポートされません。
- Cisco NX-OS リリース 9.2(3) 以降、この機能は N9K-C9264PQ、N9K-C9272Q、N9K-C9236C、N9K-C92300YC、N9K-C92304QC、N9K-C9232C、N9K-C92300YC、および 9300-EX の各プラットフォームをサポートしています。
- Cisco NX-OS リリース 10.2(2)F 以降、200K MAC は Cisco N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。

次は、L2 ヘビー モードの設定の例を表示します。

```
switch (config)# sh system routing mode
switch# Configured System Routing Mode: L2 Heavy
switch# Applied System Routing Mode: L2 Heavy
switch#
switch# show run | i system
switch# system routing template-l2-heavy
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。

コマンド	目的
show mac address-table limit	MACアドレステーブルの制限設定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。 （注） Cisco NX-OS リリース 10.2（1）以降、Cloudscale ASIC を使用する Cisco Nexus 9000 と Nexus 3000 スイッチは、show mac address 出力で MAC の経過時間を報告しません。age カラムは無視できます。以前のリリースで報告された固定値 0 の代わりに、NA が報告されるようになりました。これは表示上の制限にすぎません。MAC エージングは引き続き機能的に適用されます。
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。

レイヤ 2 スイッチングの設定例

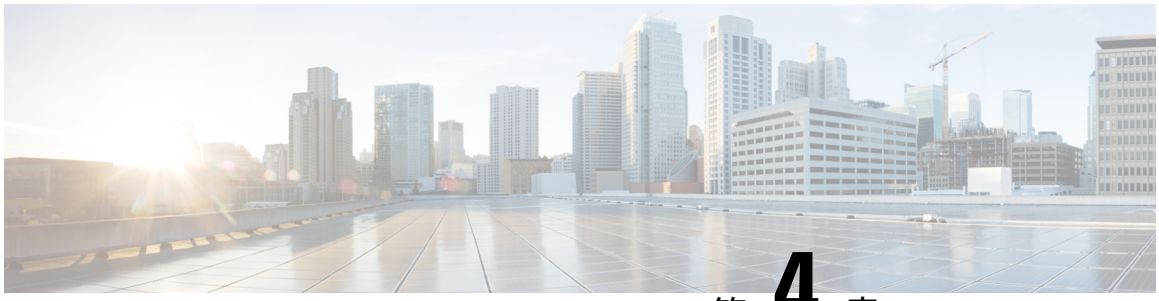
次に、スタティック MAC アドレスを追加し、MAC アドレスのデフォルトのグローバル エージング タイムを変更する例を示します。

```
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	マニュアル タイトル
スタティック MAC アドレス	『*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*』
インターフェイス	『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』
高可用性	『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』
システム管理	『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』



第 4 章

Flex Link の設定

この章では、Cisco NX-OS 9000 シリーズ スイッチで Flex Link を設定する方法について説明します。Flex Link は相互バックアップを提供するインターフェイスのペアです。

この章は、次の項目を取り上げます。

- Flex Link について （23 ページ）
- 注意事項と制約事項 （25 ページ）
- デフォルト設定 （26 ページ）
- Flex Link の設定 （27 ページ）
- 設定の確認 （31 ページ）

Flex Link について

このセクションは、次のトピックで構成されています。

Flex Link

Flex Link はレイヤ 2 インターフェイス（スイッチポートまたはポート チャネル）のペアであり、片方のインターフェイスが他方のバックアップとして動作するように設定されています。

この機能は、スパニングツリー プロトコル（STP）の代替ソリューションとして提供され、ユーザが STP をオフにしても、基本的なリンク冗長性は確保されます。通常、カスタマーがスイッチで STP を実行しないネットワークの Flex Link を設定します。スイッチで STP を設定する場合、STP がすでにリンク レベルの冗長性またはバックアップを提供しているので Flex Link の設定は必要ありません。

（注） STP は、ネットワーク ノードインターフェイス（NNI）上で、デフォルトでイネーブルに設定されています。拡張ネットワーク インターフェイス（ENI）ではディセーブルに設定されていますが、イネーブルにできます。STP は、ユーザネットワーク インターフェイス（UNI）ではサポートされていません。

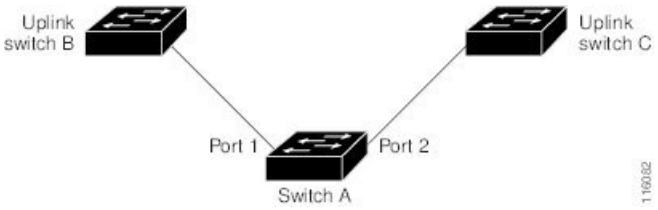
別のレイヤ 2 インターフェイスを Flex Link またはバックアップ リンクとして割り当てることで、1 つのレイヤ 2 インターフェイス（アクティブ リンク）に Flex Link を設定します。リンクの 1 つがアップでトラフィックを転送しているときは、もう一方のリンクがスタンバイ モードで、このリンクがシャットダウンした場合にトラフィックの転送を開始できるように準備しています。どの時点でも、1 つのインターフェイスのみがリンクアップ ステートでトラフィックを転送しています。プライマリ リンクがシャットダウンされると、スタンバイ リンクがトラフィックの転送を開始します。アクティブ リン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

次の図の **Flex Links コンフィギュレーションの例** で、A のポート 1 と 2 はアップリンクスイッチ B と C に接続されています。それらは Flex Link として設定されているため、インターフェイスのうち 1 つだけがトラフィックを転送し、その他はスタンバイモードになります。ポート 1 がアクティブ リンクである場合、ポート 1 とスイッチ B との間でトラフィックの転送が開始され、ポート 2（バックアップ リンク）とスイッチ C との間のリンクでは、トラフィックは転送されません。ポート 1 がダウンすると、ポート 2 がアップ状態になってスイッチ C へのトラフィックの転送を開始します。ポート 1 が再びアップ状態に戻ってもスタンバイ モードになり、トラフィックを転送しません。ポート 2 がトラフィック転送を続けます。

プリエンプション

また、優先してトラフィックの転送に使用するポートを指定して、プリエンプション メカニズムを設定することもできます。次の図で、たとえば、Flex Link ペアをプリエンプション モードで設定できます。このシナリオでは、ポート 1 がバックアップ状態になったあと、ポート 1 の帯域幅がポート 2 よりも大きい場合、ポート 1 は 35 秒後に転送を開始し、ポート 2 はスタンバイになります。これを行うには、switchport backup interface preemption mode bandwidth および switchport backup interface preemption delay インターフェイス コンフィギュレーション コマンドを入力します。

図 *1 : Flex Link* の設定例



プライマリ（転送）またはリンクがダウンすると、トラップによってネットワーク管理ステーションが通知を受けます。Flex Link はレイヤ 2 ポートおよびポート チャネルだけでサポートされます。 **trunk access** VLANまたはレイヤ3ポートではサポートされません。

マルチキャスト

Flex Link インターフェイスが mrouter ポートとして学習されると、リンクアップしている場合、スタンバイ（非転送）インターフェイスも mrouter ポートとして相互学習されます。この相互学習は、内部ソフトウェアのステート メンテナンス用であり、マルチキャスト高速コン

バージェンスがイネーブルでない限り、IGMP 動作またはハードウェア転送に対して関連性はありません。マルチキャスト高速コンバージェンスを設定すると、相互学習された mrouter ポートがただちにハードウェアに追加されます。Flex Link では、IPv4 IGMP のマルチキャスト高速コンバージェンスをサポートしています。

注意事項と制約事項

Flex Link を設定する場合は、次のガイドラインおよび制約事項を考慮してください。

- Flex link は次のプラットフォームでサポートされます: Cisco Nexus 9300-EX、9300-FX、9300-FX2、C9364C スイッチ
- Flex Link は、IPv4 マルチキャストの Cisco Nexus 9300-FX、9300-FX2、および 9348GC-FXP スイッチでサポートされます。
- Flex Link インターフェイスで、スパニング ツリー プロトコルは明示的にディセーブルになっているため、同じトポロジーでその他の冗長パスを設定してループを発生させないように確認してください。また、spanning-tree ポート タイプの標準コマンドを使用して、アップストリーム スイッチに対応するリンクを設定します。これにより、Bridge Assurance によってブロックされないようになります。
- Flex Link はアップリンク インターフェイス向けに設計されます。これは通常トランク ポートとして設定されます。リンク バックアップ メカニズムとして、Flex Link ペアは同じ設定の内容（同じスイッチポート モードおよび許可済み VLAN のリスト）を持つ必要があります。Port-profile は Flex Link ペアの設定などをアップするための便利なツールです。Flex Link では、2 つのインターフェイスが同じ設定であることは必須ではありません。ただし、設定が長期間不一致であることはフォーワーディングの問題、特にファイルオーバーの間に、問題が生じる可能性があります。
- Flex Link は、次のインターフェイス タイプで設定できません。
  - レイヤ 3 インターフェイス
  - SPAN 宛先
  - ポート チャネル メンバー
  - プライベート VLAN を使用して設定されているインターフェイス
  - エンド ノード モードのインターフェイス
  - レイヤ 2 マルチパス化
- 任意のアクティブ リンクに対して設定可能な Flex Link バックアップ リンクは 1 つだけで、アクティブ インターフェイスとは異なるインターフェイスでなければなりません。
- インターフェイスが所属できる Flex Link ペアは 1 つだけです。つまり、インターフェイスは 1 つのアクティブ リンクに対してだけ、バックアップ リンクになることができます。

- どちらのリンクも、EtherChannelに属するポートには設定できません。ただし、2つのポート チャネル（EtherChannel 論理インターフェイス）を Flex Link として設定でき、ポート チャネルおよび物理インターフェイスを Flex Link として設定して、ポート チャネルか物理インターフェイスのどちらかをアクティブ リンクにすることができます。
- バックアップ リンクはアクティブ リンクと同じタイプ（ビット イーサネットまたはポート チャネル）にする必要はありません。ただし、スタンバイ リンクがトラフィック転送を開始した場合にループが発生したり動作が変更したりしないように、両方の Flex Link を同様の特性で設定する必要があります。
- STP は Flex Link ポートでディセーブルです。ポート上にある VLAN が STP 用に設定されている場合でも、Flex Link ポートは STP に参加しません。STP がイネーブルでない場合は、設定されているトポロジでループが発生しないようにしてください。

（注） STP を使用できるのは、NNI または ENI 上だけです。

- STP 機能（たとえば、PortFast、および BPDU ガード）を Flex Link ポートで設定しないでください。
- Flex Link ペアでデフォルト インターフェイス CLI（アクティブおよびスタンバイ）はサポートされていません。ブレークアウト/インのいずれかがプライマリまたはスタンバイ インターフェイスで実行されている場合、Flex Link 設定は削除されます。
- vPC はサポートされていません。Flex Link は、設定の簡素化が求められ、アクティブ-アクティブ冗長の必要性がない vPC の代わりに使用されます。
- Cisco NX-OS リリース 9.3(5) 以降、Flex Link 機能は Cisco Nexus 9300-GX、N9K-C93108TC-FX3H、および N9K-C93108TC-FX3P プラットフォーム スイッチでサポートされています。
- Cisco NX-OS リリース 10.1(1) 以降、Flex Link 機能は Cisco N9K-C93180YC-FX3 プラットフォーム スイッチでサポートされています。
- Cisco NX-OS リリース 10.2(2)F 以降、PVLAN と Flex Link 機能は Cisco N9K-9332D-GX2B プラットフォーム スイッチでサポートされています。

デフォルト設定

パラメータ	デフォルト
Flex Link	ディセーブル
Multicast Fast-Convergence	ディセーブル
Flex Linkプリエンプションモード	オフ

パラメータ	デフォルト
Flex Linkプリエンプション遅延	35 秒

Flex Link の設定

FlexLink の設定

レイヤ 2 インターフェイス（スイッチ ポートまたはポート チャネル）のペアを、1 つのインターフェイスがもう一方のバックアップとして機能するように設定されている Flex Link インターフェイスとして設定できます。

始める前に

これらは、この機能のガイドラインおよび制限事項です。（ガイドラインと制約事項を参照してください。）

手順の概要

1. **configure terminal**
2. **feature flexlink**
3. **interface**{ **ethernet** *slot*/ *port* | **port-channel** *channel no*
4. **switchport backup interface** {**ethernet** *slot*/ *port* | **port-channel** *channel-no*} [**multicast fast-convergence**]
5. （任意） **end**
6. （任意） **show interface switchport backup**
7. （任意） **copy running-config startup config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**feature flexlink**	Flex Link をイネーブルにします。
ステップ 3	**interface**{ **ethernet** *slot*/ *port*	**port-channel** *channel no*	イーサネットまたはポート チャネル 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。

	コマンドまたはアクション	目的
ステップ 4	**switchport backup interface** {**ethernet** *slot/ port* | **port-channel** *channel-no*} [**multicast fast-convergence**]	Flex Link ペアのバックアップ インターフェイスとして物理レイヤ 2 インターフェイス（イーサネットまたはポート チャネル）を指定します。1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。 • ethernet slot/port：バックアップ イーサネット インターフェイスを指定します。スロット番号は 1～2、ポート番号は 1～48 です。 • port-channel port-channel-no：バックアップ ポート チャネル インターフェイスを指定します。port-channel-no の番号は 1 ～ 4096 です。 • multicast：マルチキャスト パラメータを指定します。 • fast-convergence：バックアップ インターフェイスの高速コンバージェンスを設定します。
ステップ 5	（任意） **end**	特権 EXEC モードに戻ります。
ステップ 6	（任意） **show interface switchport backup**	設定を確認します。
ステップ 7	（任意） **copy running-config startup config**	スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

例

次の例は、イーサネット スイッチポート バックアップのペア（イーサネット 1/1 がアクティブなインターフェイスであり、イーサネット 1/2 がバックアップ インターフェイスである）を設定する方法を示しています。

```
switch(config)# feature flexlink
switch(config)# interface ethernet 1/1
switch(config-if)# switchport backup interface ethernet 1/2
switch(config-if)# exit
switch(config)# interface port-channel300
switch(config-if)# switchport backup interface port-channel301
switch(config-if)# show ip igmp snooping mrouter
Type: S - Static, D - Dynamic, V - vPC Peer Link,
      I - Internal,C - Co-learned, U - User Configured
Vlan  Router-port   Type      Uptime      Expires
200   Po300          D         13:13:47    00:03:15
200   Po301          DC        13:13:47    00:03:15
```

次の例は、マルチキャスト高速コンバージェンスを使用した、ポート チャネル スイッチポート バックアップのペアを設定する方法を示しています。

```
switch(config)# interface port-channel10
switch(config-if)# switchport backup interface port-channel20 multicast fast-convergence
```

次の例は、Flex Link インターフェイス（po305 と po306）のマルチキャスト コンバージェンスの例を示します。po305 で一般クエリーを受信すると、mrouter ポートと po306 が相互学習されます。

```
switch(config)# interface po305
Switch(config-if)# switchport backup interface po306
switch# show ip igmp snooping mrouter
Type: S - Static, D - Dynamic, V - vPC Peer Link, I - Internal, C - Co-learned
Vlan  Router-port   Type      Uptime      Expires
4     Po300         D         00:00:12    00:04:50
4     Po301         DC        00:00:12    00:04:50
```

Flex Link プリエンプションの設定

Flex Links ペア（アクティブ リンクおよびバックアップ リンク）のプリエンプション スキームを設定します。

始める前に

これらは、この機能のガイドラインおよび制限事項です。（ガイドラインと制約事項を参照してください。）

Flex Link の定義および有効化(Flex Link の設定を参照してください。)

割り当てるポートがある場合、プリエンプション モードの内容を決めてください。(プリエンプション を参照してください。)

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **switchport backup interface ethernet** *slot/port*
4. **switchport backup interface ethernet** *slot / port* **preemption mode {forced | bandwidth | off}**
5. **switchport backup interface ethernet** *slot / port* **preemption delay** *delay-time*
6. （任意） **end**
7. （任意） **show interface switchport backup**
8. （任意） **copy running-config startup config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface ethernet** *slot/port*	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インター

	コマンドまたはアクション	目的
		フェイスは物理レイヤ 2 インターフェイスまたはポートチャネル（論理インターフェイス）に設定できます。
ステップ 3	**switchport backup interface ethernet** *slot/port*	物理レイヤ2インターフェイス（またはポートチャネル）を、インターフェイスを装備したFlex Linkペアの一部として設定します。1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 4	**switchport backup interface ethernet** *slot / port* **preemption mode {forced | bandwidth | off}**	物理レイヤ 2 インターフェイス（イーサネットまたはポートチャネル）を、Flex Linkペアの一部として設定します。1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。 • preemption：バックアップ インターフェイス ペアのプリエンプション スキームを設定します。 • mode：プリエンプション モードを指定します。 Flex Link インター ペアのプリエンプション メカニズムとプリエンプション遅延を設定します。次のプリエンプション モードを設定することができます。 • **forced**：アクティブインターフェイスが常にバックアップインターフェイスより先に使用されます。 • **bandwidth**：より大きい帯域幅のインターフェイスが常にアクティブインターフェイスとして動作します。 • **off**：アクティブからバックアップへのプリエンプションは発生しません。 （注） 帯域幅プリエンプション モードの間、帯域幅の変更のみが考慮されます。速度の変更は無視されます。
ステップ 5	**switchport backup interface ethernet** *slot / port* **preemption delay** *delay-time*	ポートが他のポートより先に使用されるまでの遅延時間を設定します。delay-time の範囲は 1 ～ 300 秒です。デフォルトのプリエンプション遅延は 35 秒です。 （注）

	コマンドまたはアクション	目的
		遅延時間の設定は、forced モードおよび bandwidth モードでのみ有効です。
ステップ 6	（任意） **end**	特権 EXEC モードに戻ります。
ステップ 7	（任意） **show interface switchport backup**	設定を確認します。
ステップ 8	（任意） **copy running-config startup config**	スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

例

次に、プリエンプション モードを強制に設定し、遅延時間を 50 に設定し、設定を確認する方法の例を示します。

```
switch(config)# configure terminal
switch(config)# interface ethernet 1/48
switch(config-if)# switchport backup interface ethernet 1/4 preemption mode forced
switch(config-if)# switchport backup interface ethernet 1/4 preemption delay 50
switch(config-if)# end
switch# show interface switchport backup detail


Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------

Ethernet1/48            Ethernet1/4             Active Down/Backup Down
        Preemption Mode  : forced
        Preemption Delay : 50 seconds
        Multicast Fast Convergence  : Off
        Bandwidth : 10000000 Kbit (Ethernet1/48), 10000000 Kbit (Ethernet1/4)
```

設定の確認

コマンド	目的
show interface switchport backup	すべてのスイッチ ポート Flex Link インターフェイスに関する情報を表示します。
show interface switchport backup detail	すべてのスイッチ ポート Flex Link インターフェイスの詳細情報を表示します。
show running-config backup **show startup-config backup**	バックアップインターフェイスの実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーションを表示します。

コマンド	目的
show running-config flexlink **show startup-config flexlink**	Flex Linkインターフェイスの実行コンフィギュレーションファイルまたはスタートアップコンフィギュレーションを表示します。

次の例は、Flex Link ペアのサマリー設定を示します。

```
9k-203-Pip(config)# show interface switchport backup


Switch Backup Interface Pairs:

Active Interface Backup Interface State
------------------------------------------------------------------------
Ethernet1/9 port-channel103 Active Standby/Backup Up
Ethernet1/12 Ethernet1/13 Active Up/Backup Standby
Ethernet1/21 port-channel203 Active Up/Backup Standby
Ethernet1/24 Ethernet1/25 Active Up/Backup Standby
port-channel301 port-channel302 Active Down/Backup Up


k-203-Pip(config)# show interface switchport backup detail


Switch Backup Interface Pairs:

Active Interface Backup Interface State
------------------------------------------------------------------------
Ethernet1/9 port-channel103 Active Standby/Backup Up
Preemption Mode : bandwidth
Preemption Delay : 1 seconds
Multicast Fast Convergence : On
Bandwidth : 1000000 Kbit (Ethernet1/9), 2000000 Kbit (port-channel103)

..
```

次の例は、すべてのスイッチ ポート Flex Link インターフェイスに関する情報を示します。

```
switch# show interface switchport backup


Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
Ethernet1/1             Ethernet1/2             Active Down/Backup Down
Ethernet1/8             Ethernet1/45            Active Down/Backup Down
Ethernet1/48            Ethernet1/4             Active Down/Backup Down
port-channel10          port-channel20          Active Down/Backup Up
port-channel300         port-channel301         Active Down/Backup Down
```

次の例は、すべてのスイッチ ポート Flex Link インターフェイスの詳細を示します。

```
switch# show interface switchport backup detail


Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
```

```
--------------------------------------------------------------------------------
Ethernet1/1             Ethernet1/2             Active Down/Backup Down
        Preemption Mode  : off
        Multicast Fast Convergence  : Off
        Bandwidth : 10000000 Kbit (Ethernet1/1), 10000000 Kbit (Ethernet1/2)

Ethernet1/8             Ethernet1/45            Active Down/Backup Down
        Preemption Mode  : forced
        Preemption Delay : 10 seconds
        Multicast Fast Convergence  : Off
        Bandwidth : 10000000 Kbit (Ethernet1/8), 10000000 Kbit (Ethernet1/45)

Ethernet1/48            Ethernet1/4             Active Down/Backup Down
        Preemption Mode  : forced
        Preemption Delay : 50 seconds
        Multicast Fast Convergence  : Off
        Bandwidth : 10000000 Kbit (Ethernet1/48), 10000000 Kbit (Ethernet1/4)

port-channel10          port-channel20          Active Down/Backup Up
        Preemption Mode  : forced
        Preemption Delay : 10 seconds
        Multicast Fast Convergence  : Off
        Bandwidth : 100000 Kbit (port-channel10), 10000000 Kbit (port-channel20)

port-channel300         port-channel301         Active Down/Backup Down
        Preemption Mode  : off
        Multicast Fast Convergence  : Off
        Bandwidth : 100000 Kbit (port-channel300), 100000 Kbit (port-channel301)
```

次の例は、バックアップ インターフェイスの実行コンフィギュレーションを示します。

```
switch# show running-config backup

!Command: show running-config backup
!Time: Sun Mar  2 03:05:17 2014

version 6.0(2)A3(1)
feature flexlink


interface port-channel10
  switchport backup interface port-channel20 preemption mode forced
  switchport backup interface port-channel20 preemption delay 10

interface port-channel300
  switchport backup interface port-channel301

interface Ethernet1/1
  switchport backup interface Ethernet1/2

interface Ethernet1/8
  switchport backup interface Ethernet1/45 preemption mode forced
  switchport backup interface Ethernet1/45 preemption delay 10

interface Ethernet1/48
  switchport backup interface Ethernet1/4 preemption mode forced
  switchport backup interface Ethernet1/4 preemption delay 50
```

次の例は、バックアップインターフェイスのスタートアップ コンフィギュレーションを表示します。

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

```
!Command: show startup-config backup
!Time: Sun Mar  2 03:05:35 2014
!Startup config saved at: Sun Mar  2 02:54:58 2014

version 6.0(2)A3(1)
feature flexlink


interface port-channel10
  switchport backup interface port-channel20 preemption mode forced
  switchport backup interface port-channel20 preemption delay 10

interface Ethernet1/8
  switchport backup interface Ethernet1/45 preemption mode forced
  switchport backup interface Ethernet1/45 preemption delay 10
```

次の例は、バックアップインターフェイスのスタートアップコンフィギュレーションを表示します。

```
switch# show startup-config backup

!Command: show startup-config backup
!Time: Sun Mar  2 03:05:35 2014
!Startup config saved at: Sun Mar  2 02:54:58 2014

version 6.0(2)A3(1)
feature flexlink


interface port-channel10
  switchport backup interface port-channel20 preemption mode forced
  switchport backup interface port-channel20 preemption delay 10

interface Ethernet1/8
  switchport backup interface Ethernet1/45 preemption mode forced
  switchport backup interface Ethernet1/45 preemption delay 10
```

次の例は、Flex Link の実行コンフィギュレーションを示しています。

```
switch# show running-config flexlink

!Command: show running-config flexlink
!Time: Sun Mar  2 03:11:49 2014

version 6.0(2)A3(1)
feature flexlink


interface port-channel10
  switchport backup interface port-channel20 preemption mode forced

interface port-channel300
  switchport backup interface port-channel301

interface port-channel305
  switchport backup interface port-channel306

interface Ethernet1/1
  switchport backup interface Ethernet1/2

interface Ethernet1/8
  switchport backup interface Ethernet1/45 preemption mode forced
  switchport backup interface Ethernet1/45 preemption delay 10
```

```
interface Ethernet1/48
  switchport backup interface Ethernet1/4 preemption mode forced
  switchport backup interface Ethernet1/4 preemption delay 50
```

次の例は、Flex Link のスタートアップ コンフィギュレーションを示しています。

```
switch# show startup-config flexlink

!Command: show startup-config flexlink
!Time: Sun Mar  2 03:06:00 2014
!Startup config saved at: Sun Mar  2 02:54:58 2014

version 6.0(2)A3(1)
feature flexlink


interface port-channel10
  switchport backup interface port-channel20 preemption mode forced
  switchport backup interface port-channel20 preemption delay 10

interface Ethernet1/8
  switchport backup interface Ethernet1/45 preemption mode forced
  switchport backup interface Ethernet1/45 preemption delay 10
```

（注） を使用する前に、すべてのFlexLinkペアの設定を無効にする必要があります。**no feature flexlink**

確認するために、次のように実行すると確認メッセージが表示されます。**no feature flexlink**

```
"WARNING!!! Please remove all flexlink configuration before disabling feature flexlink.

Failure to do so may put ports in inconsistent state. Do you want to proceed? Y/N :"
```

このメッセージは、DMEがシステムで有効になっている場合にのみ表示されます。

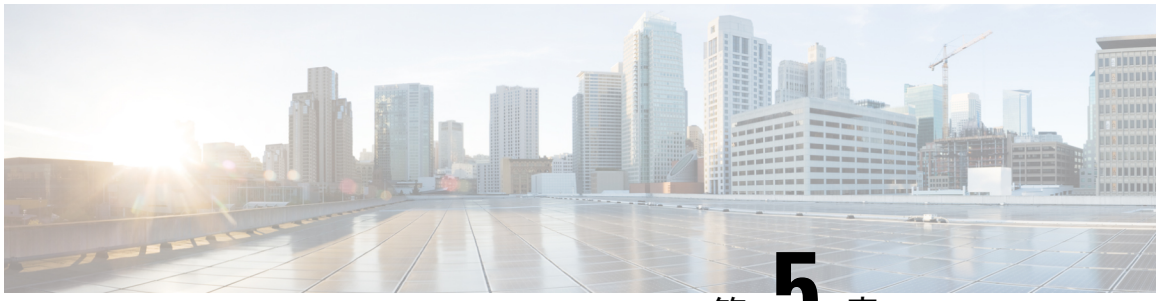
ユーザがこのコマンドを続行することを選択した場合、フレックスリンクピア設定は実行コンフィギュレーションに残ります。

これにより、FlexLink設定の一部であるポートでシステムの不整合が発生する可能性があります。

システムが不整合状態になると、ユーザはシステムを回復する必要があります。

回復するには、コマンドを使用して再設定し、コマンドを使用して各インターフェイスペアの設定を削除する必要があります。**feature flexlinkno switchport backup interface Ethernet x/y**

すべてのペア設定が削除されると、ユーザは実行できます。**no feature flexlink**



第 5 章

VLAN の設定

- VLAN について, on page 37
- VLAN 設定の前提条件, on page 42
- VLAN の設定に関するガイドラインおよび制約事項 （42 ページ）
- VLAN のデフォルト設定, on page 43
- VLAN の設定, on page 44
- VLAN の設定の確認, on page 54
- VLAN 統計情報の表示とクリア, on page 54
- VLAN の設定例, on page 54
- VLAN に関する追加情報, on page 55

VLAN について

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

どのようなスイッチポートでもVLANに属すことができ、ユニキャスト、ブロードキャスト、マルチキャストのパケットは、その VLAN に属する端末だけに転送またはフラッディングされます。各 VLAN は論理ネットワークと見なされ、VLAN に属さないステーション宛てのパケットはルータで転送する必要があります。

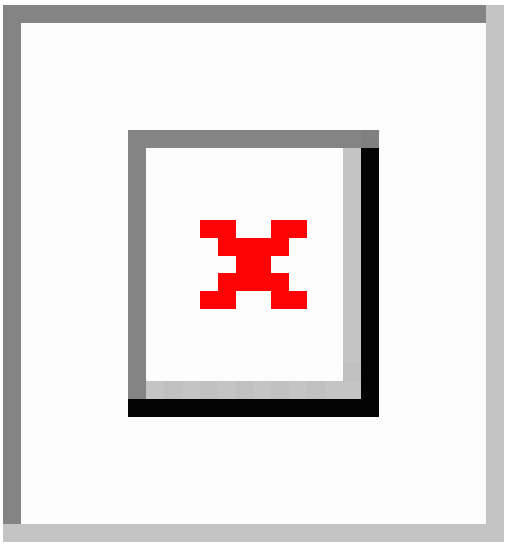
VLAN の概要

VLANは、ユーザの物理的な場所に関係なく、機能またはアプリケーションによって論理的にセグメント化されるスイッチド ネットワーク内の端末のグループです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンド ステーションもグループ化できます。

どのようなスイッチポートでもVLANに属すことができ、ユニキャスト、ブロードキャスト、マルチキャストのパケットは、その VLAN に属する端末だけに転送またはフラッディングされます。各 VLAN は 1 つの論理ネットワークであると見なされます。VLAN に属していないステーション宛てのパケットは、ルータを経由して転送する必要があります。次の図は、論理ネットワークとしての VLAN を図示したものです。エンジニアリング部門のステーション、

マーケティング部門のステーション、および会計部門のステーションはそれぞれ別の VLAN に割り当てられています。

Figure 2: 論理的に定義されたネットワークとしての ***VLAN***



VLAN は通常、IP サブネットワークに関連付けられますたとえば、特定の IP サブネットに含まれるエンド ステーションはすべて同じ VLAN に属します。VLAN 間で通信するには、トラフィックをルーティングする必要があります。

デフォルトでは、新規に作成された VLAN は動作可能です。つまり、新規に作成された VLAN は、非シャットダウンの状態になります。また、トラフィックを通過させるアクティブ ステート、またはパケットを通過させない一時停止ステートに、VLAN を設定することもできます。デフォルトでは、VLAN はアクティブ ステートでトラフィックを通過させます。

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

VLAN の範囲

Note Cisco Nexus 9000 デバイスでは、拡張システム ID が常に自動的にイネーブルになります。

このデバイスは IEEE 802.1Q 標準に従って、最大 4095 の VLAN をサポートします。これらの VLAN は、ソフトウェアによっていくつかの範囲に分割され、範囲によって用途が少しずつ異なります。

設定の制限については、ご使用のスイッチの検証済みの拡張性の制限に関するマニュアルを参照してください。

この表では、VLAN 範囲について説明します。

***Table 3: VLAN* の範囲**

VLAN の番号	数の範囲	使用法
1	標準	シスコのデフォルトです。この VLAN は使用できますが、変更と削除はできません。
2 ～ 1005	標準	これらの VLAN は作成、使用、変更、および削除ができます。
1006 ～ 3967	拡張	これらの VLAN は作成、命名、使用ができます。以下のパラメータは変更できません。 • ステートは必ず、アクティブです。 • VLAN は常にイネーブルです。これらの VLAN はシャットダウンできません。
3968 ～ 4095	内部割り当て	これらの予約 VLAN は、内部デバイスによる使用のために割り当てられています。

Note システムは降順で入力された範囲を受け入れますが、シスコでは昇順で範囲を入力することを推奨します。

たとえば、VLAN の範囲を 1602 ～ 1607 から削除する場合、1602 ～ 1607 として値を入力することを推奨します。1607 ～ 1602 は可能ですが、推奨しません。誤って範囲を 1602 ～ 7 として入力すると、1602 ～ 1607 ではなく、7 ～ 1602 の VLAN が削除されます。

予約済み VLAN について

予約済みVLAN（3968ー4095）に関する注意事項を次に示します。

- このソフトウェアは、内部 VLAN の使用を必要とするマルチキャストや診断などの機能用に、VLAN 番号のグループを割り当てます。デフォルトでは、このような内部使用のために 128 の予約済み VLAN（3968 ～ 4095）からなるブロックが割り当てられます。
- 予約済みVLANの範囲は、system vlan-idで変更できます。 **vlan reserve** コマンドを使用します。これにより、異なる範囲のVLANを予約済みVLANとして使用するように設定できます。選択したVLANは、128のグループで予約する必要があります。
  - VLAN 3968 ～ 4092 は他の目的で構成できます。ただし、VLAN 3999 は除きます。これは、デフォルトの内部 VLAN の使用方法が変更された場合でも、内部で使用されるためです。
  - VLAN 4093ー4095は常に内部使用のために予約されており、他の目的には使用できません。

次の例を参考にしてください。

```
system vlan 400 reserve
```

VLAN 400-527を予約します。

新しい予約範囲は、実行コンフィギュレーションが保存され、デバイスがリロードされた後に有効になります。

- VLANs 4093 ～ 4095 は常に内部使用に予約されていて、その他の目的に使用できません。

  この例では、コマンドの結果、VLAN 400ー527が予約され、VLAN 4093ー4095も予約されます。

- **no system vlan** *vlan-id* **reserve**コマンドは、デバイスのリロード後に、予約済みVLANの範囲をデフォルトの3968ー4095の範囲に変更します。
- **show system vlan reserved** コマンドを使用し、 コマンドを使用して、現在および将来の予約済みVLAN範囲の範囲を確認します。

VLAN 予約の例

次は、VLAN 予約（イメージのリロードの前後）の設定の例を示します。

```
************************************************
CONFIGURE NON-DEFAULT RANGE, "COPY R S" AND RELOAD
************************************************
switch(config)# system vlan 400 reserve
"vlan configuration 400-527" will be deleted automatically.
Vlans, SVIs and sub-interface encaps for vlans 400-527 need to be removed by the user.
Continue anyway? (y/n) [no] y
Note: After switch reload, VLANs 400-527 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)# show system vlan reserved

system current running vlan reservation: 3968-4095

system future running vlan reservation: 400-527


switch(config)# copy running-config startup-config
[########################################] 100%

switch(config)# reload
This command will reboot the system. (y/n)?  [n] y

************
AFTER RELOAD
************

switch# show system vlan reserved

system current running vlan reservation: 400-527
```

VLAN の作成、削除、変更

Note デフォルトでは、すべての Cisco Nexus 9396 および Cisco Nexus 93128 ポートはレイヤ 2 ポートです。

デフォルトでは、すべての Cisco Nexus 9504 および Cisco Nexus 9508 ポートはレイヤ 3 ポートです。

VLAN には 1 ～ 3967 の番号が付けられます。スイッチ ポートとして設定したポートはすべて、レイヤ 2 デバイスとしてのスイッチの初回起動時に、デフォルト VLAN に割り当てられます。デフォルト VLAN（VLAN1）はデフォルト値だけを使用し、デフォルト VLAN でアクティビティの作成、削除、一時停止を行うことはできません。

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

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

VLAN の範囲により、次のパラメータを VLAN 用に設定できます（デフォルト VLAN を除く）。

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

最大 128 文字の VLAN ロング ネームを設定できます。VLAN ロング ネームを設定するには、VTP がトランスペアレント モードである必要があります。

Note VLAN アクセス ポートまたはトランク ポートとしてのポートの設定と、VLAN へのポートの割り当ての詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

特定の VLAN を削除すると、その VLAN に関連するポートは非アクティブになり、トラフィックは流れなくなります。トランク ポートから特定の VLAN を削除すると、その VLAN だけがシャットダウンし、トラフィックは引き続き、トランク ポート経由で他のすべての VLAN 上で転送されます。

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

Note 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せん。変更を反映するには、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。

VLAN のハイ アベイラビリティ

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

VLAN を使用しているときに、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。

Note ハイ アベイラビリティ機能の詳細については、『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

VLAN 設定の前提条件

VLAN 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。
- VLAN を変更するには、その VLAN が作成されている必要があります。

VLAN の設定に関するガイドラインおよび制約事項

VLAN 設定時のガイドラインと制限事項は次のとおりです。

- キーワードが付いている **show** コマンドはサポートされていません。 **internal**
- 1 つの VLAN または VLAN 範囲を設定できます。

  多数の VLAN を設定する場合は、最初に **vlan** コマンドを使用して VLAN を作成します（たとえば、 **vlan** *200-300, 303-500*）。。VLAN が正常に作成された後、これらの VLAN に順番に名前を付けるか設定します。

- 内部使用のために予約された VLAN グループ内の VLAN は、作成、変更、または削除することはできません。
- VLAN1 は、デフォルト VLAN です。この VLAN の作成、変更、または削除はできません。
- VLAN 1006 ～ 3967 は常にアクティブ ステートなので、常にイネーブルです。これらの VLAN のステートを一時停止またはシャットダウンすることはできません。
- スパニングツリー モードを変更すると、レイヤ 2 VLAN と同じ VLAN ID を共有するレイヤ 3 サブインターフェイス VLAN は、ハードウェアの再プログラミングの結果として発生するマイクロ秒のトラフィック ドロップの影響を受ける可能性があります。
- デフォルトで VLAN 3968 ～ 4095 は内部デバイス用に予約されています。
- Cisco NX-OS リリース 9.2(3) 以降では、VLAN を vn-segments を持つように設定できます。
- QOS/ACL/SPANはFEX HIFではサポートされません。

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。

***Table 4: VLAN* パラメータのデフォルト値**

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

VLAN の設定

Note VLAN へのレイヤ 2 インターフェイスの割り当て（アクセスまたはトランク ポート）の詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。デフォルトでは、すべてのインターフェイスが VLAN1 に割り当てられます。

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

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。

Note 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。

Note 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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**vlan** {*vlan-id* | *vlan-range*}
	Example:
	`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 ～ 3967 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。VLAN 範囲の詳細については、VLAN の範囲, on page 38を参照してください。

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

ステップ 4	(Optional) **show vlan** **Example:** `switch# show vlan`	VLAN の情報およびステータスを表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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)# exit
switch(config)#
```

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。

- 名前
- ステータス
- シャットダウン

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**vlan** {*vlan-id* | *vlan-range*}
	Example:
	`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。VLAN 範囲に関する詳細は、VLAN の範囲, on page 38 を参照してください。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show vlan** **Example:** `switch# show vlan`	VLAN の情報およびステータスを表示します。

	Command or Action	Purpose
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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。

- 名前
- ステータス
- シャットダウン

Note 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。

SUMMARY STEPS

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

VLAN の設定

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**vlan** {*vlan-id* | *vlan-range*}
	Example:
	`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。VLAN範囲の詳細については、VLANの範囲, on page 38を参照してください。

ステップ 3	**name** *vlan-name* **Example:** `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。 **Note** 128文字の名前がサポートされます（VLANロングネーム）。
ステップ 4	**state** {**active** | **suspend**} **Example:** `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 ～ 3967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** **Example:** `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 ～ 3967はシャットダウンできません。

ステップ 6	**exit**
	Example:
	`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	(Optional) **show vlan** **Example:**	VLANの情報およびステータスを表示します。

	Command or Action	Purpose
	`switch# show vlan`	
ステップ 8	(Optional) **show vtp status** **Example:** `switch# show vtp status`	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	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。 **Note** 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せん。変更を反映するには、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。

Example

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)#
```

VLAN 作成前の VLAN 設定

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

手順

	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 モードに入ります。

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。

例

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 の長い名前のイネーブル化

最大 128 文字の VLAN ロング ネームを設定できます。

（注） タイミング（When） **system vlan long-name** Cisco Nexus 9000シリーズスイッチはVTPオフモードで起動します。

VTP トランスペアレント モードの有効化:

1. VTP の無効化
2. 削除 **system vlan long-name** from the start-up configuration
3. VTPの再有効化

始める前に

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 の構成」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

手順

	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。

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	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

例

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
```

トランク ポートでの内部 VLAN および外部 VLAN マッピングの設定

内部 VLAN および外部 VLAN からポートのローカル（変換先）VLAN への VLAN 変換を設定できます。

内部 VLAN および外部 VLAN マッピングに関する注意点

- VLAN 変換（マッピング）は、ネットワーク フォワーディング エンジン（NFE）を搭載した Cisco Nexus 9000 シリーズ スイッチでサポートされます。、VLAN 変換は Cisco Nexus 9300-EX スイッチでサポートされます。
- 内部および外部 VLAN は、これらが設定されているポートのトランク許可リストに含めることはできません。

  次に例を示します。

```
switchport vlan mapping 11 inner 12 111
switchport trunk allowed vlan 11-12,111 /***Not valid because 11 is outer VLAN and
12 is inner VLAN.***/
```

- 同じポート上で、2 つのマッピング（変換）設定に、同じ内容の外部（あるいはオリジナル）VLAN もしくは変換先 VLAN を含めることはできません。複数の内部 VLAN および外部 VLAN のマッピング設定については、同じ内部 VLAN を含めることができます。

  次に例を示します。

```
switchport vlan mapping 101 inner 102 1001
switchport vlan mapping 101 inner 103 1002  /***Not valid because 101 is already
used as an original VLAN.***/
switchport vlan mapping 111 inner 104 1001  /***Not valid because 1001 is already
used as a translated VLAN.***/
switchport vlan mapping 106 inner 102 1003  /***Valid because inner vlan can be the
 same.***/
```

- トランク ポートでのポート VLAN マッピングは、Network Forwarding Engine (NFE) 搭載の Cisco Nexus 9000 シリーズ スイッチ、Cisco Nexus 9200、9300-EX、9300-FX、および EX/FX ライン カード搭載の Cisco Nexus 9500 プラットフォーム スイッチでサポートされます。
- VLAN 変換は VXLAN 対応 VLAN ではサポートされません。

手順の概要

1. **configure terminal**
2. **interface** *type port*
3. [**no**] **switchport mode trunk**
4. **switchport vlan mapping enable**
5. **switchport vlan mapping** *outer-vlan-id* **inner** *inner-vlan-id translated-vlan-id*
6. （任意） **copy running-config startup-config**
7. （任意） **show interface** [*if-identifier*] **vlan mapping**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type port*	インターフェイス設定モードを開始します。
ステップ 3	[**no**] **switchport mode trunk**	トランク 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	**switchport vlan mapping enable**	スイッチ ポートでの VLAN 変換をイネーブルにします。VLAN 変換はデフォルトでディセーブルです。 （注） VLAN 変換を無効にするには、このコマンドの **no** 形式を使用します。
ステップ 5	**switchport vlan mapping** *outer-vlan-id* **inner** *inner-vlan-id translated-vlan-id*	内部 VLAN および外部 VLAN を他の VLAN に変換します。
ステップ 6	（任意） **copy running-config startup-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） スイッチ ポートが動作するトランク ポートになるまで、VLAN 変換設定は有効になりません。
ステップ 7	（任意） **show interface** [*if-identifier*] **vlan mapping**	インターフェイスの範囲または特定のインターフェイスについて、VLAN マッピング情報を表示します。

例

この例では、ダブル タグ VLAN トラフィック（内部 VLAN 12、外部 VLAN 11）から VLAN 111 への変換を設定する方法を示します。

```
switch# config t
switch(config)# interface ethernet1/1
switch(config-if)# switchport mode trunk
switch(config-if)# switchport vlan mapping enable
switch(config-if)# switchport vlan mapping 11 inner 12 111
switch(config-if)# switchport trunk allowed vlan 101-170
switch(config-if)# no shutdown
```

```
switch(config-if)# show mac address-table dynamic vlan 111

Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False
   VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
*  111     0000.0092.0001   dynamic  0         F      F    nve1(100.100.100.254)
*  111     0000.0940.0001   dynamic  0         F      F    Eth1/1
```

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。

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 に関する追加情報

関連資料

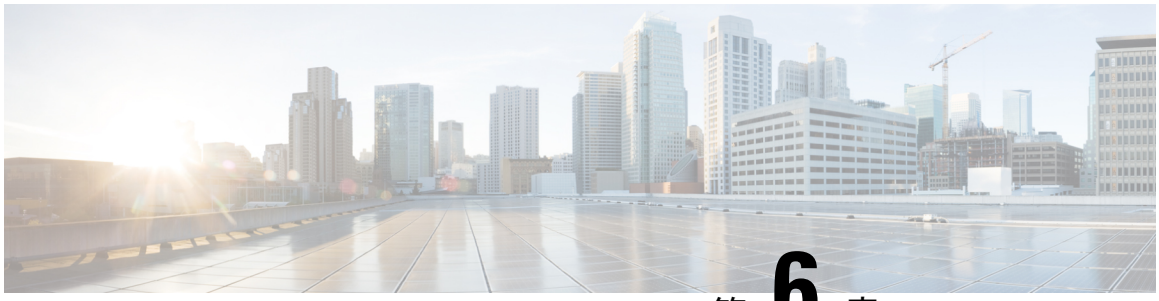
関連項目	マニュアル タイトル
NX-OS レイヤ 2 スイッチングの設定	『*Cisco Nexus 9000* シリーズ *NX-OS Layer 2* スイッチング設定ガイド』
インターフェイス、VLAN インターフェイス、IP アドレス指定、ポート チャネル	『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』
マルチキャスト ルーティング	『*Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide*』
NX-OS の基礎	『*Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide*』
高可用性	『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』
システム管理	『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

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 https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIB



第 6 章

VTP の設定

- VTP の概要 （57 ページ）
- VTP の設定に関する注意事項および制約事項 （59 ページ）
- デフォルト設定, on page 59
- VTP の設定, on page 60

VTP の概要

サポートされている VTP は、VTP バージョン 1 および 2 です。

（注） 実際に VLAN を作成せずに VLAN を設定できます。詳細については、VLAN 作成前の VLAN 設定 （49 ページ）を参照してください。

VTP

VTP は、VTP ドメイン内の VLAN の追加、削除、名前変更を管理することで VLAN の一貫性を維持する、レイヤ 2 メッセージング プロトコルです。VTP ドメインは、同じ VTP ドメイン名を共有し、トランク インターフェイスを使用して接続される、1 つ以上のネットワーク装置で構成されます。各ネットワーク装置は、1 つの VTP ドメインだけに属することができます。

レイヤ 2 トランク インターフェイス、レイヤ 2 ポート チャネル、および仮想ポート チャネル（vPC）は、VTP 機能をサポートしています。

VTP は、デフォルトではデバイスでディセーブルになっています。VTP をイネーブルにして設定するには、コマンドライン インターフェイス（CLI）を使用します。VTP をディセーブルにすると、デバイスで VTP プロトコル パケットが中継されません。

Note VTP は Cisco Nexus 9000 シリーズ デバイスでトランスペアレント モードだけで動作し、デバイス全体に VTP ドメインを拡張できます。

デバイスが VTP トランスペアレント モードの場合、デバイスはトランク ポート上で受信したすべての VTP プロトコル パケットを他のすべてのトランク ポートに中継します。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。

Note ネットワークで VTP がサポートされている場合、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 は正常に機能しなくなります。

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 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

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。

VTP がトランスペアレント モードの場合、最大 128 文字の VLAN ロング ネームを設定できます。

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 の設定に関する注意事項および制約事項

VTP 設定時の注意事項と制約事項は次のとおりです。

- **show** コマンド（**internal** キーワード付き）はサポートされていません。
- SNMP では、VTP 機能がイネーブルかどうかが vlanTrunkPortVtpEnabled オブジェクトによって示されます。vlanTrunkPortVtpEnabledオブジェクトのステータスは、 **show vtp trunk interface eth a/b** コマンドを使用します。
- VTP アドバタイズメントは、Cisco Nexus ファブリック エクステンダのポートからは送信されません。
- VTP プルーニングは、透過的なデバイスでは実行できません。VTP ドメインに透過的なデバイスがある場合は、VTP プルーニングを無効にする必要があります。ネイバー デバイスで VTP プルーニングが無効になっていない場合、Cisco Nexus デバイスは、Nexus を指すリンクで VLAN がプルーニング/無効になるため、ネイバー デバイスから MAC を学習しません。

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。

Table 5: **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	空白
VTP バージョン	1
インターフェイス単位の VTP	有効（Enabled）

VTP の設定

CiscoNexus 9000 デバイスで VTP を設定できます。

Note 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。

Note VTP が機能するのは、トランスペアレント モードだけです。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

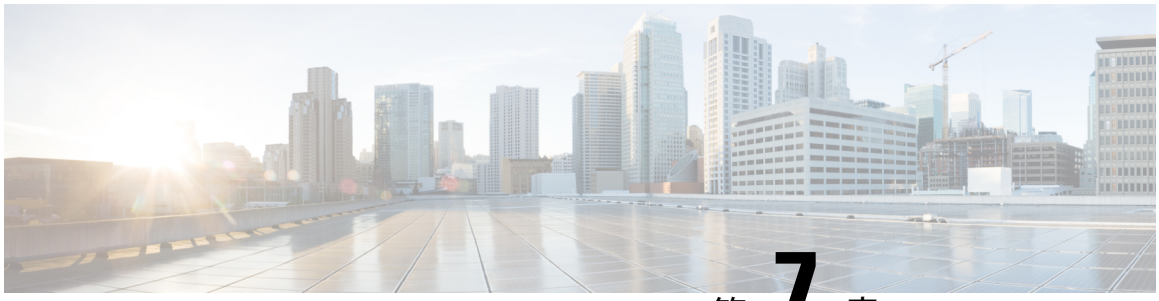
ステップ 2	**feature vtp**
	Example:
	`switch(config)# feature vtp`
	`switch(config)#`
		デバイスの VTP をイネーブルにします。デフォルトでは無効になっています。

	Command or Action	Purpose
ステップ 3	**vtp domain** *domain-name* **Example:** `switch(config)# vtp domain accounting`	このデバイスを追加する 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**} **Example:** `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 file** *file-name* **Example:** `switch(config)# vtp file vtp.dat`	VTP 設定を保存する IFS ファイル システム ファイルの ASCII ファイル名を指定します。
ステップ 6	**vtp password** *password-value* **Example:** `switch(config)# vtp password cisco`	VTP 管理ドメイン用のパスワードを指定します。

ステップ 7	**exit**
	Example:
	`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 8	(Optional) **show vtp status** **Example:** `switch# show vtp status`	バージョン、モード、リビジョン番号など、デバイス上の VTP 設定に関する情報を表示します。
ステップ 9	(Optional) **show vtp counters** **Example:** `switch# show vtp counters`	デバイス上の VTP アドバタイズメントに関する統計情報を表示します。
ステップ 10	(Optional) **show vtp interface** **Example:** `switch# show vtp interface`	VTP-enabled インターフェイスのリストを表示します。
ステップ 11	(Optional) **show vtp password** **Example:** `switch# show vtp password`	管理 VTP ドメイン用のパスワードを表示します。
ステップ 12	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

VTP の設定



第 7 章

NX-OS を使用したプライベート VLAN の設定

- プライベート VLAN について, on page 63
- プライベート VLAN の前提条件, on page 72
- プライベート VLAN の設定に関するガイドラインおよび制約事項 （73 ページ）
- プライベート VLAN のデフォルト設定, on page 76
- プライベート VLAN の設定, on page 77
- プライベート VLAN 設定の確認, on page 98
- プライベート VLAN の統計情報の表示とクリア, on page 98
- プライベート VLAN の設定例, on page 98
- プライベート VLAN の追加情報（CLI バージョン）, on page 99

プライベート VLAN について

Cisco Nexus NX-OS 7.0(3)I1(2) 以降、プライベート VLAN 機能がサポートされています。

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

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

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

プライマリ VLAN は、セカンダリ VLAN を関連付けるブロードキャスト ドメインを定義します。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかの場合があります。独立 VLAN 上のホストは、プライマリ VLAN 内で関連付けられた無差別ポートとだけ通

信します。コミュニティ VLAN 上のホストは、同じコミュニティ VLAN 上のホスト間および関連付けられた無差別ポートとだけ通信し、独立ポートまたは他のコミュニティ VLAN 内のポートとは通信しません。

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

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。

Note 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。

プライベート VLAN のプライマリ VLAN とセカンダリ VLAN

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

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

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

プライベート VLAN の機能は、VLAN のレイヤ 2 ブロードキャスト ドメインをサブドメインに分割できます。サブドメインは、プライマリ VLAN とセカンダリ VLAN で構成されるプライベート VLAN のペアで表されます。プライベート VLAN ドメインには複数のプライベート VLAN のペアを設定でき、それぞれのペアを各サブドメインに割り当てることができます。プライベート VLAN ドメイン内のすべての VLAN ペアは、同じプライマリ VLAN を共有します。セカンダリ VLAN ID は、各サブドメインの区別に使用されます。

Note プライベート VLAN ドメインには、プライマリ VLAN が 1 つのみ含まれています。

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

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

プライベート VLAN ポート

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

プライベート VLAN ポートのタイプは、次のとおりです。

- 無差別ポート：無差別ポートは、プライマリ VLAN に属します。無差別ポートは、無差別ポートとアソシエートされているセカンダリ VLAN に属し、プライマリ VLAN とアソシエートされている、すべてのインターフェイスと通信でき、この通信可能なインターフェイスには、コミュニティ ポートと独立ホスト ポートも含まれます。プライマリ VLAN には、複数の無差別ポートを含めることができます。各無差別ポートには、ポートにアソシエートされている、複数のセカンダリ VLAN を含めることができ、また、セカンダリ VLAN を含めないこともできます。無差別ポートとセカンダリ VLAN が同じプライマリ VLAN にある限り、セカンダリ VLAN は、複数の無差別ポートとアソシエートすることができます。このアソシエーションは、ロードバランシングまたは冗長性のために使用することもできます。セカンダリ VLAN を無差別ポートに関連付けないこともできますが、その場合、セカンダリ VLAN はレイヤ 3 インターフェイスと通信できません。

Note ベストプラクティスとして、プライマリのすべてのセカンダリ ポートをマッピングして、トラフィックの損失を最小限に抑える必要があります。

- 無差別トランク：複数のプライマリ VLAN のトラフィックを伝送するように無差別トランク ポートを設定できます。プライベート VLAN のプライマリ VLAN およびすべてまたは選択した関連付けられた VLAN を無差別トランク ポートにマップします。各プライマリ VLAN と関連付けられた 1 つのセカンダリ VLAN はプライベート VLAN のペアとなります。また、各無差別トランク ポートに最大 16 のプライベート VLAN のペアを設定できます。

Note プライマリ プライベート VLAN に加え、標準の VLAN でもプライベート VLAN 無差別トランク ポートでトラフィックが伝送されます。

- 独立ポート：独立ポートは、セカンダリ独立VLANに属するホストポートです。このポートは同一プライベート VLAN ドメイン内のその他のポートからレイヤ 2 で完全に分離されていますが、関連付けられた無差別ポートとは通信できます。プライベートVLANは、無差別ポートからのトラフィックを除き、独立ポート宛のトラフィックをすべてブロックします。独立ポートから受信されたトラフィックは、無差別ポートにだけ転送されます。特定の独立 VLAN に複数の独立ポートを設定し、その独立 VLAN 内で各ポートを他のすべてのポートから完全に分離できます。
- 独立トランクまたはセカンダリ トランク：複数の独立 VLAN のトラフィックを伝送するように独立トランク ポートを設定できます。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 つのセカンダリ VLAN は、1 つの独立トランク ポートにはできません。各プライマリ VLAN と関連付けられた 1 つのセカンダリ VLAN はプライベート VLAN のペアとなります。また、各独立トランク ポートに最大 16 のプライベート VLAN のペアを設定できます。

Note セカンダリ プライベート VLAN に加え、標準の VLAN でもプライベート VLAN 独立トランク ポートでトラフィックが伝送されます。

- コミュニティ ポート：コミュニティ ポートは、1 つのコミュニティ セカンダリ VLAN に属するホスト ポートです。コミュニティ ポートは、同じコミュニティ VLAN にある他のポートおよびアソシエートされている無差別ポートと通信します。これらのインターフェイスは、他のコミュニティにある他のすべてのインターフェイスおよびプライベートVLANドメイン内のすべての独立ポートから、レイヤ 2 で分離されています。

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

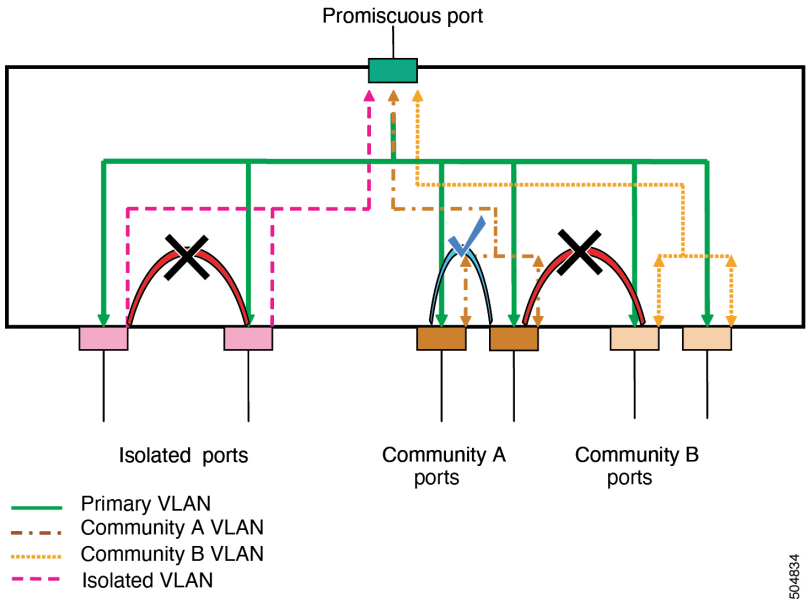
プライマリ、独立、およびコミュニティ プライベート VLAN

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

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

Figure 3: プライベート *VLAN* のレイヤ *2* トラフィック フロー

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



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

無差別ポートは 1 つのプライマリ VLAN の専用ポートになりますが、複数の独立 VLAN および複数のコミュニティ VLAN で使用できます(レイヤ 3 ゲートウェイは、無差別ポートを介してデバイスに接続されます。) 無差別ポートでは、広範囲なデバイスをプライベート VLAN のアクセス ポイントとして接続できます。たとえば、すべてのプライベート VLAN サーバーを

管理ワークステーションから監視したりバックアップしたりするのに、無差別ポートを使用できます。

Note プライベート VLAN の無差別および独立トランク ポートを設定できます。これらの無差別トランク ポートと独立トランク ポートは、標準の VLAN に加え、複数のプライマリおよびセカンダリ VLAN のトラフィックを伝送できます。

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

スイッチング環境では、個々のエンド ステーションに、または共通グループのエンド ステーションに、個別のプライベート VLAN や、関連する IP サブネットを割り当てることができます。エンド ステーションはデフォルト ゲートウェイとの通信を行うだけで、プライベート VLAN の外部と通信することができます。

Note レイヤ 3 ゲートウェイを設定するには、VLAN インターフェイス機能をイネーブルにしておく必要があります。VLAN ネットワーク インターフェイスと IP アドレス設定の詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

プライマリ VLAN とセカンダリ VLAN の関連付け

セカンダリ VLAN 内のホスト ポートでプライベート VLAN 外と通信するには、セカンダリ VLAN をプライマリ VLAN に関連付ける必要があります。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。

Note 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。

Note 関連付け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、元のアソシエーションが復元されます。

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 を再作成してセカンダリ VLAN として設定すると元に戻ります。

Note この動作は、Catalyst デバイスの動作と異なります。

Note （**no private-vlan primary** コマンドを発行して）プライマリ VLAN のタイプを通常/ユーザ VLAN に変更すると、そのプライマリ VLAN の下のすべてのアソシエーションが動作不能になります。ただし、同じ VLAN のタイプを通常/ユーザ VLAN からプライマリ VLAN に変更した場合、タイプ変更後にプライマリ VLAN で再設定されない限り、プライマリ VLAN でのアソシエーションは引き続き動作しません。

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。

プライベート VLAN 内のブロードキャスト トラフィック

プライベート VLAN にあるポートからのブロードキャスト トラフィックは、次のように流れます。

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

プライベート VLAN ポートの分離

プライベート VLAN を使用すると、次のように、エンド ステーションへのアクセスを制御できます。

- エンドステーションに接続されているインターフェイスを選択して独立ポートとして設定し、レイヤ2の通信をしないようにします。たとえば、エンドステーションがサーバの場合、この設定によりサーバ間のレイヤ 2 通信ができなくなります。
- デフォルト ゲートウェイおよび選択したエンド ステーション（バックアップ サーバーなど）に接続されているインターフェイスを無差別ポートとして設定し、すべてのエンドステーションがデフォルト ゲートウェイにアクセスできるようにします。

プライベート VLAN および VLAN インターフェイス

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

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

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

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

Note VLANインターフェイスを設定するには、VLANインターフェイス機能をイネーブルにしておく必要があります。VLAN インターフェイスおよび IP アドレスの設定の詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

複数のデバイスにまたがるプライベート VLAN

複数のデバイスにわたるようにプライベート VLAN を拡張するには、プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN を、プライベート VLAN をサポートする他のデバイス

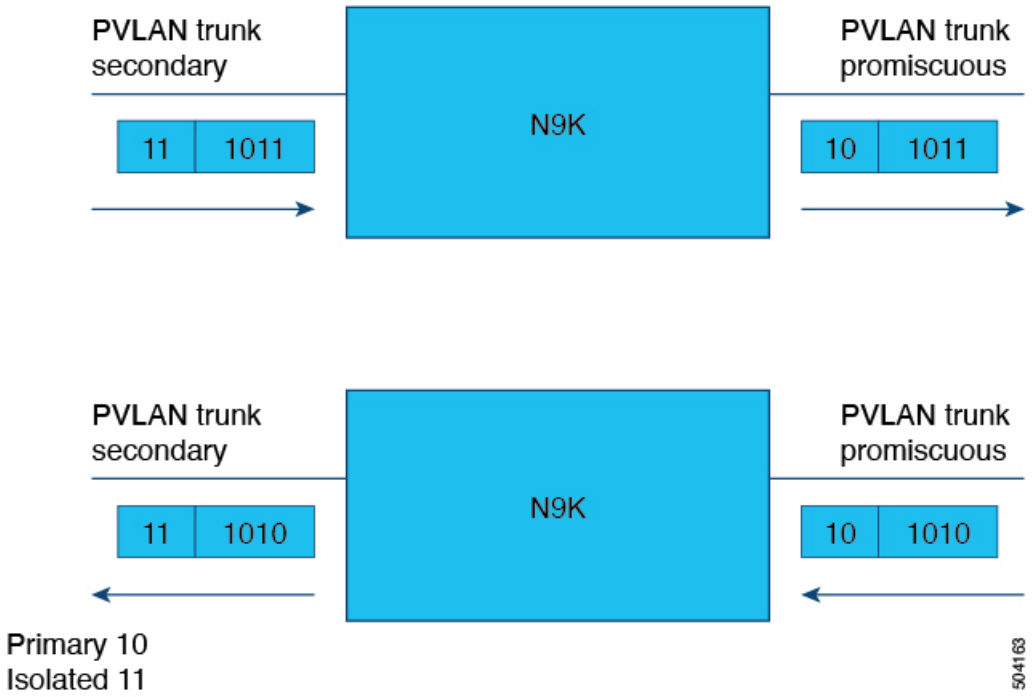
にトランキングします。プライベート VLAN 設定のセキュリティを保持して、プライベート VLAN として設定された VLAN が他の目的に使用されないようにするには、プライベート VLAN ポートが設定されていないデバイスを含め、すべての中間デバイスにプライベート VLAN を設定します。

内部 VLAN タグを保持するプライベート VLAN

Cisco NX-OS リリース 10.2(3)F 以降、グローバル **system dot1q-tunnel transit** <*vlan*> を構成している場合トランジット ボックスとして機能するサポートされている Cisco Nexus スイッチでコマンドを実行すると、2 つ以上のタグを持つプライベート VLAN トランク ポートに着信するパケットは保持され、内部タグを削除せずに送信されます。このコマンドの詳細については、cisco.com の関連リリースの『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

（注） PVLAN と QinQ が同じポートで設定されている場合、内部タグの保存は機能しません。

次の図は、パケットが PVLAN セカンダリ トランクから PVLAN 無差別トランクに移動したり、その逆に移動したりするときの、サポートされている Cisco Nexus スイッチでの内部タグの保持を示しています。



サンプル設定を次に示します。

```
vlan 10
private-vlan primary
private-vlan association 11-12
vlan 11
private-vlan isolated
```

```
vlan 12
private-vlan community

interface Ethernet1/1
switchport
switchport mode private-vlan trunk secondary
switchport private-vlan association trunk 10 11
no shutdown

interface Ethernet1/2
switchport
switchport mode private-vlan trunk promiscuous
switchport private-vlan mapping trunk 10 11-12
no shutdown

(config)# system dot1q-tunnel transit vlan 10,11
```

FEXホストインターフェイスポート上のプライベートVLAN

7.0（3）I2（1）以降、Cisco Nexus NX-OSは、Cisco Nexus 2000ファブリックエクステンダのホスト側ポート（FEX HIFポート）でプライベートVLAN（PVLAN）をサポートします。

PVLANは、単一接続ホストおよび単一接続FEX HIF設定でサポートされます。

（注） FEX HIF PC / VPC（ポートチャネル/仮想ポートチャネル）およびFEX AA（アクティブ/アクティブ）設定はサポートされていません。

プライベート VLAN のハイ アベイラビリティ

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

Note プライベート VLAN が設定されている場合（7.0（3）I1（2） 以前の場合）、Cisco NX-OS の以前のバージョンへのダウングレードはサポートされていません。

Note ハイ アベイラビリティ機能、の詳細については、『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide* 』を参照してください。

プライベート VLAN の前提条件

プライベート VLAN 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。
- プライベート VLAN 機能をイネーブルにする必要があります。

プライベート VLAN の設定に関するガイドラインおよび制約事項

プライベート VLAN 設定時のガイドラインと制約事項 PVLAN は次のとおりです。

- 無差別モードで vPC ポートチャネルの PVLAN マッピングを変更すると、vPC セカンダリの vPC PO メンバーがフラップします。
- **show** コマンド（**internal** キーワード付き ）はサポートされていません。
- デバイスで PVLAN 機能を適用できるようにするには、あらかじめ PVLAN をイネーブルにしておく必要があります。
- PVLAN は、これらのスイッチの vPC およびポート チャネルでサポートされています。
  - Cisco Nexus 9200 シリーズ
  - Cisco Nexus 9300、9300-EX、9300-FX、9300-FX2 および 9300-FX3 シリーズ スイッチ
  - Cisco Nexus 9500 シリーズ スイッチ（N9K-X9432C-S 以外のライン カードを搭載したもの）

  PVLAN は、これらのスイッチの vPC およびポート チャネルではサポートされません。
  - Cisco Nexus 3232C および 3264Q スイッチ
- デバイスでこの機能を適用するには、VLANインターフェイス機能をイネーブルにする必要があります。
- セカンダリ VLAN を設定する前に、セカンダリ VLAN として設定するすべての VLAN の VLAN ネットワーク インターフェイスをシャットダウンします。
- スタティック MAC が通常の VLAN で作成され、その VLAN がセカンダリ VLAN に変換されると、Cisco NX-OS はセカンダリ VLANで設定された MAC をスタティック MAC として維持します。
- PVLAN は、次のように PVLAN ポート モードをサポートします。
  - プロミスキャス
  - 無差別トランク
  - ホストを分離する
  - 独立ホストトランク。
  - コミュニティホスト。

- Cisco NX-OS リリース 9.2(1) 以降、PVLAN は VXLAN をサポートします。
- プライベート VLAN は、ポート チャネルのポート モードをサポートします。
- プライベート VLAN は、仮想ポートチャネル（vPC）インターフェイスのポート モード サポートを提供します。
- PVLAN無差別トランクまたはPVLAN独立トランクを設定する場合は、IDで指定されたリストで非PVLANを許可することを推奨します。 **switchport private-vlan trunk allowed** コマンドを使用します。PVLANは、PVLANトランクモードに応じてマッピングまたは関連付けられます。

（注） 2 番目のスイッチを無差別または隔離された PVLAN トランクに接続することはできません。PVLAN無差別トランクまたはPVLAN隔離トランクは、ホストスイッチでのみサポートされます。

- **system private-vlan fex trunk** コマンドは、Cisco Nexus 9300 -FX、-FX2、-FX3 プラットフォーム スイッチでサポートされていません。次の PVLAN モードは、シングルホーム FEX 構成の FEX ポートおよびポート チャネルでのみサポートされます（AA または ST vPC モードではサポートされません）。
  - Isolated host
  - Community host
  - Isolated trunk

  これらのモードは、シングルホーム FEX 構成の FEX ポートおよびポート チャネルでのみサポートされます（AA または ST vPC モードではサポートされません）。
- PVLANはPACLおよびRACLをサポートします。
- PVLANは次のようにSVIをサポートします。
  - プライマリVLAN上のSVI。
  - SVI の プライマリおよびセカンダリ IP アドレス。
  - プライマリSVIのHSRP。
- PVLANはレイヤ2転送をサポートします。
- PVLANは次のようにSTPをサポートします。
  - RSTP
  - MST
- PVLANは、通常のトランクポートを介してスイッチ間でサポートされます。
- PVLANは、Cisco Nexus 9396PQおよび93128TXスイッチの10Gポートでサポートされます。

- PVLAN設定は、Cisco Nexus 9300シリーズスイッチのALEポートではサポートされません。
- PVLANポートモードは、Cisco Nexus 3164Qスイッチではサポートされていません。
- Network Forwarding Engine（NFE）では、PVLANはブレークアウトをサポートしません。
- PVLANは、vPCまたはポートチャネルFEXポートではサポートされません。
- PVLANは、IPマルチキャストまたはIGMPスヌーピングをサポートしません。
- Cisco NX-OS リリース9.3(3) 以降では、次の機能が C9316D-GX、C93600CD-GX、および C9364C-GX スイッチでサポートされています。
  - vPC
  - 200k MAC スケール
  - Dot1x
  - ポート セキュリティ
  - 選択的 QinQ
  - マルチプル プロバイダ VLAN を装備した選択的 QinQ
- Cisco NX-OSリリース9.3（5）以降、PVLANはDHCPスヌーピングをサポートします。
- Cisco NX-OS リリース 9.3(5) 以降、PVLAN は N9K-C93180YC-FX3S プラットフォーム スイッチでサポートされています。
- PVLANはPVLAN QoSをサポートしません。
- PVLANはVACLをサポートしません。
- PVLANはVTPをサポートしません。
- PVLANはトンネルをサポートしません。
- 送信元がPVLAN VLANの場合、PVLANはSPANをサポートしません。
- PVLAN の一部になるように共有インターフェイスを設定できません。詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。
- Cisco NX-OS CLIでは、PVLANグループごとに複数の独立VLAN設定を設定できますが、このような設定はサポートされていません。PVLANグループには、最大で1つの独立VLANを設定できます。
- Cisco NX-OS Release 7.0（3）I5（1）以降では、VLANでのPVLANアソシエーションはサポートされていません。
- このコマンドにより、PVLANでのアソシエーションが非アクティブになります。**no private-vlan primary** 後続のコマンドを発行しても、PVLANでのアソシエーションは動作可能になりません。**private-vlan primary** PVLANで再度アソシエーションを適用する必要があります。

- プライベートポートモードを非PVLANポートモードに変更するには、default interfaceコマンドを入力し、インターフェイスで非PVLANポートモードを設定します。
- PVLAN ホスト ポートおよび通常のトランクの MAC アドレス学習は、プライマリ VLAN で行われます。通常のトランクの場合、パケットはセカンダリ VLAN を使用して交換されますが、MAC 学習は引き続きプライマリ VLAN で実施されます。
- PVLAN は、N9K-X9636C-R、N9K-X9636Q-R、 N9K-X9636C-RX ライン カードを搭載した Cisco Nexus 9500 Series スイッチではサポートされていません。
- Cisco NX-OSリリース10.1（2）以降では、vPC孤立ポートでのPVLANとportSec機能の組み合わせには、ピアとトリガー間での動的なMac同期に制限があります。
- Cisco NX-OS Release 10.2(2)F 以降、次の機能が Cisco N9K-9332D-GX2B プラットフォーム スイッチでサポートされます。
  - PVLAN および Flex Link
  - VPC
  - 選択的 QinQ
  - マルチプル プロバイダ VLAN を装備した選択的 QinQ
- Cisco NX-OS リリース 10.2(3)F 以降では、グローバル **system dot1q-tunnel transit** コマンドがトランジット ボックスとして機能する Nexus スイッチで設定されている場合、パケットが 2 つ以上のタグで着信すると、内部 VLAN を持つプライベート VLANタグ保存機能により、PVLANの内部タグを保存できます。この機能は、EX、FX、FX2、FX3、GX、および GX2B ベースの Cisco Nexus 9000 シリーズ TOR スイッチでのみサポートされています。
- PVLAN と Q-in-Q が同じポートで設定されている場合、内部タグの保存は機能しません。
- Cisco NX-OS リリース 以降では、2 番目のスイッチを無差別トランク ポートまたは隔離 PVLAN トランク ポートに接続できます。

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。

Table 6: **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	無効化

プライベート VLAN の設定

指定した VLAN をプライベート VLAN として割り当てる前に、VLAN を作成しておく必要があります。

VLAN インターフェイスへの IP アドレスの割り当ての詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

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

プライベート VLAN のイネーブル化（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。

Note 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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**feature private-vlan**
	Example:
	`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。
		Note

	Command or Action	Purpose
		no feature private-vlanコマンドを使用してプライベートVLAN機能をディセーブルにする前に、PVLAN設定を完全に削除する必要があります。以前のソフトウェアリリースでは、**no feature private-vlan** コマンドを適用する前に、すべてのPVLANポートを動作上ダウン状態にする必要があります。

ステップ 3	**exit**
	Example:
	`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	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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）

Note 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。

SUMMARY STEPS

1. **config t**
2. **vlan** {*vlan-id* | *vlan-range*}
3. [**no**] **private-vlan** {**community** | **isolated** | **primary**}
4. **exit**
5. (Optional) **show vlan private-vlan** [*type*]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

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

ステップ 3	[**no**] **private-vlan** {**community** | **isolated** | **primary**} **Example:** `switch(config-vlan)# private-vlan primary`	VLAN を、コミュニティ VLAN、独立 VLAN、またはプライマリ プライベート VLAN 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。 または 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。

ステップ 4	**exit**
	Example:
	`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。

	Command or Action	Purpose
ステップ 5	(Optional) **show vlan private-vlan** [*type*] **Example:** `switch# show vlan private-vlan`	プライベート VLAN の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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。
- *secondary-vlan-list* を入力するか、**add** キーワード *secondary-vlan-list* を追加して、プライマリ VLAN とセカンダリ VLAN の関連付けを行います。
- **remove** を入力します キーワード *secondary-vlan-list* を削除して、セカンダリ VLAN とプライマリ VLAN との関連付けをクリアします。
- 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、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、元のアソシエーションが復元されます。

no vlan コマンドは、プライマリ VLAN に対して、その VLAN に関連付けされているすべてのプライベート VLAN が失われます。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。

Before you begin

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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**vlan** *primary-vlan-id*
	Example:
	`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	[**no**] **private-vlan association** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*} **Example:** `switch(config-vlan)# private-vlan association 100-105,109`	コマンドの 1 つの形式を使用して、 セカンダリ VLAN をプライマリ VLAN に関連付けます。 または プライマリ VLAN からすべての関連付けを削除し、通常の VLAN モードに戻します。

	Command or Action	Purpose

ステップ 4	**exit**
	Example:
	`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	(Optional) **show vlan private-vlan** [**type**] **Example:** `switch# show vlan private-vlan`	プライベート VLAN の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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）

Note プライベート VLN 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の詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

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

Note 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。

Before you begin

- 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。
- 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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface vlan** *primary-vlan-ID*
	Example:
	`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	[**no**] **private-vlan mapping** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*} **Example:** `switch(config-if)# private-vlan mapping 100-105, 109`	セカンダリ VLAN を、プライマリ VLAN の SVI またはレイヤ 3 インターフェイスにマッピングします。これにより、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングが可能になります。 または セカンダリ VLAN とプライマリ VLAN 間のレイヤ 3 インターフェイスへのマッピングを消去します。

ステップ 4	**exit**
	Example:
	`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。

	Command or Action	Purpose
ステップ 5	(Optional) **show interface vlan** *primary-vlan-id* **private-vlan mapping** **Example:** `switch(config)# show interface vlan 101 private-vlan mapping`	インターフェイスのプライベート VLAN 情報を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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。

Note 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。

Before you begin

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。

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. **switchport mode private-vlan host**

4. [**no**] **switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*}
5. **exit**
6. (Optional) **show interface switchport**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *type slot/port*
	Example:
	`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**
	Example:
	`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	[**no**] **switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*} **Example:** `switch(config-if)# switchport private-vlan host-association 10 50`	レイヤ 2 ホスト ポートを、プライベート VLAN のプライマリ VLAN およびセカンダリ VLAN に関連付けます。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかとして設定できます。 または 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。

ステップ 5	**exit**
	Example:
	`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	(Optional) **show interface switchport** **Example:** `switch# 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。
ステップ 7	(Optional) **copy running-config startup-config** **Example:**	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。

	Command or Action	Purpose
	switch(config)# copy running-config startup-config	

Example

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

レイヤ 2 インターフェイスをプライベート VLAN 独立トランス ポートとして設定できます。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。

始める前に

プライベート VLAN 機能がイネーブルであることを確認してください。

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. [**no**] **switchport private-vlan association trunk** {*primary-vlan-id* [*secondary-vlan-id*]}
8. **exit**
9. （任意） **show interface switchport**
10. （任意） **copy running-config startup-config**

手順の詳細

手順

	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 モードに入ります。

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。

ステップ 5	（任意） **switchport private-vlan trunk native vlan** *vlan-id* 例： `switch(config-if)# switchport private-vlan trunk native vlan 5`	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。

	コマンドまたはアクション	目的
		（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	[**no**] **switchport private-vlan association trunk** {*primary-vlan-id* [*secondary-vlan-id*]}
	例：
	`switch(config-if)# switchport private-vlan association trunk 10 101`
	`switch(config-if)#`
		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。
		または
		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。

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	（任意） **show interface switchport** 例： `switch# 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。
ステップ 10	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-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。

例

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。

Before you begin

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。

SUMMARY STEPS

1. **config t**
2. **interface** {*type slot/port*}
3. **switchport mode private-vlan promiscuous**
4. [**no**] **switchport private-vlan mapping** {*primary-vlan-id*} {*secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list*}
5. **exit**
6. (Optional) **show interface switchport**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	Command or Action	Purpose

ステップ 2	**interface** {*type slot/port*}
	Example:
	`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** **Example:** `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	[**no**] **switchport private-vlan mapping** {*primary-vlan-id*} {*secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list*} **Example:** `switch(config-if)# switchport private-vlan mapping 10 50`	レイヤ 2 ポートを無差別ポートとして設定し、このポートをプライマリ VLAN および選択したセカンダリ VLAN のリストに関連付けます。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかとして設定できます。 または プライベート VLAN から、マッピングをクリアします。

ステップ 5	**exit**
	Example:
	`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	(Optional) **show interface switchport** **Example:** `switch# 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。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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

レイヤ 2 インターフェイスをプライベート VLAN の無差別トランク 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ます。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。

始める前に

プライベート VLAN 機能がイネーブルであることを確認してください。

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. [**no**]**switchport private-vlan mapping trunk** *primary-vlan-id* [*secondary-vlan-id*] {**add** *secondary-vlan-list* | **remove** *secondary-vlan-id*}
8. **exit**
9. （任意） **show interface switchport**
10. （任意） **copy running-config startup-config**

手順の詳細

手順

	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 モードに入ります。

ステップ 2	**interface** {*type slot/port*} 例：	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。

	コマンドまたはアクション	目的
	`switch(config)# interface ethernet 2/1` `switch(config-if)#`	

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。

ステップ 5	（任意） **switchport private-vlan trunk native vlan** *vlan-id* 例： `switch(config-if)# switchport private-vlan trunk native vlan 5`	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	[**no**]**switchport private-vlan mapping trunk** *primary-vlan-id* [*secondary-vlan-id*] {**add** *secondary-vlan-list* | **remove** *secondary-vlan-id*} 例：	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

	コマンドまたはアクション	目的
	`switch(config-if)# switchport private-vlan mapping trunk 4 5` `switch(config-if)#`	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。 または 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。

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	（任意） **show interface switchport** 例： `switch# 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。
ステップ 10	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-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。

例

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 10 20
switch(config-if)# switchport private-vlan mapping trunk 11 21
switch(config-if)# exit
switch(config)#
```

FEX トランクでの PVLAN の有効化

デフォルトでは、PVLAN は非 PVLAN FEX トランクでダウンしています。次のグローバル設定では、非 PVLAN FEX トランクで PVLAN を起動できます。

（注） FEX トランク上の PVLAN は、リーフ スパイン エンジン（LSE）を使用する FEX ではサポートされません。

手順の概要

1. [**no**] **system private-vlan fex trunk**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	[**no**] **system private-vlan fex trunk** 例： `switch(config)# system private-vlan fex trunk`	FEX トランクの PVLAN 設定を有効にします。

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

次に、PVLANホストモードとホストアソシエーションPVLANペアを設定します。

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. **switchport mode private-vlan host**
4. [**no**] **switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*}
5. **exit**
6. (Optional) **show interface switchport**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *type slot/port*
	Example:
	`switch(config)# interface ethernet 110/1/1`
	`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**
	Example:
	`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	[**no**] **switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*} **Example:** `switch(config-if)# switchport private-vlan host-association 10 50`	プライマリ VLANおよび関連付けられたセカンダリ VLANのポートでホストアソシエーションPVLANペアを設定します。

ステップ 5	**exit**
	Example:
	`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	(Optional) **show interface switchport** **Example:** `switch# 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。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

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

次に、分離トランクポートとホスト関連付け PVLAN ペアを設定します。

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. [**no**] **switchport private-vlan association trunk** {*primary-vlan-id* [*secondary-vlan-id*]}
8. **exit**
9. （任意） **show interface switchport**
10. （任意） **copy running-config startup-config**

手順の詳細

手順

	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 モードに入ります。

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。

ステップ 5	（任意） **switchport private-vlan trunk native vlan** *vlan-id* 例：	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）

	コマンドまたはアクション	目的
	`switch(config-if)# switchport private-vlan trunk native vlan 5`	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	[**no**] **switchport private-vlan association trunk** {*primary-vlan-id* [*secondary-vlan-id*]}
	例：
	`switch(config-if)# switchport private-vlan association trunk 10 101`
	`switch(config-if)#`
		プライマリ VLAN 用にポート上に独立トランク PVLAN ペア、および関連付けされたセカンダリ VLAN を設定します。セカンダリ VLAN は独立 VLAN である必要があります。

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	（任意） **show interface switchport** 例： `switch# 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。
ステップ 10	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-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。

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。

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	マニュアル タイトル
VLANインターフェイス、IPアドレス指定	『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』
スタティック MAC アドレス、セキュリティ	『*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*』
Cisco NX-OS の基礎	『*Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide*』
高可用性	『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』
システム管理	『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』

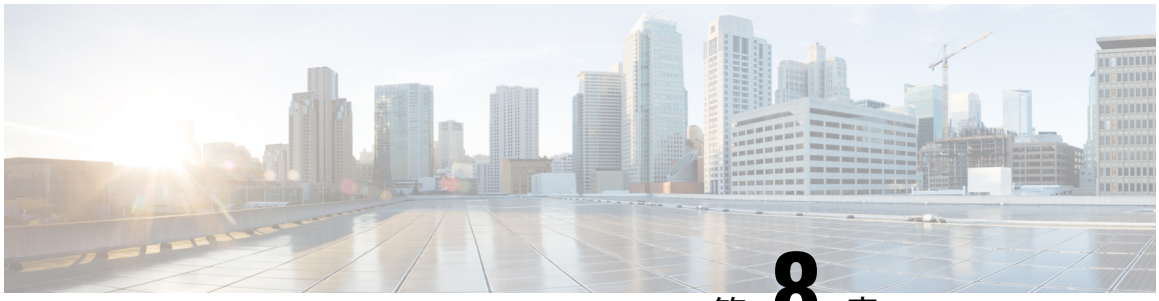
関連項目	マニュアル タイトル
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリースノート	『*Cisco Nexus 9000 Series NX-OS Release Notes*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
• CISCO-PRIVATE-VLAN-MIB	詳細については、ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.htmlを参照してください。



第 8 章

スイッチング モードの設定

- スイッチング モードに関する情報 （101 ページ）
- スイッチング モードに関するガイドラインと制限事項 （102 ページ）
- スイッチング モードのデフォルト設定 （102 ページ）
- スイッチング モードの設定 （103 ページ）

スイッチング モードに関する情報

スイッチング モードは、スイッチがパケット ヘッダーの宛先の詳細を読み取ったらすぐにフレーム転送を開始するか、またはフレーム全体を受信して、巡回冗長検査（CRC）でエラーをチェックしてからネットワークへのフレーム転送を開始するかを決定します。

スイッチングモードは、ハードウェアを介してスイッチまたはルーティングされるすべてのパケットに適用され、リブートや再起動後も永続的に保存できます。

スイッチは、次のスイッチング モードのいずれかで動作します。

カットスルー スイッチング モード

カットスルー スイッチング モードはデフォルトでイネーブルになっています。カットスルー スイッチング モードで動作するスイッチは、パケット ヘッダーの宛先の詳細を読み取ったらすぐにフレームの転送を開始します。カットスルーモードのスイッチは、フレーム全体の受信を完了する前にデータを転送します。

カットスルー モードのスイッチング速度は、Store-and-Forward スイッチング モードのスイッチング速度より速くなります。

Store-and-Forward スイッチング モード

Store-and-Forward スイッチングがイネーブルの場合、スイッチは各フレームの巡回冗長検査（CRC）エラーをチェックしてから、ネットワークにフレームを転送します。各フレームは、フレーム全体を受信してチェックされるまで保存されます。

フレーム全体を受信してチェックされるまでフレームの転送は待ち状態になるため、Store-and-Forward スイッチング モードのスイッチング速度は、カットスルー スイッチング モードのスイッチング速度より遅くなります。

スイッチング モードに関するガイドラインと制限事項

各スイッチング モードについて、次のガイドラインおよび制約事項を考慮してください。

カットスルー スイッチング モードに関するガイドラインおよび制約事項

- **show** コマンド（**internal** キーワード付き）はサポートされていません。
- カットスルースイッチでFCSエラーが検出された場合でも、FCSエラーパケットがドロップされないことがあります。出力ポートからのパケット送信がすでに進行中である場合です。すでに出力ポートから送信された CRC パケットをカットスルースイッチが検出すると、パケットの CRC フィールドがストンプされ、通常は出力インターフェイスで出力エラーとしてマークされます。パケットは、次のストアアンドフォワードネットワークノードでドロップされますが、経路上のすべてのノードもカットスルースイッチングを行っている場合には、接続先に配信されます。
- FCS エラーがあるパケットは、SPAN が設定されている場合はミラーリングされません。

Store-and-Forward スイッチング モードに関するガイドラインおよび制約事項

- **show** コマンド（**internal** キーワード付き）はサポートされていません。
- FCS エラーがあるパケットはドロップされます。
- FCS エラーがあるパケットは、SPAN が設定されている場合はミラーリングされません。
- CPU ポートは、常に Store-and-Forward モードで動作します。CPU に転送された FCS エラーがあるパケットはすべてドロップされます。
- Store-and-Forward モードでは、ポートがオーバーサブスクライブされていて、入力レートが出力ポートのスイッチング容量を超えていることをスイッチが確認するとそのポートが自動的にアクティブになります。たとえば、ポートの入力レートが 10 ギガビットで、出力ポートのスイッチング容量が 1 ギガビットの場合です。

（注） グローバル コンフィギュレーションは、Store-and-Forward モードがオーバーサブスクライブ ポートに対してアクティブになっていても、変更されません。

スイッチング モードのデフォルト設定

カットスルー スイッチングは、デフォルトでイネーブルになっています。

スイッチング モードの設定

スイッチング モードの設定

Store-and-Forward スイッチングのイネーブル化

（注） Store-and-Forward スイッチング モードをイネーブルにすると、ポート間のスイッチングの遅延に影響を及ぼすことがあります。

手順の概要

1. switch# **configure terminal**
2. switch(config) # **switching-mode store-forward**
3. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **switching-mode store-forward**	Store-and-Forward スイッチング モードをイネーブルにします。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	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。

例

次に、Store-and-Forward スイッチングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config) # switching-mode store-forward
switch(config) #
```

カットスルー スイッチングの再イネーブル化

カットスルー スイッチングは、デフォルトでイネーブルになっています。カットスルー スイッチングを再イネーブル化するには、**no switching-mode store-forward** 形式で使用します。 コマンドを使用します。

手順の概要

1. switch# **configure terminal**
2. switch(config) # **no switching-mode store-forward**
3. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

手順

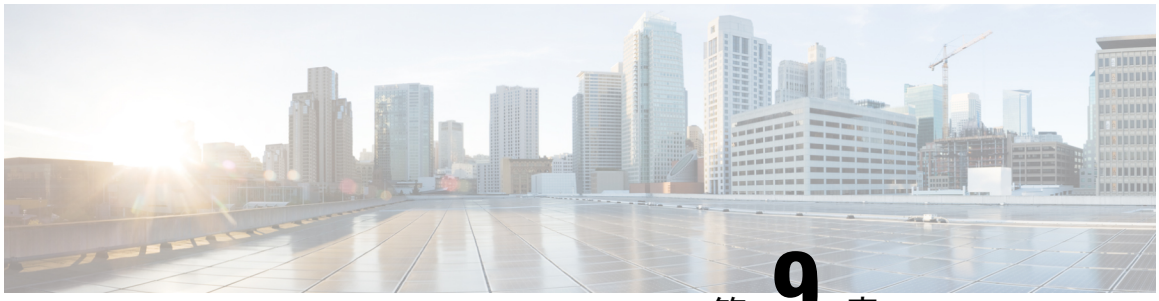
	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **no switching-mode store-forward**	Store-and-Forward スイッチング モードをディセーブルにします。カットスルー スイッチング モードをイネーブルにします。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギ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。

例

次に、カットスルー スイッチングを再度イネーブルにする例を示します。

```
switch# configure terminal
switch(config) # no switching-mode store-forward
switch(config) #
```

（注） コマンド **no switching-mode store-forward** は、Cisco Nexus 9800 シリーズ スイッチではサポートされていません。このプラットフォームではカットスルー モードが使用できないためです。



第 9 章

Cisco NX-OS を使用した Rapid PVST+ の設定

- Rapid PVST+ について, on page 105
- Rapid PVST+ を設定するための前提条件, on page 124
- Rapid PVST+ の設定に関するガイドラインおよび制約事項 （124 ページ）
- Rapid PVST+ のデフォルト設定, on page 125
- Rapid PVST+ の設定, on page 126
- Rapid PVST+ の設定の確認, on page 144
- Rapid PVST+ 統計情報の表示およびクリア（CLI バージョン）, on page 144
- Rapid PVST+ の設定例, on page 144
- Rapid PVST+ の追加情報（CLI バージョン）, on page 145

Rapid PVST+ について

Note レイヤ 2 インターフェイスの作成の詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

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

Note このマニュアルでは、IEEE 802.1w および IEEE 802.1s を指す用語として、「スパニングツリー」を使用します。このマニュアルで IEEE 802.1D STP に関して説明する場合は、具体的に 802.1D と表記されます。

Note Rapid PVST+ はデフォルトの STP モードです。

Rapid PVST+ プロトコルは、VLAN 単位で実装される IEEE 802.1w 標準（高速スパニングツリー プロトコル（RSTP））です。Rapid PVST+ は、個別の VLAN でなく、すべての VLAN に対応する単一の STP インスタンスが規定された IEEE 802.1Q VLAN 標準と相互運用されます。

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

RSTP は、元の STP 規格 802.1D の拡張版で、より高速な収束が可能です。

Note デバイスは、Rapid PVST+ に対して中断のない完全アップグレードをサポートしています。中断のない完全アップグレードの詳細については、『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』を参照してください。

STP

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

STP の概要

レイヤ 2 イーサネット ネットワークが正常に動作するには、2 つの端末間で存在できるアクティブ パスは 1 つだけです。STP の動作はエンド ステーションに対してトランスペアレントなので、単一の LAN セグメントに接続されているのか、それとも複数セグメントからなるスイッチド LAN に接続されているのかを、エンド ステーションが検知することはできません。

フォールトトレラントなインターネットワークを作成する場合、ネットワーク上のすべてのノード間にループフリー パスを構築する必要があります。STP アルゴリズムは、スイッチド レイヤ 2 ネットワーク上で最良のループフリー パスを算出します。レイヤ 2 LAN ポートは STP フレーム（ブリッジ プロトコル データ ユニット（BPDU））を一定の時間間隔で送受信します。ネットワーク デバイスは、これらのフレームを転送せずに、フレームを使用してループフリー パスを構築します。

エンド ステーション間に複数のアクティブ パスがあると、ネットワーク内でループが発生する原因になります。ネットワークにループが存在する場合、エンド ステーションが重複したメッセージを受信したり、ネットワーク デバイスが複数のレイヤ 2 LAN ポート上でエンド ステーション MAC アドレスを学習したりする可能性があります。

STP は、ルート ブリッジおよびそのルートからレイヤ 2 ネットワーク上のすべてのネットワーク デバイスへのループフリー パスを備えたツリーを定義します。STP は冗長データパスを強制的にブロック状態にします。スパニングツリーのネットワーク セグメントに障害が発生した

場合、冗長パスがあると、STP アルゴリズムにより、スパニングツリー トポロジが再計算され、ブロックされたパスがアクティブになります。

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

トポロジの作成方法

スパニングツリーに参加している LAN 内のすべてのデバイスは、BPDU を交換して、ネットワーク内の他のスイッチに関する情報を収集します。この BPDU の交換により、次のアクションが発生します。

- そのスパニングツリー ネットワーク トポロジでルート スイッチが 1 台選択されます。
- LAN セグメントごとに指定スイッチが 1 台選定されます。
- 冗長スイッチ ポートをバックアップ ステートにすることにより、スイッチド ネットワーク上のループが排除されます。スイッチド ネットワーク内のどの場所からも、ルート デバイスに到達するために必要でないパスは、すべて STP ブロック ステートになります。

アクティブなスイッチド ネットワーク上のトポロジは、次の情報によって決定されます。

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

スイッチド ネットワークでは、ルート スイッチが論理的にスパニングツリー トポロジの中心になります。STP は BPDU を使用して、スイッチド ネットワークのルート スイッチおよびルート ポートを選定します。

Note **mac-address bpdu source version 2** STP が新しいシスコの MAC アドレス（00:26:0b:xx:xx:xx）を、vPC ポートで生成される BDPU の発信元アドレスとして使用できるようになります。

このコマンドを適用するには、両方の vPC ピア スイッチまたはピアの設定が同一である必要があります。

STP 不整合に起因するトラフィックの中断を最小限に抑えるため、このコマンドを実行する前に、エッジデバイスの EtherChannel ガードをディセーブルにすることを強くお勧めします。両方のピアの更新後に、EtherChannel ガードを再びイネーブルにします。

ブリッジ ID

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

ブリッジ プライオリティ値

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

デバイスのブリッジ ID（ルート ブリッジの ID を判別するためにスパニングツリー アルゴリズムで使用され、最小値が優先される）に指定できるのは、4096 の倍数だけです。

Note このデバイスでは、拡張システム ID は常にイネーブルです。拡張システム ID をディセーブルにできません。

拡張システム ID を伴わない

デバイスでは常に 12 ビット拡張システム ID が使用されます。

Figure 4: **拡張システム *ID* が指定されたブリッジ *ID***

次の図に、ブリッジ ID の一部である 12 ビット拡張システム ID フィールドを示します。

次の表に、拡張システム ID がどのようにブリッジ ID と組み合わされて、VLAN 固有の識別子として機能するかを示します。

Table 7: **拡張システム *ID* をイネーブルにしたブリッジ プライオリティ値および拡張システム *ID***

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

STP MAC アドレス割り当て

Note デバイスでは常に MAC アドレス リダクションがイネーブルです。

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

MACアドレスリダクションをイネーブルにすると、ルートブリッジプライオリティは、4096 + VLAN ID の倍数となります。デバイスのブリッジ ID（ルート ブリッジの ID を判別するためにスパニングツリーアルゴリズムで使用され、最小値が優先される）に指定できるのは、4096 の倍数だけです。指定できるのは次の値だけです。

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

STP は、拡張システム ID および MAC アドレスを使用して、VLAN ごとにブリッジ ID を一意にします。

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

BPDU

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

- 送信側ネットワーク デバイスがルート ブリッジになると見なしているネットワーク デバイスの固有のブリッジ ID
- ルートまでの STP パス コスト

- 送信側ブリッジのブリッジ ID
- メッセージ経過時間
- 送信側ポートの ID
- Hello タイマー、転送遅延タイマー、最大エージング タイム プロトコル タイマー
- STP 拡張プロトコルの追加情報

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

BPDU 交換によって次の処理が行われます。

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

ルート ブリッジの選定

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

ブリッジ プライオリティ値を変更すると、デバイスがルート ブリッジとして選出される可能性が変わります。小さい値を設定するほどその可能性が大きくなり、大きい値を設定するほどその可能性は小さくなります。

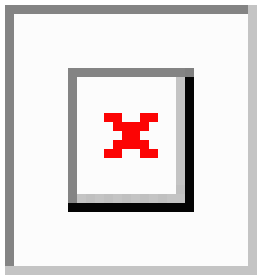
STP ルート ブリッジは、レイヤ 2 ネットワークにおける各スパニングツリー トポロジの論理上の中心です。レイヤ2ネットワーク内のどの場所からでも、ルートブリッジに到達するために必要でないパスは、すべて STP ブロッキング モードになります。

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

スパニングツリー トポロジの作成

最適なネットワーク デバイスがルート ブリッジになるように、デバイスの数値を下げることで、ルートとして最適なネットワーク デバイスを使用する、新しいスパニングツリー トポロジを形成するように強制的に再計算させることができます。

Figure 5: スパニングツリー トポロジ



この図では、スイッチ A がルート ブリッジに選定されます。これは、すべてのネットワーク装置でブリッジプライオリティがデフォルト（32768）に設定されており、スイッチ A の MAC アドレスが最小であるためです。しかし、トラフィック パターン、フォワーディング ポートの数、リンク タイプによっては、スイッチ A が最適なルートブリッジでないことがあります。

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

スイッチ B のあるポートが光ファイバ リンクであり、スイッチ B の別のポート（シールドなしツイストペア（UTP）リンク）がルート ポートであるとします。ネットワーク トラフィックを高速の光ファイバ リンクに流した方が効率的です。光ファイバ ポートの STP ポート プライオリティをルートポートよりも高いプライオリティに変更すると（数値を下げる）、光ファイバ ポートが新しいルート ポートになります。

Rapid PVST+

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

設定された各 VLAN 上で RSTP の単一インスタンスまたはトポロジが実行され、VLAN 上の各 Rapid PVST+ インスタンスに 1 つのルート デバイスが設定されます。Rapid PVST+ の実行中には、VLAN ベースで STP をイネーブルまたはディセーブルにできます。

Rapid PVST+ の概要

Rapid PVST+ は、VLAN ごとに実装されている IEEE 802.1w（RSTP）規格です。（手作業で STP をディセーブルにしていない場合、）STP の 1 つのインスタンスは、設定されている各 VLAN で実行されます。VLAN 上の各 Rapid PVST+ インスタンスには、1 つのルート スイッチがあります。Rapid PVST+ の実行中には、VLAN ベースで STP をイネーブルまたはディセーブルにできます。

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

Rapid PVST+ では、ポイントツーポイントの配線を使用して、スパニングツリーの高速収束が行われます。Rapid PVST+ によりスパニングツリーの再設定を 1 秒未満に発生させることができます（802.1D STP のデフォルト設定では 50 秒）。PVID は自動的にチェックされます。

Note Rapid PVST+ では、VLAN ごとに 1 つの STP インスタンスがサポートされます。

Rapid PVST+ を使用すると、STP コンバージェンスが急速に発生します。デフォルトでは、STP 内の各指定ポートは 2 秒おきに BPDU を送信します。トポロジ内の指定ポートで、hello メッセージが 3 回連続して受信されない場合、または最大エージング タイムが満了した場合、ポートはテーブル内のすべてのプロトコル情報をただちに消去します。ポートで BPDU が受信されなかった回数が 3 に達するか、または最大エージング タイムが満了した場合、ポートは直接接続されたネイバーの指定ポートとの接続が切断されていると見なします。プロトコル情報の急速な経過により、障害検出を迅速に行うことができます。

Rapid PVST+ を使用すると、デバイス、デバイス ポート、または LAN の障害後に、接続をすばやく回復できます。エッジ ポート、新しいルート ポート、ポイントツーポイント リンクで接続したポートに、高速コンバージェンスが次のように提供されます。

- エッジ ポート：RSTP デバイスでエッジ ポートとしてポートを設定すると、エッジ ポートはフォワーディング ステートにすぐに移行します（この急速な移行は、PortFast と呼ばれていたシスコ特有の機能でした）。エッジ ポートとして 1 つのエンド ステーションに接続されているポートにのみ、設定する必要があります。エッジポートでは、リンクの変更時にはトポロジの変更は生成されません。

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

Note レイヤ 2 ホストに接続されたすべてのポートをエッジ ポートとして設定することを推奨します。

- ルート ポート：Rapid PVST+ が新規ルート ポートを選択した場合、古いルート ポートをブロックして、即座に新規ルート ポートをフォワーディング ステートに移行します。
- ポイントツーポイント リンク：ポイントツーポイント リンクによってあるポートと別のポートを接続することでローカル ポートが指定ポートになると、提案合意ハンドシェイクを使用して他のポートと急速な移行がネゴシエートされ、トポロジにループがなくなります。

Rapid PVST+ では、エッジ ポートとポイントツーポイント リンクでのみ、フォワーディング ステートへの急速な移行が達成されます。リンク タイプは設定が可能ですが、システムでは、

ポートのデュプレックス設定からリンク タイプ情報が自動的に引き継がれます。全二重ポートはポイントツーポイント ポートであると見なされ、半二重ポートは共有ポートであると見なされます。

エッジ ポートでは、トポロジの変更は生成されませんが、直接接続されているネイバーから 3 回連続 BPDU の受信に失敗するか、最大経過時間のタイム アウトが発生すると、他のすべての指定ポートとルート ポートにより、トポロジ変更（TC）BPDU が生成されます。この時点で、指定ポートまたはルート ポートは TC フラグが設定された BPDU を送信します。BPDU では、ポート上で TC While タイマーが実行されている限り、TC フラグが設定され続けます。TC While タイマーの値は、hello タイムに 1 秒を加えて設定された値です。トポロジ変更の初期ディテクタにより、トポロジ全体で、この情報がフラッディングされます。

Rapid PVST+ により、トポロジの変更が検出される場合、プロトコルでは次の処理が発生します。

- 必要に応じて、すべての非エッジ ルート ポートおよび指定ポートに対して、hello タイムの 2 倍の値に設定された TC While タイマーを開始します。
- これらのすべてのポートにアソシエートされている MAC アドレスがフラッシュされます。

トポロジ変更通知は、トポロジ全体で迅速にフラッディングされます。システムでトポロジの変更が受信されると、システムにより、ポート ベースでダイナミック エントリがただちにフラッシュされます。

Note TCA フラグが使用されるのは、そのデバイスが、レガシー 802.1D STP が稼働しているデバイスと相互作用している場合のみです。

トポロジの変更後、提案と合意のシーケンスがネットワークのエッジ方向に迅速に伝播され、接続がただちに回復します。

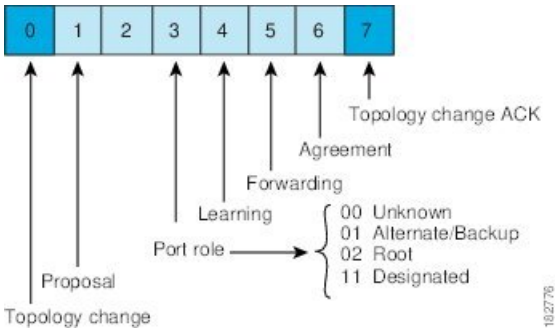
Rapid PVST+ BPDU

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

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

Figure 6: BPDU の Rapid PVST+ フラグ バイト

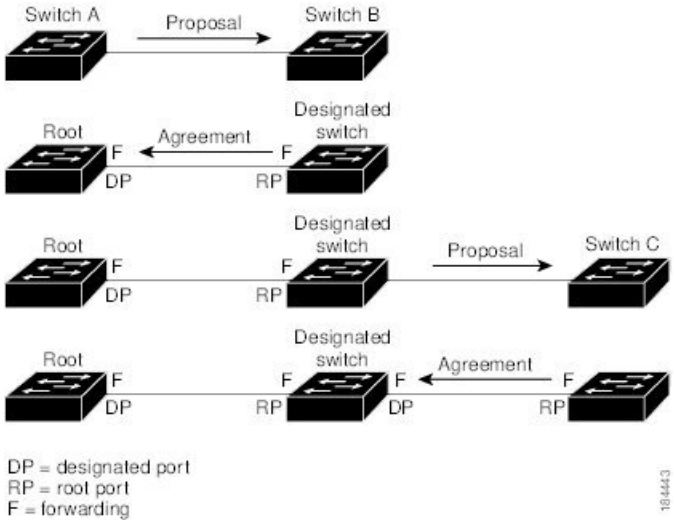
次の図に、Rapid PVST+ の BPDU フラグの使用法を示します。



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

提案と合意のハンドシェイク

Figure 7: 高速コンバージェンスの提案と合意のハンドシェイク



次の図では、スイッチ A がスイッチ B にポイントツーポイント リンクで接続され、すべてのポートはブロッキング ステートになっています。スイッチ A のプライオリティがスイッチ B のプライオリティよりも数値的に小さいとします。スイッチ A は提案メッセージ（提案フラグを設定した設定 BPDU）をスイッチ B に送信し、指定スイッチとしてそれ自体を提案します。

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

スイッチ B から合意 メッセージの受信後、スイッチ A でも、その指定ポートがただちにフォワーディング ステートに移行されます。スイッチ B がエッジ以外のすべてのポートをブロックし、かつスイッチ A とスイッチ B の間にポイントツーポイント リンクがあるので、ネットワークでループは形成されません

スイッチ C がスイッチ B に接続されると、類似したハンドシェイク メッセージのセットがやり取りされます。スイッチ C は、そのルート ポートとしてスイッチ B に接続されたポートを選択し、リンクの両端がただちにフォワーディング ステートになります。アクティブ トポロジにスイッチが追加されるたびに、このハンドシェイク プロセスが実行されます。ネットワークが収束するにつれて、提案と合意のハンドシェイクは、次の図に示すようにスパニング ツリーのルートからリーフに向かって進みます。

スイッチはポートのデュプレックス モードからリンク タイプを学習します。全二重ポートはポイントツーポイント接続と見なされ、半二重ポートは共有接続と見なされます。**spanning-tree link-type** を入力すると、デュプレックス設定によって制御されるデフォルト設定を無効にすることができます。 interface configuration コマンド

この提案と合意のハンドシェイクが開始されるのは、非エッジ ポートがブロッキング ステートからフォワーディング ステートに移行した場合だけです。次に、ハンドシェイク処理は、トポロジ全体に段階的に広がります。

プロトコル タイマー

次の表に、Rapid PVST+ のパフォーマンスに影響するプロトコル タイマーを示します。

***Table 8: Rapid PVST+* プロトコル タイマー**

変数	説明
ハロー タイマー	ネットワーク装置間で BPDU をブロードキャストする頻度を決定します。デフォルトは 2 秒で、範囲は 1 ～ 10 です。
転送遅延タイマー	ポートが転送を開始するまでの、リスニング ステートおよびラーニング ステートが継続する時間を決定します。このタイマーは通常、プロトコルによっては使用されませんが、802.1D スパニングツリーと相互に動作するときに使用されます。デフォルトは 15 秒で、範囲は 4 ～ 30 秒です。
最大エージング タイマー	ポートで受信したプロトコル情報がネットワーク デバイスで保持される期間を決定します。このタイマーは通常、プロトコルによっては使用されませんが、802.1D スパニングツリーと相互に動作するときに使用されます。デフォルトは 20 秒で、範囲は 6 ～ 40 秒です

ポート ロール

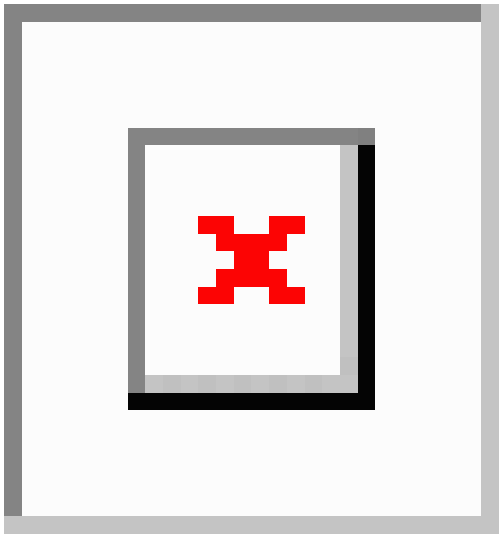
Rapid PVST+ では、ポート ロールを割り当て、アクティビティ トポロジを認識することによって、高速収束が行われます。Rapid PVST+ は、802.1D STP を利用して、最も高いスイッチ プライオリティ（最小プライオリティ値）を持つデバイスをルート ブリッジとして選択します。Rapid PVST+ により、次のポートのロールの 1 つが個々のポートに割り当てられます。

- ルート ポート：デバイスがルート ブリッジにパケットを転送するとき、最適な（コストが最小の）パスを提供します。

- 指定ポート：LAN からルート ブリッジにパケットを転送するとき、最小パス コストになる指定デバイスに接続します。指定デバイスが LAN への接続に使用したポートは、指定ポートと呼ばれます。
- 代替ポート：現在のルート ポートによって用意されているパスに、ルート ブリッジへの代替パスを用意します。また、トポロジ内の別のデバイスへのパスを提供します。
- バックアップ ポート：指定ポートが提供した、スパニング ツリーのリーフに向かうパスのバックアップとして機能します。2つのポートがポイントツーポイントリンクによってループバックで接続した場合、または共有 LAN セグメントへの複数の接続がデバイスにある場合に限り、バックアップ ポートは存在できます。バックアップ ポートは、トポロジ内のデバイスに対する別のパスを提供します。
- ディセーブル ポート：スパニング ツリーの動作において何もロールが与えられていません。

ネットワーク全体でポートのロールに一貫性のある安定したトポロジでは、Rapid PVST+ により、ルート ポートと指定ポートがすべてただちにフォワーディング ステートになり、代替ポートとバックアップ ポートはすべて、必ずブロッキング ステートになります。指定ポートはブロッキング ステートで開始されます。ポートのステートにより、転送処理および学習処理の動作が制御されます。

Figure 8: ポートのロールをデモンストレーションするトポロジのサンプル



次の図はポート ロールを示しています。ルート ポートまたは指定ポートのロールを持つポートは、アクティブなトポロジに含まれます。代替ポートまたはバックアップ ポートのロールがあるポートは、アクティブ トポロジから除外されます。

Rapid PVST+ ポート ステートの概要

プロトコル情報がスイッチド LAN を通過するとき、伝播遅延が生じることがあります。その結果、スイッチド ネットワークのさまざまな時点および場所でトポロジーの変化が発生します。レイヤ2LANポートがスパニングツリートポロジに含まれていない状態からフォワーディ

ング ステートに直接遷移すると、一時的にデータ ループが発生する可能性があります。ポートは新しいトポロジー情報がスイッチド LAN 経由で伝播されるまで待機し、それからフレーム転送を開始する必要があります。

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

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

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

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

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

ブロッキング ステート

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

ブロッキング ステートのレイヤ 2 LAN ポートは、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 モジュールから送られた BPDU を受信し、処理して送信します。
- コントロール プレーン メッセージを受信して応答します。

ラーニング ステート

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

ラーニング ステートのレイヤ 2 LAN ポートは、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を、そのアドレス データベースに取り入れます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから送られた BPDU を受信し、処理して送信します。
- コントロール プレーン メッセージを受信して応答します。

フォワーディング ステート

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

フォワーディング ステートのレイヤ 2 LAN ポートは、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転送します。
- 転送用に他のポートからスイッチングされたフレームを転送します。
- エンド ステーションの場所情報を、そのアドレス データベースに取り入れます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから受信した BPDU を処理します。
- コントロール プレーン メッセージを受信して応答します。

ディセーブル ステート

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

ディセーブルになったレイヤ 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（ラーニングは行われないため、アドレス データベースは更新されません）。
- ネイバーから BPDU を受信しません。
- システム モジュールから送信用の BPDU を受信しません。

ポート ステートの概要

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

Table 9: アクティブなトポロジのポート ステート

動作ステータス（Operational Status）	ポート状態	ポートがアクティブ トポロジに含まれているか
イネーブル	ブロッキング	いいえ
有効	ラーニング	はい
有効	転送	はい
無効	無効	×

ポート ロールの同期

デバイスがいずれかのポートで提案メッセージを受信し、そのポートが新しいルート ポートとして選択されると、Rapid PVST+ はその他すべてのポートを新しいルート情報で同期化します。

その他すべてのポートを同期化する場合、ルート ポートで受信した優位ルート情報でデバイスは同期化されます。次のうちいずれかが当てはまる場合、デバイスのそれぞれのポートは同期化されます。

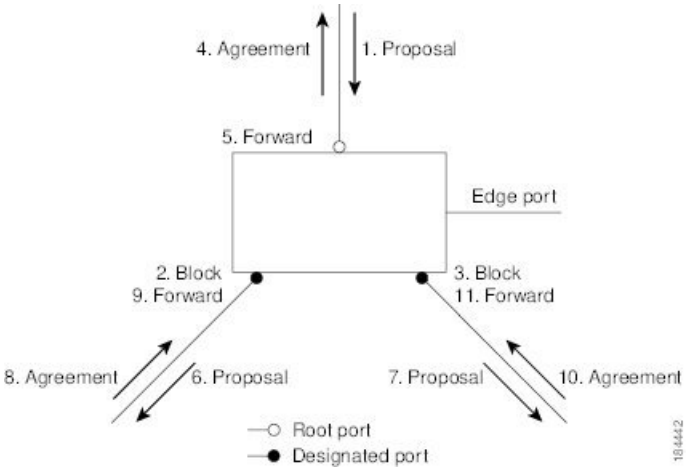
- ポートがブロッキング ステートである。
- エッジ ポートである（ネットワークのエッジに存在するように設定されたポート）。

指定されたポートは、フォワーディング ステートになっていてエッジ ポートとして設定されていない場合、Rapid PVST+ によって強制的に新しいルート情報で同期化されると、ブロッキング ステートに移行します。一般的に、Rapid PVST+ により、強制的にルート情報との同期がとられる場合で、ポートで前述の条件のいずれかが満たされない場合、ポート ステートはブロッキングに設定されます。

すべてのポートが同期化されてから、デバイスは、ルート ポートに対応する指定デバイスに合意メッセージを送信します。ポイントツーポイント リンクで接続されたデバイスがポート ロールについて合意すると、Rapid PVST+ はポート ステートをフォワーディング ステートにただちに移行します。

Figure 9: 高速コンバージェンス中のイベントのシーケンス

次の図は、同期中のイベントのシーケンスを示しています。



優位 BPDU 情報の処理

上位BPDUとは、自身のために現在保存されているものより上位であるルート情報（より小さいスイッチ ID、より小さいパス コストなど）を持つ BPDU のことです。

上位 BPDU がポートで受信されると、Rapid PVST+ は再設定を起動します。そのポートが新しいルート ポートとして提案され選択されると、Rapid PVST+ はすべての非エッジ、指定ポートを強制的に同期化します。

受信した BPDU が提案フラグを設定した Rapid PVST+ BPDU である場合、その他すべてのポートが同期化されたあとで、デバイスは合意メッセージを送信します。前のポートがブロッキング ステートになるとすぐに、新しいルート ポートがフォワーディング ステートに移行します。

ポートで受信した上位情報によりポートがバックアップ ポートまたは代替ポートになる場合、Rapid PVST+ はポートをブロッキング ステートに設定し、合意メッセージを送信します。指定ポートは、転送遅延タイマーが期限切れになるまで、提案フラグが設定された BPDU を送信し続けます。期限切れになると、ポートはフォワーディング ステートに移行します。

下位 BPDU 情報の処理

下位BPDUとは、自身のために現在保存されているものより下位であるルート情報（より大きいスイッチ ID、より大きいパス コストなど）を持つ BPDU のことです。

DP は、下位 BPDU を受信すると、独自の情報で直ちに応答します。

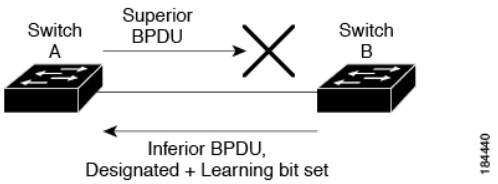
単方向リンク障害の検出：Rapid PVST+

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

UDLD の詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

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

Figure 10: 単一方向リンク障害の検出



次の図に、ブリッジングループの一般的な原因となる単方向リンク障害を示します。スイッチ A はルート ブリッジであり、スイッチ B へのリンクで BPDU は失われます。802.1w 業界標準 BPDUには、送信側ポートの役割と状態が含まれます。この情報により、スイッチBは送信される上位 BPDU に対して反応せず、スイッチ B はルート ポートではなく指定ポートであることが、スイッチ A によって検出できます。この結果、スイッチ A は、そのポートをブロックし（またはブロックし続け）、ブリッジング ループが防止されます。

ポートコスト

Note Rapid PVST+はデフォルトで、ショート（16 ビット）パスコスト方式を使用してコストを計算します。ショートパスコスト方式では、1 ～ 65,535 の範囲で任意の値を割り当てることができます。ただし、ロング（32 ビット）パスコスト方式を使用するようにデバイスを設定できます。この場合は、1 ～ 200,000,000 の範囲で任意の値を割り当てることができます。パスコスト計算方式はグローバルに設定します。

次の表に、LAN インターフェイスのメディア速度とパスコスト計算方式を使用して算出された STP ポート パスコストのデフォルト値を示します。

Table 10: デフォルト ポート コスト

帯域幅	ポートコストのショートパスコスト方式	ポートコストのロングパスコスト方式
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
10 Gbps	2	2,000
40 Gbps	1	500
100 Gbps	1	200
400 Gbps	1	50

ループが発生した場合、STP では、LAN インターフェイスの選択時に、フォワーディング ステートにするためのポート コストを考慮します。

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

アクセス ポートでは、ポート コストをポートごとに割り当てます。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ため、トランク ポート上のすべての VLAN に同じポート コストを設定できます。

ポートプライオリティ

複数のポートのパス コストが同じである場合に、冗長パスが発生すると、Rapid PVST+ はポート プライオリティを考慮して、フォワーディング ステートにする LAN ポートを選択します。Rapid PVST+ に最初に選択させる 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。指定可能なプライオリティの範囲は 0 ～ 224（デフォルトは 128）であり、32 単位で設定できます。デバイスは LAN ポートがアクセス ポートとして設定されている場合にはポート プライオリティ値を使用し、LAN ポートがトランク ポートとして設定されている場合には VLAN ポート プライオリティ値を使用します。

Rapid PVST+ と IEEE 802.1Q トランク

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

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

802.1Q トランクの詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

Rapid PVST+ のレガシー 802.1D STP との相互運用

Rapid PVST+ は、レガシー 802.1D プロトコルが稼働しているデバイスと相互運用できます。デバイスは、BPDU バージョン 0 を受信すると、802.1D を実行している機器と相互運用していることを認識します。Rapid PVST+ の BPDU はバージョン 2 です。受信した BPDU が、提案フラグを設定した 802.1w BPDU バージョン 2 である場合、デバイスはその他すべてのポートが同期化した後で合意メッセージを送信します。BPDU が 802.1D BPDU バージョン 0 である場合、デバイスは提案フラグを設定せず、ポートの転送遅延タイマーを開始します。新しいルートポートでは、フォワーディング ステートに移行するために、2 倍の転送遅延時間が必要となります。

デバイスは、次のように、レガシー 802.1D デバイスと相互運用します。

- 通知：802.1D BPDU とは異なり 802.1w は、TCN BPDU を使用しません。ただし、802.1D デバイスと相互運用性を保つために、デバイスは TCN BPDU の処理と生成を行います。
- 確認応答：802.1w デバイスは、802.1D デバイスから指定ポートで TCN メッセージを受信すると、TCA ビットを設定して 802.1D コンフィギュレーション BPDU で応答します。ただし、802.1D デバイスに接続しているルート ポートで TC While タイマー（802.1D の TC タイマーと同じ）がアクティブであり、TCA を設定したコンフィギュレーション BPDU を受信した場合、TC While タイマーはリセットされます。

  この動作方式は 802.1D デバイスだけで必要となります。802.1w BPDU では、TCA ビットは設定されません。
- プロトコル移行：802.1D デバイスとの下位互換性のため、802.1w は 802.1D コンフィギュレーション BPDU および TCN BPDU をポートごとに選択的に送信します。

  ポートが初期化されると、移行遅延タイマー（802.1w BPDU が送信される最小時間を指定）が開始され、802.1w BPDU が送信されます。このタイマーがアクティブである間、デバイスはそのポートで受信したすべての BPDU を処理し、プロトコル タイプを無視します。

  デバイスは、ポート移行遅延タイマーの満了後に 802.1D BPDU を受信すると、802.1D デバイスに接続されていると見なして 802.1D BPDU だけを使用し始めます。ただし、802.1w デバイスが 802.1D BPDU をポートで使用しており、タイマーの満了後に 802.1w BPDU を受信すると、802.1w デバイスはタイマーを再開し、802.1w BPDU をそのポートで使用し始めます。

Note 同じ LAN セグメント上のすべてのデバイスで、インターフェイスごとにプロトコルを再初期化する場合は、Rapid PVST+ を再初期化する必要があります。

Rapid PVST+ の 802.1s MST との相互運用

Rapid PVST+ は、IEEE 802.1s マルチ スパニングツリー（MST）規格とシームレスに相互運用されます。ユーザによる設定は不要です。このシームレスな相互運用をディセーブルにするには、PVST シミュレーションを使用します。

Rapid PVST+ のハイ アベイラビリティ

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

Note ハイ アベイラビリティ機能の詳細については、『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

Rapid PVST+ を設定するための前提条件

Rapid PVST+ には次の前提条件があります。

- デバイスにログインしていること。

Rapid PVST+ の設定に関するガイドラインおよび制約事項

Rapid PVST+ 設定時のガイドラインと制限事項は次のとおりです。

- **show** コマンド（**internal** キーワード付き ）はサポートされていません。
- VLAN 設定制限については『*Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*』を参照してください。
- ポート チャネリング：ポート チャネル バンドルは、単一ポートと見なされます。ポート コストは、そのチャネルに割り当てられている設定済みのすべてのポート コストの合計です。
- レイヤ 2 ホストに接続されたすべてのポートを STP エッジ ポートとして設定することを推奨します。
- STP は常にイネーブルのままにしておきます。
- タイマーは変更しないでください。安定性が低下することがあります。
- ユーザ トラフィックが管理 VLAN に流れないようにして、管理 VLAN とユーザ データを常に分離するようにしてください。

- プライマリおよびセカンダリ ルート スイッチの場所として、ディストリビューション レイヤおよびコア レイヤを選択します。
- 802.1Q トランクを介して 2 台のシスコ デバイスを接続すると、トランク上で許容される VLAN ごとにスパニングツリー BPDU が交換されます。トランクのネイティブ VLAN 上の BPDUは、タグなしの状態で、予約済み802.1Dスパニングツリーマルチキャスト MAC アドレス（01-80-C2-00-00-00）に送信されます。トランクのすべての VLAN 上の BPDU は、タグ付きの状態で、予約済み Cisco Shared Spanning Tree Protocol（SSTP）マルチキャスト MAC アドレス（01-00-0c-cc-cc-cd）に送信されます。

Rapid PVST+ のデフォルト設定

次の表に、Rapid PVST+ パラメータのデフォルト設定を示します。

Table 11: 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+ **Caution** 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）
ポートのステート	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	short

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。 • 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 • 40 ギガビット イーサネット： • ショート：1 • ロング：500
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。

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。同じシャーシ上で MST と Rapid PVST+ を同時に実行することはできません。

Note 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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mode rapid-pvst** **Example:** `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。 **Note** 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**
	Example:
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

	Command or Action	Purpose
ステップ 4	(Optional) **show running-config spanning-tree all** **Example:** `switch# show running-config spanning-tree all`	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	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

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#
```

Note Rapid PVST +はデフォルトで有効になっているため、 **show running** 設定結果を参照するためにshow runningコマンドを入力しても、RapidPVST+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。

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。

Note 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。

SUMMARY STEPS

1. **config t**
2. **spanning-tree vlan** *vlan-range* or **no spanning-tree vlan** *vlan-range*
3. **exit**
4. (Optional) **show spanning-tree**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree vlan** *vlan-range* or **no spanning-tree vlan** *vlan-range* **Example:** `switch(config)# spanning-tree vlan 5`	• **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 ～ 3967 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。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show spanning-tree** **Example:** `switch# show spanning-tree`	STP の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

次の例は、VLAN 5 で STP をイネーブルにする方法を示しています。

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

Note 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。スパニングツリーは、VLAN の一部のスイッチおよびブリッジでディセーブルにしておきながら、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。

Caution 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。

Note STPはデフォルトで有効になっているため、show running 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。

次のコマンドを入力すると、 **spanning-tree vlan** *vlan-range* **root primary** コマンドを 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。

Caution 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。

Note ルート ブリッジとして設定されたデバイスで、**spanning-tree mst hello-time** を使用して hello タイム、転送遅延時間、最大エージング タイムを手動で設定しないでください。, **spanning-tree mst forward-time**, and **spanning-tree mst max-age** グローバル設定コマンド。

SUMMARY STEPS

1. **config t**
2. **spanning-tree vlan** *vlan-range* **root primary**
3. **exit**
4. (Optional) **show spanning-tree**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree vlan** *vlan-range* **root primary** **Example:** `switch(config)# spanning-tree vlan 2 root primary`	スパニングツリーのルート ブリッジのブリッジ プライオリティを設定します。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show spanning-tree** **Example:** `switch# show spanning-tree`	STP の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

次に、デバイスをルート ブリッジとして設定する例を示します。

```
switch# config t
switch(config)# spanning-tree vlan 2 root primary
switch(config)# exit
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。

diameterを入力します 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 台の端末間におけるブリッジ ホップの最大数）を指定するには、 キーワードを使用します。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、最大エージング タイムが自動的に選択されます。これにより、STP コンバージェンスの時間が大幅に削減されます。**hello-time** を入力できます。 キーワードを使用して、自動的に計算される hello タイムをオーバーライドできます。

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。

Note ルート ブリッジとして設定されたデバイスで、**spanning-tree mst hello-time** を使用して hello タイム、転送遅延時間、最大エージング タイムを手動で設定しないでください。, **spanning-tree mst forward-time**, and **spanning-tree mst max-age** グローバル設定コマンド。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**config t** **Example:**	コンフィギュレーション モードに入ります。

	Command or Action	Purpose
	`switch# config t` `switch(config)#`	
ステップ 2	**spanning-tree vlan** *vlan-range* **root secondary** [**diameter** *dia* [**hello-time** *hello-time*]] **Example:** `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 ～ 3967 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**
	Example:
	`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	(Optional) **show spanning-tree vlan** *vlan_id* **Example:** `switch# show spanning-tree vlan 5`	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	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

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。

Note 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。

SUMMARY STEPS

1. **config t**
2. **spanning-tree vlan** *vlan-range* **priority** *value*

3. **exit**
4. (Optional) **show spanning-tree vlan** *vlan_id*
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree vlan** *vlan-range* **priority** *value* **Example:** `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。その他の値はすべて拒否されます。デフォルト値は 32768 です。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show spanning-tree vlan** *vlan_id* **Example:** `switch# show spanning-tree vlan 5`	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	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *type slot/port*
	Example:
	`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* **Example:** `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。その他の値はすべて拒否されます。デフォルト値は 128 です。

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

	Command or Action	Purpose
ステップ 5	(Optional) **show spanning-tree interface** {**ethernet** *slot/port* | *port channel channel-number*} **Example:** `switch# show spanning-tree interface ethernet 2/10`	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	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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。

Note 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。

SUMMARY STEPS

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. (Optional) **show spanning-tree pathcost method**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree pathcost method** {**long** | **short**} **Example:** `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*
	Example:
	`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*] **Example:** `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 **Note** 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。

ステップ 5	**exit**
	Example:
	`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	(Optional) **show spanning-tree pathcost method** **Example:** `switch# show spanning-tree pathcost method`	STP パスコスト方式を表示します。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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。

Note 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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree vlan** *vlan-range* **hello-time** *value* **Example:** `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** **Example:**	コンフィギュレーション モードを終了します。

	Command or Action	Purpose
	`switch(config)# exit` `switch#`	
ステップ 4	(Optional) **show spanning-tree vlan** *vlan_id* **Example:** `switch# show spanning-tree vlan 5`	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	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	Command or Action	Purpose
ステップ 2	**spanning-tree vlan** *vlan-range* **forward-time** *value* **Example:** `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**
	Example:
	`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	(Optional) **show spanning-tree vlan** *vlan_id* **Example:** `switch# show spanning-tree vlan 5`	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	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree vlan** *vlan-range* **max-age** *value* **Example:** `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**
	Example:
	`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	(Optional) **show spanning-tree vlan** *vlan_id* **Example:** `switch# show spanning-tree vlan 5`	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	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *type slot/port*
	Example:
	`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*} **Example:** `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**
	Example:
	`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	(Optional) **show spanning-tree** **Example:** `switch# show spanning-tree`	STP の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**clear spanning-tree detected-protocol** [**interface** {**ethernet** *slot/port* | **port channel** *channel-number*}] **Example:** `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。

Example

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。
show spanning-treeshow 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 vlanshow spanning-tree vlan *vlan-id* **bridge**	STP ブリッジの情報を表示します。

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

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

switch(config)# 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)#
```

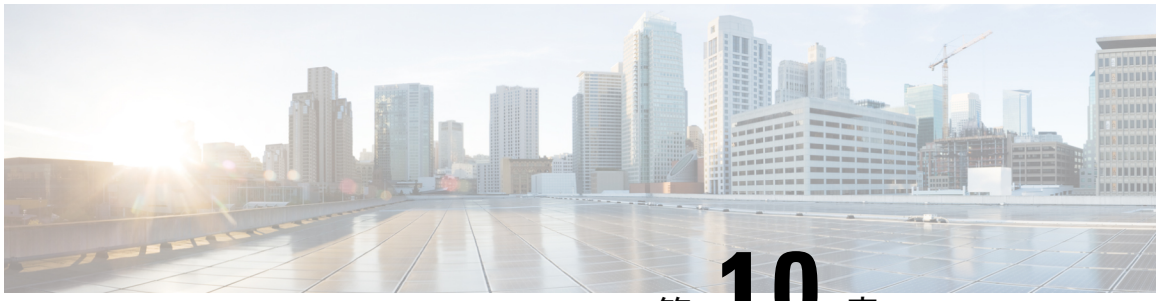
Rapid PVST+ の追加情報（CLI バージョン）

関連資料

関連項目	マニュアル タイトル
レイヤ2インターフェイス	『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』
Cisco NX-OS の基礎	『*Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide*』
システム管理	『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』

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	—



第 10 章

Cisco NX-OS を使用した MST の設定

- MST について, on page 147
- MST の前提条件, on page 156
- MST の設定に関するガイドラインおよび制約事項 （156 ページ）
- MST のデフォルト設定, on page 158
- MST の設定, on page 159
- MST の設定の確認, on page 186
- MST 統計情報の表示およびクリア（CLI バージョン）, on page 187
- MST の設定例, on page 187
- MST の追加情報（CLI バージョン）, on page 189

MST について

Note レイヤ 2 インターフェイスの作成の詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

IEEE 802.1s 標準の MST を使用すると、スパニングツリー インスタンスに複数の VLAN を割り当てることができます。MST は、デフォルトのスパニングツリー モードではありません。Rapid per VLAN Spanning Tree（Rapid PVST+）がデフォルト モードです。MST インスタンスは、同じ名前、リビジョン番号、VLAN からインスタンスへのマッピングと組み合わされて、MST 領域が形成されます。MST 領域は、領域外のスパニングツリー設定への単一のブリッジとして表示されます。MST がネイバー デバイスから IEEE 802.1D スパニングツリー プロトコル（STP）メッセージを受信すると、該当するインターフェイスとの境界が形成されます。

Note このマニュアルでは、IEEE 802.1w および IEEE 802.1s を指す用語として、「スパニングツリー」を使用します。このマニュアルで IEEE 802.1D スパニングツリー プロトコルに関して説明する場合は、具体的に 802.1D と表記されます。

MST の概要

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

MST は、複数の VLAN をスパニングツリー インスタンスにマッピングします。各インスタンスには、他のスパニングツリーインスタンスとは別のスパニングツリー トポロジがあります。このアーキテクチャでは、データ トラフィックに対して複数のフォワーディング パスがあり、ロード バランシングが可能です。これによって、非常に多数の VLAN をサポートする際に必要な STP インスタンスの数を削減できます。MST では、1 つのインスタンス（転送パス）で障害が発生しても他のインスタンス（転送パス）に影響しないため、ネットワークのフォールト トレランスが向上します。

MST では、各 MST インスタンスで IEEE 802.1w 規格を採用することによって、明示的なハンドシェイクによる高速収束が可能なため、802.1D 転送遅延がなくなり、ルート ブリッジ ポートと指定ポートが迅速にフォワーディング ステートに変わります

デバイスでは常にMACアドレス リダクションがイネーブルです。この機能はディセーブルにはできません。

MST ではスパニング ツリーの動作が改善され、次の STP バージョンとの下位互換性を維持しています。

- 元の 802.1D スパニング ツリー
- Rapid per-VLAN スパニングツリー（Rapid PVST+）

Note

- IEEE 802.1 は、Rapid Spanning Tree Protocol（RSTP）で定義されて、IEEE 802.1D に組み込まれました。
- IEEE 802.1 は MST で定義され、IEEE 802.1Q に組み込まれました。

。

MST 領域

MST インスタンスにデバイスを参加させるには、常に同じ MST 設定情報を使用してデバイスを設定する必要があります。

同一の MST 設定を持つ、相互接続されたデバイスの集合を MST 領域といいます。MST リージョンは、同じ MST 設定で MST ブリッジのグループとリンクされます。

MST 設定により、各デバイスが属する MST 領域が制御されます。この設定には、領域名、リビジョン番号、VLAN/MST インスタンス割り当てマッピングが含まれます。

リージョンには、同一の MST コンフィギュレーションを持った 1 つまたは複数のメンバが必要です。各メンバには、802.1w Bridge Protocol Data Unit（BPDU：ブリッジ プロトコル データ ユニット）を処理する機能が必要です。ネットワーク内の MST リージョンには、数の制限はありません。

各デバイスは、単一の MST 領域内で、インスタンス 0 を含む最大 65 個の MST インスタンスをサポートできます。インスタンスは、1 ～ 4094 の範囲の任意の番号によって識別されます。インスタンス 0 は、特別なインスタンスである IST 用に予約されています。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。

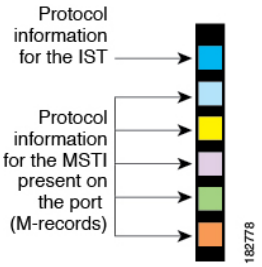
MST 領域は、隣接の MST 領域、他の Rapid PVST+ 領域、802.1D スパニングツリー プロトコルへの単一のブリッジとして表示されます。

Note ネットワークを、非常に多数の領域に分けることは推奨しません。

MST BPDU

各デバイスで使用できる MST BPDU は、インターフェイスごとに 1 つだけです。この BPDU が、デバイス上の各 MSTI の M レコードを伝達します。IST だけが MST リージョンの BPDU を送信します。すべての M レコードは、IST が送信する 1 つの BPDU でカプセル化されています。MST BPDU はすべてのインスタンスの情報を伝送するため、MST をサポートするために処理しなければならない BPDU の数は、Rapid PVST+ と比べて大幅に削減されます。

Figure 11: MSTI の M レコードが含まれる MST BPDU



MST 設定情報

単一の MST 領域内にあるすべてのデバイスで MST 設定を同一にする必要がある場合は、ユーザ側で設定します。

MST 設定では、次の 3 つのパラメータを設定できます。

- 名前：32 文字の文字列。MST リージョンを指定します。ヌルで埋められ、ヌルで終了します。
- リビジョン番号：現在の MST 設定のリビジョンを指定する 16 ビットの符号なし数字。

Note MST 設定の一部として必要な場合、リビジョン番号を設定する必要があります。MST 設定をコミットするたびにリビジョン番号が自動的に増加することはありません。

- VLAN/MST インスタンス マッピング：要素が 4096 あるテーブルで、サポート対象の、存在する可能性のある各 VLAN が該当のインスタンスに関連付けられます。最初（0）と最後（4095）の要素は 0 に設定されています。要素番号 X の値は、VLAN X がマッピングされるインスタンスを表します。

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

MST BPDU には、これらの 3 つの設定パラメータが含まれています。MST ブリッジは、これら 3 つの設定パラメータが厳密に一致する場合、MST BPDU をそのリージョンに受け入れます。設定属性が 1 つでも異なっていると、MST ブリッジでは、BPDU が別の MST リージョンのものであると見なされます。

IST、CIST、CST

IST、CIST、CST の概要

すべての STP インスタンスが独立している Rapid PVST+ と異なり、MST は IST、CIST、および CST スパニングツリーを次のように確立して、維持します。

- IST は、MST 領域で実行されるスパニングツリーです。

  MST は、それぞれの MST 領域内で追加のスパニングツリーを確立して維持します。このスパニングツリーは、Multiple Spanning Tree Instance（MSTI）と呼ばれます。

  インスタンス 0 は、IST という、領域の特殊インスタンスです。IST は、すべてのポートに必ず存在します。IST（インスタンス 0）は削除できません。デフォルトでは、すべての VLAN が IST に割り当てられます。その他すべての MSTI には、1 ～ 4094 の番号が付きます。

  IST は、BPDU の送受信を行う唯一の STP インスタンスです。他の MSTI 情報はすべて MST レコード（M レコード）に含まれ、MST BPDU 内でカプセル化されます。

  同じリージョン内のすべての MSTI は同じプロトコル タイマーを共有しますが、各 MSTI には、ルート ブリッジ ID やルート パス コストなど、それぞれ独自のトポロジ パラメータがあります。

  MSTI は、リージョンに対してローカルです。たとえば、リージョン A とリージョン B が相互接続されている場合でも、リージョン A にある MSTI 9 は、リージョン B にある MSTI 9 には依存しません。領域の境界をまたいで使用されるのは、CST 情報だけです。

- CST は、MST リージョンと、ネットワーク上で実行されている可能性がある 802.1D および 802.1w STP のインスタンスを相互接続します。CST は、ブリッジ型ネットワーク全体

で 1 つ存在する STP インスタンスで、すべての MST リージョン、802.1w インスタンスおよび 802.1D インスタンスを含みます。

- CIST は、各 MST リージョンの IST の集合です。CIST は、MST リージョン内部の IST や、MST リージョン外部の CST と同じです。

MST 領域で計算されるスパニングツリーは、スイッチ ドメイン全体を含んだ CST 内のサブツリーとして認識されます。CIST は、802.1w、802.1s、802.1D 標準をサポートするデバイスで動作するスパニングツリーアルゴリズムによって形成されます。MST リージョン内の CIST は、リージョン外の CST と同じです。

MST 領域内でのスパニングツリーの動作

IST は領域内のすべての MST デバイスを接続します。IST が収束すると、IST のルートは CIST リージョナル ルートになります。ネットワークに領域が 1 つしかない場合、CIST リージョナル ルートは CIST ルートにもなります。CIST ルートが領域外にある場合、領域の境界にある MST デバイスの 1 つが CIST リージョナル ルートとして選択されます。

MST デバイスは、初期化されると、CIST のルートおよび CIST リージョナル ルートとして自分自身を識別する BPDU を送信します。BPDU では、CIST ルートのパス コストおよび CIST リージョナル ルートへのパス コストの両方がゼロに設定されます。このデバイスはすべての MSTI も初期化し、そのすべてのルートであることを申告します。このデバイスは、ポートで現在保存されている情報よりも優位の MSTI ルート情報（低いスイッチ ID や低いパス コストなど）を受信すると、CIST リージョナル ルートとしての申告を放棄します。

初期化中に、MST リージョン内に独自の CIST リージョナル ルートを持つ多くのサブ リージョンが形成される場合があります。デバイスは、同一領域のネイバーから優位 IST 情報を受信すると、古いサブ領域を離れ本来の CIST リージョナル ルートを含む新しいサブ領域に加わります。このようにして、真の CIST リージョナル ルートが含まれているサブ リージョン以外のサブ領域はすべて縮小します。

MST 領域内のすべてのデバイスは、同一 CIST リージョナル ルートで合意する必要があります。領域内の任意の 2 つのデバイスは、共通 CIST リージョナル ルートに収束する場合、MSTI のポート ロールのみを同期化します。

MST 領域間のスパニングツリー動作

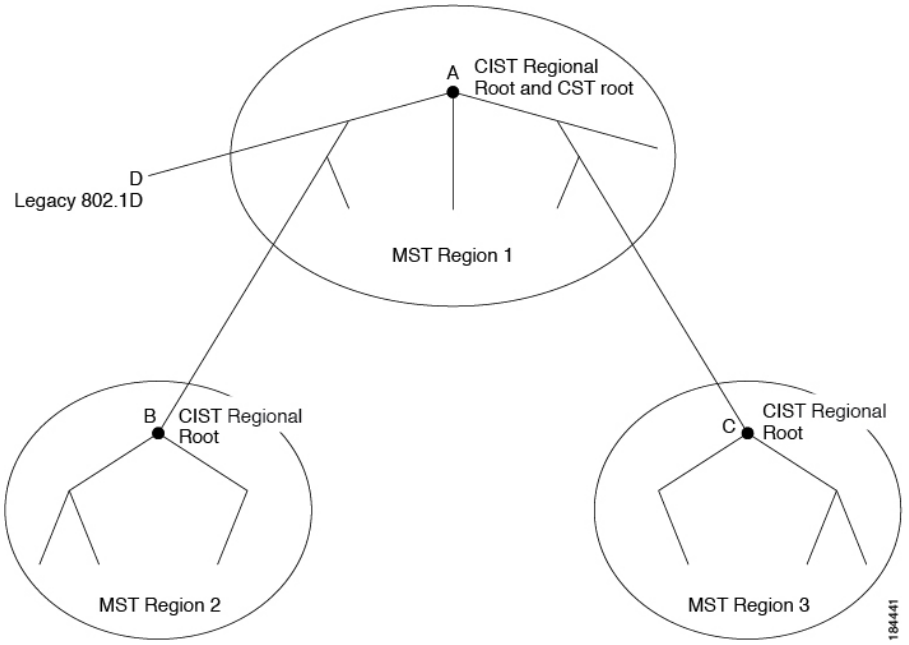
領域または 802.1w か 802.1D の STP インスタンスがネットワーク内に複数ある場合、MST は CST を確立して維持します。これには、ネットワークのすべての MST 領域およびすべての 802.1w と 802.1D の STP デバイスが含まれます。MSTI は、リージョンの境界で IST と結合して CST になります。

IST は領域内のすべての MST デバイスを接続し、スイッチド ドメイン全体を網羅する CIST でサブツリーのように見えます。サブツリーのルートは CIST リージョナル ルートです。隣接する STP デバイスおよび MST 領域には、MST 領域が仮想デバイスのように見えます。

***Figure 12: MST** リージョン、**CIST** リージョナル ルート、**CST** ルート*

次の図に、3 つの MST 領域と 1 台の 802.1D デバイス（D）を含むネットワークを示します。リージョン 1 の CIST リージョナル ルート（A）は、CIST ルートでもあります。リージョン 2

の CIST リージョナル ルート（B）、およびリージョン 3 の CIST リージョナル ルート（C）は、CIST 内のそれぞれのサブツリーのルートです。



BPDU を送受信するのは CST インスタンスのみです。MSTI は自身のスパニングツリー情報を BPDU に（M レコードとして）追加し、同じ MST 領域内のネイバー デバイスと相互作用して、最終的なスパニングツリートポロジを計算します。BPDUの送信に関連するスパニングツリー パラメータ（hello タイム、転送時間、最大エージング タイム、最大ホップ カウントなど）は、CST インスタンスにのみ設定されますが、すべての MSTI に影響します。スパニングツリー トポロジに関連するパラメータ（スイッチ プライオリティ、ポート VLAN コスト、ポート VLAN プライオリティなど）は、CST インスタンスと MSTI の両方に設定できます。

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

MST 用語

MST の命名規則には、内部パラメータまたはリージョナル パラメータの識別情報が含まれます。これらのパラメータは MST 領域内だけで使用され、ネットワーク全体で使用される外部パラメータと比較されます。CIST だけがネットワーク全体に広がるスパニングツリー インスタンスなので、CIST パラメータだけに外部修飾子が必要になり、修飾子またはリージョン修飾子は不要です。MST 用語を次に示します。

- CIST ルートは CIST のルート ブリッジで、ネットワーク全体にまたがる一意のインスタンスです。
- CIST 外部ルート パス コストは、CIST ルートまでのコストです。このコストは MST 領域内で変化しません。CIST には、MST 領域が単一のデバイスのように見えます。CIST 外部ルート パス コストは、この仮想デバイス、およびどの領域にも属さないデバイスの間で計算されるルート パス コストです。

- CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。CIST ルートが領域内にない場合、CIST リージョナル ルートは領域内の CIST ルートに最も近いデバイスです。CIST リージョナル ルートは、IST のルート ブリッジとして動作します。
- CIST 内部ルート パス コストは、領域内の CIST リージョナル ルートまでのコストです。このコストは、IST つまりインスタンス 0 だけに関連します。

ホップ カウント

MST リージョン内の STP トポロジを計算する場合、MST はコンフィギュレーション BPDU のメッセージ有効期間と最大エージング タイムの情報は使用しません。代わりに、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 メカニズムを使用します。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用すると、領域内の最大ホップ数を設定し、IST およびその領域のすべての MSTI に適用できます。

ホップ カウントは、メッセージ エージ情報と同じ結果になります（再設定を開始）。インスタンスのルート ブリッジは、コストが 0 でホップ カウントが最大値に設定された BPDU（M レコード）を常に送信します。デバイスは、この BPDU を受信すると、受信した残存ホップ カウントから 1 を差し引き、生成する BPDU の残存ホップ カウントとしてこの値を伝播します。カウントがゼロに達すると、デバイスは BPDU を廃棄し、ポート用に維持されている情報をエージングします。

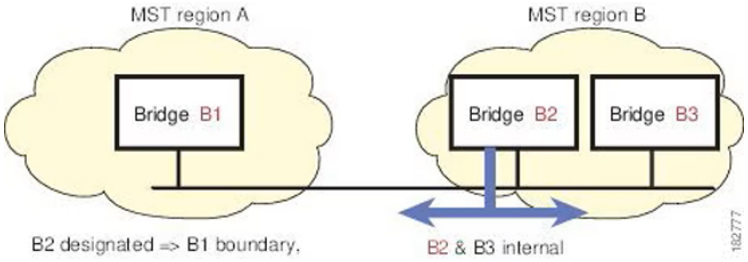
BPDU の 802.1w 部分に格納されているメッセージ有効期間および最大エージング タイムの情報は、領域全体で同じです（IST の場合のみ）。同じ値が、境界にある領域の指定ポートによって伝播されます。

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

境界ポート

境界ポートは、LAN に接続されたポートで、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。

Figure 13: 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。

単方向リンク障害の検出：MST

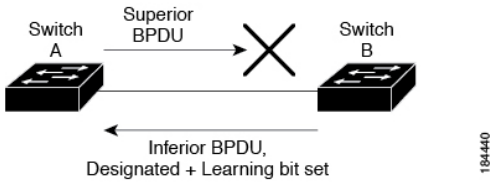
現在、IEEE MST 標準に単方向リンク障害の検出機能はありませんが、標準に準拠した実装には組み込まれています。この機能のベースとなるのは、異議メカニズムです。ソフトウェアは、受信した BPDU でポートのロールおよびステートの一貫性をチェックし、ブリッジング ループの原因となることがある単方向リンク障害を検出します。この機能は、異議メカニズムに基づいています。

Note 単方向リンク検出（UDLD）の詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

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

Figure 14: 単一方向リンク障害の検出

次の図に、ブリッジング ループの一般的な原因となる単方向リンク障害を示します。スイッチ A はルート ブリッジであり、スイッチ B へのリンクで BPDU は失われます。Rapid PVST+ (802.1w)および MST BPDU には、送信側ポートの役割と状態が含まれます。この情報により、スイッチ B は送信される上位 BPDU に対して反応せず、スイッチ B はルート ポートではなく指定ポートであることが、スイッチ A によって検出できます。この結果、スイッチ A は、そのポートをブロックし（またはブロックし続け）、ブリッジング ループが防止されます。



ポート コストとポート プライオリティ

スパニングツリーはポートコストを使用して、指定ポートを決定します。値が低いほど、ポート コストは小さくなります。スパニングツリーでは、最小のコスト パスが選択されます。デフォルト ポート コストは、次のように、インターフェイス帯域幅から取得されます。

- 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
- 40 ギガビット イーサネット：500

ポート コストを設定すると、選択されるポートが影響を受けます。

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

コストが同じポートを差別化するために、ポートプライオリティが使用されます。値が小さいほど、プライオリティが高いことを示します。デフォルトのポートの優先順位は 128 です。プライオリティは、0 ～ 224 の間の値に、32 ずつ増やして設定できます。

IEEE 802.1D との相互運用性

MST を実行するデバイスでは組み込みプロトコル移行機能がサポートされ、802.1D STP デバイスとの相互運用が可能になります。このデバイスで 802.1D コンフィギュレーション BPDU（プロトコル バージョンが 0 に設定されている BPDU）を受信する場合、そのポート上の 802.1D BPDU のみが送信されます。また、MST デバイスは、802.1D BPDU、別の領域に関連する MST BPDU（バージョン 3）、802.1w BPDU（バージョン 2）のうちいずれかを受信すると、ポートが領域の境界にあることを検出できます。

ただし、このデバイスは、802.1D BPDU を受信しなくなっても、MST モードに自動的に戻りません。802.1D デバイスが指定デバイスでない場合、802.1D デバイスがリンクから削除されたかどうかを検出できないからです。このデバイスの接続先デバイスが領域に加わったとき、デバイスは境界ロールをポートに割り当て続けることもあります。

プロトコル移行プロセスを再開する（強制的に隣接デバイスと再ネゴシエーションさせる）には、**clear spanning-tree detected-protocols** コマンドを入力します。

リンク上にあるすべての Rapid PVST+ スイッチ（およびすべての 8021.D STP スイッチ）では、MST BPDU を 802.1w BPDU の場合と同様に処理できます。MST デバイスは、バージョン 0 設定とトポロジ変更通知（TCN）BPDU、またはバージョン 3 MST BPDU のどちらかを境界ポートで送信できます。境界ポートは LAN に接続します。つまり、単一スパニングツリー デバイスまたは MST 設定が異なるデバイスのいずれかである指定デバイスに接続します。

MST は、MST ポート上で先行標準 MSTP を受信するたびに、シスコの先行標準 MSTP と相互に動作します。明示的な設定は必要ありません。

また、インターフェイスを設定して、先行標準の MSTP メッセージを事前に送信することもできます。

MST のハイ アベイラビリティ

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

デバイスは、MSTに対して中断のない完全アップグレードをサポートします。中断のないアップグレードとハイ アベイラビリティ機能の詳細については、『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

MST の前提条件

MST には次の前提条件があります。

- デバイスにログインしていること。

MST の設定に関するガイドラインおよび制約事項

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

MST 設定時のガイドラインと制約事項は次のとおりです。

- MST 設定制限については、『*Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*』を参照してください。
- **show** コマンド（**internal** キーワード付き ）はサポートされていません。
- MST をイネーブルにする必要があります。Rapid PVST+ は、デフォルトのスパニングツリー モードです。
- 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。
- VLAN 3968 ～ 4095 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。
- 1 つのデバイスに最大 65 個の MST インスタンスを設定できます。
- デフォルトでは、すべての VLAN が MSTI 0（IST）にマッピングされます。
- ロード バランスは、MST 領域の内部でのみ実行できます。
- MSTI にマッピングされたすべての VLAN が、トランクによって伝送されているか、または伝送から除外されていることを確認します。
- STP は常にイネーブルのままにしておきます。

- タイマーは変更しないでください。ネットワークの安定性が低下することがあります。
- ユーザ トラフィックを管理 VLAN から切り離し、管理 VLAN をユーザ データから分離します。
- プライマリおよびセカンダリ ルート スイッチの場所として、ディストリビューション レイヤおよびコア レイヤを選択します。
- ポート チャネリング：ポート チャネル バンドルは、単一ポートと見なされます。ポート コストは、そのチャネルに割り当てられている設定済みのすべてのポート コストの合計です。
- VLAN を MSTI にマッピングすると、この VLAN が以前の MSTI から自動的に削除されます。
- 1 つの MSTI に任意の個数の VLAN をマッピングできます。
- Rapid PVST+ と MST クラウド、または PVST+ と MST クラウドとの間でロード バランシングを実現するには、すべての MST 境界ポートがフォワーディング ステートでなければなりません。MST クラウドの CIST リージョナル ルートが CST のルートでなければなりません。MST クラウドが複数の MST 領域で構成されている場合、MST 領域の 1 つに CST ルートが含まれていなければならず、その他のすべての MST 領域では MST クラウド内に含まれるルートへのパスが、Rapid PVST+ または PVST+ クラウドよりも良好なものでなければなりません。
- ネットワークを多数の領域に分割しないでください。ただしこの状況を避けられない場合は、レイヤ 2 デバイスによって相互接続された、より小さい LAN にスイッチド LAN を分割することを推奨します。
- MST 設定サブモードの場合、次の注意事項が適用されます。
  - 各コマンド参照行により、保留中のリージョン設定が作成されます。
  - 保留中のリージョン設定により、現在のリージョン設定が開始されます。
  - 変更をコミットすることなく MST コンフィギュレーション サブモードを終了するには、**abort** コマンドを入力します。
  - MST コンフィギュレーション サブモードを終了し、サブモードを終了する前に行ったすべての変更をコミットするには、**exit** または **end** コマンドを入力するか、または **Ctrl + Z** キーを押します。

（注） このソフトウェアは、MST に対して中断のない完全アップグレードをサポートします。

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。

Table 12: 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	有効（Enabled）
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 **Caution** 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
改定	0
[インスタンス ID（Instance ID）]	インスタンス 0。VLAN 1 ～ 3967 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。 • 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 • 40 ギガビット イーサネット：500
hello タイム	2 秒
転送遅延時間	15 秒

パラメータ	デフォルト
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

MST の設定

Note Cisco IOS の CLI に慣れている場合、この機能のシスコ ソフトウェア コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

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。

Note 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。

SUMMARY STEPS

1. **config t**
2. **spanning-tree mode mst** または **no spanning-tree mode mst**.
3. **exit**
4. (Optional) **show running-config spanning-tree all**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mode mst** または **no spanning-tree mode mst**. **Example:** `switch(config)# spanning-tree mode mst`	• **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。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show running-config spanning-tree all** **Example:** `switch# show running-config spanning-tree all`	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	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

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。

Note 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。さらに、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。

SUMMARY STEPS

1. **config t**
2. **spanning-tree mst configuration** または **no spanning-tree mst configuration**
3. **exit** または **abort**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst configuration** または **no spanning-tree mst configuration**
	Example:
	`switch(config)# spanning-tree mst configuration`
	`switch(config-mst)#`
		• **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/MSTI マッピング
		• MST リビジョン番号
		• **no spanning-tree mst configuration**
		MST リージョン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。

ステップ 3	**exit** または **abort**	• **exit**

	Command or Action	Purpose

	Example:
	`switch(config-mst)# exit`
	`switch(config)#`
		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。

ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

次に、デバイスでMSTコンフィギュレーション サブモードを開始する例を示します。

```
switch# config t
switch(config)# spanning-tree mst configuration
switch(config-mst)# exit
switch(config)#
```

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。

SUMMARY STEPS

1. **config t**
2. **spanning-tree mst configuration**
3. **name** *name*
4. **exit** または **abort**
5. (Optional) **show spanning-tree mst configuration**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	Command or Action	Purpose

ステップ 2	**spanning-tree mst configuration**
	Example:
	`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	**name** *name* **Example:** `switch(config-mst)# name accounting`	MST 領域の名前を指定します。*name* 文字列の最大の長さは 32 文字であり、大文字と小文字が区別されます。デフォルトは空の文字列です。

ステップ 4	**exit** または **abort**
	Example:
	`switch(config-mst)# exit`
	`switch(config)#`
		• **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。

ステップ 5	(Optional) **show spanning-tree mst configuration** **Example:** `switch# show spanning-tree mst configuration`	MST の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

次の例は、MST リージョンの名前の設定方法を示しています。

```
switch# config t
switch(config)#  spanning-tree mst configuration
switch(config-mst)# name accounting
switch(config-mst)# exit
switch(config)#
```

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。

SUMMARY STEPS

1. **config t**
2. **spanning-tree mst configuration**

3. **revision** *version*
4. **exit** または **abort**
5. (Optional) **show spanning-tree mst configuration**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst configuration**
	Example:
	`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* **Example:** `switch(config-mst)# revision 5`	MST リージョン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	**exit** または **abort**
	Example:
	`switch(config-mst)# exit`
	`switch(config)#`
		• **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。

ステップ 5	(Optional) **show spanning-tree mst configuration** **Example:** `switch# show spanning-tree mst configuration`	MST の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

次に、MSTI 領域のリビジョン番号を 5 に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst configuration
switch(config-mst)# revision 5
switch(config-mst)#
```

MST リージョンでの設定の指定

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 つのメンバまたは複数のメンバを存在させることができます。各メンバでは、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 リージョンには、数の制限はありませんが、各リージョンでは、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。

SUMMARY STEPS

1. **config t**
2. **spanning-tree mst configuration**
3. **instance** *instance-id* **vlan** *vlan-range*
4. **name** *name*
5. **revision** *version*
6. **exit** または **abort**
7. **show spanning-tree mst configuration**
8. **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst configuration**
	Example:
	`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* **Example:** `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。

	Command or Action	Purpose
		• **vlan** の場合 *vlan-range* の範囲は 1 ～ 3967 です。VLAN を MSTI にマップする場合、マッピングは増加され、コマンドに指定した VLAN は、以前マッピングした VLAN に追加されるか、そこから削除されます。 VLAN 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* **Example:** `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* **Example:** `switch(config-mst)# revision 1`	設定リビジョン番号を指定します。範囲は 0 ～ 65535 です。

ステップ 6	**exit** または **abort**
	Example:
	`switch(config-mst)# exit`
	`switch(config)#`
		• **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。

ステップ 7	**show spanning-tree mst configuration** **Example:** `switch# show spanning-tree mst configuration`	（任意）MST 設定を表示します。
ステップ 8	**copy running-config startup-config** **Example:** `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。

Example

次の例は、MST コンフィギュレーション モードを開始し、VLAN 10 ～ 20 を MSTI 1 にマッピングし、リージョンに *region1* という名前を付けて、設定リビジョンを 1 に設

定し、保留中の設定を表示し、変更を適用してグローバル コンフィギュレーション モードに戻る方法を示しています。

```
switch# config t
switch(config)# spanning-tree mst configuration
switch(config-mst)# instance 1 vlan 10-20
switch(config-mst)# name region1
switch(config-mst)# revision 1
switch(config-mst#) exit
switch(config)# show spanning-tree mst configuration

Name      [region1]
Revision  1
Instances configured 2
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------
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 ～ 4095 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。

Note 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。

Note MSTI はディセーブルにできません。

SUMMARY STEPS

1. **config t**
2. **spanning-tree mst configuration**
3. **instance** *instance-id* **vlan** *vlan-range* or **no instance** *instance-id* **vlan** *vlan-range*
4. **exit** または **abort**
5. (Optional) **show spanning-tree mst configuration**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst configuration**
	Example:
	`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* or **no instance** *instance-id* **vlan** *vlan-range* **Example:** `switch(config-mst)# instance 3 vlan 200`	• **instance** *instance-id* **vlan** *vlan-range* 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 リージョンでの IST 用に予約されています。 • *vlan-range* の範囲は 1 ～ 3967 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。 • **no instance** *instance-id* **vlan** *vlan-range* 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。

ステップ 4	**exit** または **abort**
	Example:
	`switch(config-mst)# exit`
	`switch(config)#`
		• **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。

ステップ 5	(Optional) **show spanning-tree mst configuration** **Example:** `switch# show spanning-tree mst configuration`	MST の設定を表示します。

	Command or Action	Purpose
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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)# exit
switch(config)#
```

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。

spanning-tree vlan *vlan_ID* **primary root** 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、このコマンドは機能しません。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.
```

Note 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。

diameterを入力します 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 台の端末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** キーワードを使用して、自動的に計算される hello タイムをオーバーライドできます。

Note ルート ブリッジとして設定されたデバイスで、以下のコマンドを使用して、hello タイム、転送遅延時間、最大エージング タイムを手動で設定しないでください。**spanning-tree mst hello-timespanning-tree mst forward-time**、および **spanning-tree mst max-age** グローバル コンフィギュレーション コマンド。

SUMMARY STEPS

1. **config t**
2. **spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]] or **no spanning-tree mst** *instance-id* **root**
3. **exit** または **abort**
4. (Optional) **show spanning-tree mst**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]] or **no spanning-tree mst** *instance-id* **root** **Example:** `switch(config)# spanning-tree mst 5 root primary`	• **spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]] 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。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、MSTI インスタンス 0 の場合にのみ使用できます。 • **hello-time** には *seconds* には、ルート ブリッジが設定メッセージを生成するインターバルを秒単位で指定します。有効範囲は 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。
ステップ 3	**exit** または **abort** **Example:**	• **exit**

	Command or Action	Purpose
	`switch(config)# exit` `switch#`	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。
ステップ 4	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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)# exit
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。

SUMMARY STEPS

1. **config t**
2. **spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia*[**hello-time** *hello-time*]] or **no spanning-tree mst** *instance-id* **root**
3. **exit**
4. (Optional) **show spanning-tree mst**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia*[**hello-time** *hello-time*]] or **no spanning-tree mst** *instance-id* **root** **Example:** `switch(config)# spanning-tree mst 5 root secondary`	• **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。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、MSTI インスタンス 0 の場合にのみ使用できます。 • **hello-time** には *seconds* には、ルート ブリッジが設定メッセージを生成するインターバルを秒単位で指定します。有効範囲は 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。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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)# exit
switch#
```

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。

Note **spanning-tree mst priority** コマンドを使用するときは注意してください。 コマンドを使用します。ほとんどの場合、**spanning-tree mst root primary**を入力することを推奨します。 および **spanning-tree mst root secondary** スイッチ プライオリティを変更するためにグローバル設定コマンドを使用します。

SUMMARY STEPS

1. **config t**
2. **spanning-tree mst** *instance-id* **priority** *priority-value*
3. **exit**
4. (Optional) **show spanning-tree mst**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	Command or Action	Purpose
ステップ 2	**spanning-tree mst** *instance-id* **priority** *priority-value* **Example:** `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。範囲は 1 ～ 4094 です。 • *priority-value* 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。 使用可能な値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。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**
	Example:
	`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	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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)# exit
switch#
```

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。

SUMMARY STEPS

1. **config t**
2. **interface** {{*type slot/port*} | {**port-channel** *number*}}
3. **spanning-tree mst** *instance-id* **port-priority** *priority*
4. **exit**
5. (Optional) **show spanning-tree mst**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** {{*type slot/port*} | {**port-channel** *number*}}
	Example:
	`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* **Example:** `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。範囲は 1 ～ 4094 です。 • *priority* の範囲は 0 ～ 224 で、32 ずつ増加します。デフォルト値は 128 です。値が小さいほど、プライオリティが高いことを示します。 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** **Example:**	インターフェイス モードを終了します。

	Command or Action	Purpose
	`switch(config-if)# exit` `switch(config)#`	
ステップ 5	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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。

Note MST はロング パスコスト計算方式を使用します。

SUMMARY STEPS

1. **config t**
2. **interface** {{*type slot/port*} | {**port-channel** *number*}}
3. **spanning-tree mst** *instance-id* **cost** {*cost* | *auto*}
4. **exit**
5. (Optional) **show spanning-tree mst**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** {{*type slot/port*} | {**port-channel** *number*}}
	Example:
	`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*} **Example:** `switch(config-if)# spanning-tree mst 4 cost 17031970`	コストを設定します。 ループが発生した場合、MST はパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。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。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。

ステップ 4	**exit**
	Example:
	`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	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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。

Note **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。

SUMMARY STEPS

1. **config t**
2. **spanning-tree mst hello-time** *seconds*
3. **exit**
4. (Optional) **show spanning-tree mst**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst hello-time** *seconds* **Example:** `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

	Command or Action	Purpose
		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**
	Example:
	`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	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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)# exit
switch#
```

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。

SUMMARY STEPS

1. **config t**
2. **spanning-tree mst forward-time** *seconds*
3. **exit**
4. (Optional) **show spanning-tree mst**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**config t** **Example:**	コンフィギュレーション モードに入ります。

	Command or Action	Purpose
	`switch# config t` `switch(config)#`	
ステップ 2	**spanning-tree mst forward-time** *seconds* **Example:** `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**
	Example:
	`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	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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)# exit
switch#
```

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。

SUMMARY STEPS

1. **config t**
2. **spanning-tree mst max-age** *seconds*
3. **exit**
4. (Optional) **show spanning-tree mst**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst max-age** *seconds* **Example:** `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。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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)# exit
switch#
```

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）。

SUMMARY STEPS

1. **config t**
2. **spanning-tree mst max-hops** *hop-count*
3. **exit**
4. (Optional) **show spanning-tree mst**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst max-hops** *hop-count* **Example:** `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**
	Example:
	`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	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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)# exit
switch#
```

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。インターフェイスを設定して、先行標準の MSTP メッセージを事前に送信できます。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。

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree mst pre-standard**
4. **exit**
5. (Optional) **show spanning-tree mst**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *type slot/port*
	Example:
	`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** **Example:** `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**
	Example:
	`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	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。

	Command or Action	Purpose
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**config t** **Example:**	コンフィギュレーション モードに入ります。

	Command or Action	Purpose
	`switch# config t` `switch(config)#`	

ステップ 2	**interface** *type slot/port*
	Example:
	`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*} **Example:** `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**
	Example:
	`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	(Optional) **show spanning-tree** **Example:** `switch# show spanning-tree`	STP の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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 または異なるリージョンに関連付けられている MST BPDU を受信するときに、ポートがリージョン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。

SUMMARY STEPS

1. **clear spanning-tree detected-protocol** [**interface** *interface* [*interface-num* | *port-channel*]]

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**clear spanning-tree detected-protocol** [**interface** *interface* [*interface-num* | *port-channel*]] **Example:** `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。

Example

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 の設定の確認

MST 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show running-config spanning-tree [**all**]	STP 情報を表示します。
show spanning-tree mst configuration	MST 情報を表示します。
show spanning-tree mst [**detail**]	MST インスタンスの情報を表示します。
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。

コマンド	目的
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。

MST 統計情報の表示およびクリア（CLI バージョン）

MST 設定情報を表示するには、次のいずれかの作業を実行します。

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。

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(config-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

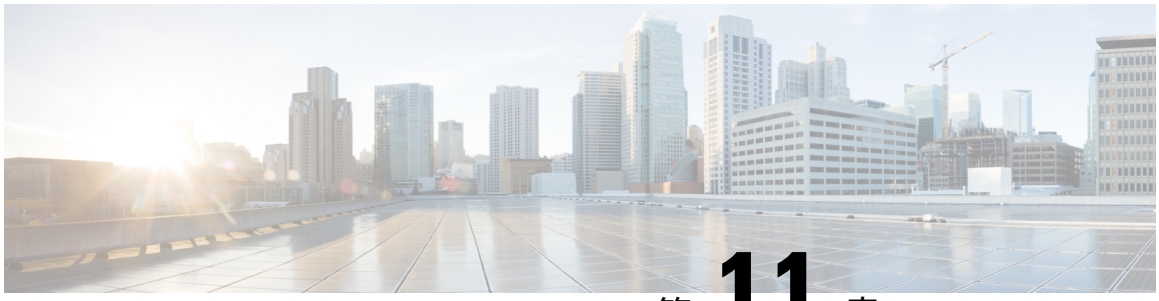
関連項目	マニュアル タイトル
レイヤ2インターフェイス	『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』
NX-OS の基礎	『*Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide*』
高可用性	『*Cisco Nexus 9000 Series High Availability and Redundancy Guide*』
システム管理	『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』

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。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.



第 11 章

Cisco NX-OS を使用した STP 拡張の設定

- STP 拡張機能について, on page 191
- STP 拡張機能の前提条件, on page 198
- STP 拡張機能の設定に関するガイドラインおよび制約事項 （198 ページ）
- STP 拡張機能のデフォルト設定, on page 200
- STP 拡張機能の設定手順, on page 200
- STP 拡張機能の設定の確認, on page 221
- STP 拡張機能の設定例, on page 221
- STP 拡張機能の追加情報（CLI バージョン）, on page 222

STP 拡張機能について

Note レイヤ 2 インターフェイスの作成の詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

ループ回避を改善し、ユーザによる設定ミスを削減し、プロトコルパラメータの制御を向上するために、シスコは STP に拡張機能を追加しました。IEEE 802.1w 高速スパニングツリー プロトコル（RSTP）規格に同様の機能が統合されていることも考えられますが、ここで紹介する拡張機能を使用することを推奨します。PVST シミュレーションを除き、これらの拡張機能はすべて、Rapid PVST+ および MST の両方で使用できます。PVST シミュレーションを使用できるのは、MST だけです。

使用できる拡張機能は、スパニングツリー エッジ ポート（従来の PortFast の機能を提供）、ブリッジ保証、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 PVT シミュレーションです。これらの機能の大部分は、グローバルに、または指定インターフェイスに適用できます。

Note このマニュアルでは、IEEE 802.1w および IEEE 802.1s を指す用語として、「スパニングツリー」を使用します。IEEE 802.1D STP について説明している箇所では、802.1D と明記します。

STP ポート タイプ

スパニングツリー ポートは、エッジ ポート、ネットワーク ポート、または標準ポートとして構成できます。ポートは、ある一時点において、これらのうちいずれか 1 つの状態をとります。デフォルトのスパニング ツリー ポート タイプは「標準」です。

レイヤ 2 ホストに接続するエッジ ポートは、アクセス ポートまたはトランク ポートのどちらかになります。

Note レイヤ2スイッチまたはブリッジに接続しているポートをエッジポートとして設定すると、ブリッジング ループが発生することがあります。

ネットワーク ポートは、レイヤ 2 スイッチまたはブリッジだけに接続します。

Note レイヤ 2 ホストまたはエッジ デバイスに接続されたポートを、誤ってスパニングツリー ネットワーク ポートとして設定した場合、これらのポートは自動的にブロッキング ステートに移行します。

STP エッジ ポート

STPエッジポートは、レイヤ2ホストだけに接続します。エッジポート インターフェイスは、ブロッキング ステートやラーニング 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（この直接移行動作は、以前は、シスコ独自の機能 PortFast として設定していました）。

レイヤ 2 ホストに接続したインターフェイスでは、STP のブリッジ プロトコル データ ユニット（BPDU）を受信しないようにします。

Bridge Assurance

Bridge Assurance を使用すると、ネットワーク内でブリッジング ループの原因となる問題の発生を防ぐことができます。具体的には、Bridge Assurance を使用して、単方向リンク障害または他のソフトウェア障害、およびスパニングツリーアルゴリズムの停止後もデータ トラフィックを転送し続けているデバイスから、ネットワークを保護します。

Note Bridge Assurance は、Rapid PVST+ および MST だけでサポートされています。

Bridge Assurance は通常リンクでの作動に 2 秒、VPC ピアリンクでは 84 秒以下かかります。

Bridge Assurance はデフォルトでイネーブルになっており、グローバル単位でだけディセーブルにできます。また、Bridge Assurance をイネーブルにできるのは、ポイントツーポイント リンクに接続されたスパニングツリー ネットワーク ポートだけです。Bridge Assurance は必ず、

リンクの両端でイネーブルにする必要があります。リンクの一端のデバイスでBridge Assuranceがイネーブルであっても、他端のデバイスが Bridge Assurance をサポートしていない、または Bridge Assurance がイネーブルではない場合、接続ポートはブロックされます。

Bridge Assurance をイネーブルにすると、BPDU が hello タイムごとに、動作中のすべてのネットワーク ポート（代替ポートとバックアップ ポートを含む）に送出されます。所定の期間 BPDU を受信しないポートは、ブロッキング ステートに移行し、ルート ポートの決定に使用されなくなります。BPDU を再度受信するようになると、そのポートで通常のスパニングツリー状態遷移が再開されます。

Figure 15: 標準的な ***STP*** トポロジのネットワーク

次の図は、標準的な STP トポロジを示しています。

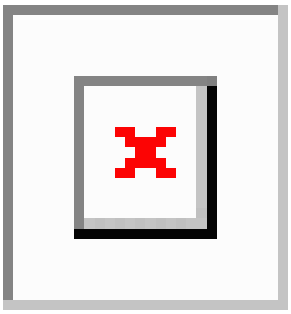


Figure 16: Bridge Assurance を実行していないネットワークの問題

次の図は、Bridge Assurance を実行していない場合、デバイスの障害発生時にネットワークで発生する可能性のある問題を示しています。

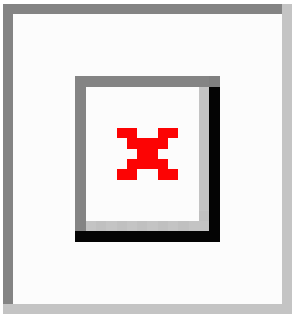


Figure 17: Bridge Assurance を実行しているネットワークの ***STP*** トポロジ

次の図は、Bridge Assurance がイネーブルになっているネットワークで、すべての STP ネットワーク ポートから双方向 BPDU が発行される一般的な STP トポロジを示しています。

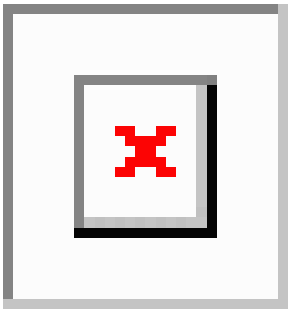
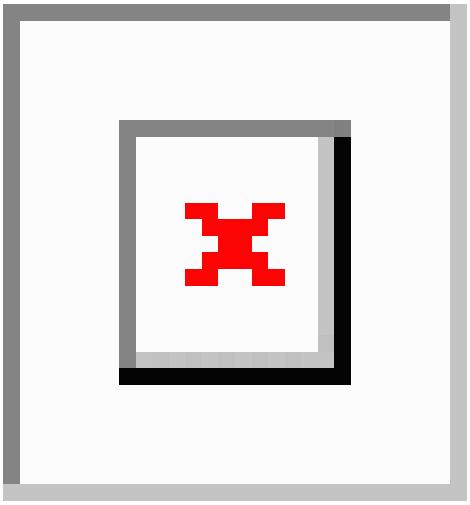


Figure 18: Bridge Assurance によるネットワーク上の問題の回避

次の図は、ネットワーク上で Bridge Assurance をイネーブルにした場合に、ネットワーク上の問題が発生しない理由を示しています。



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2LAN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。

Note 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。

Caution 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。

***Table 13: 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]	有効	有効	イネーブル [2]
デフォルト	有効	無効	無効
デフォルト	無効	N/A	無効
無効	N/A	N/A	無効
有効	N/A	N/A	有効

1 明示的なポート設定はありません。
2 ポートは最低 10 個の 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。

ループ ガード

ループ ガードを使用すると、ポイントツーポイント リンク上の単方向リンク障害によって発生することがあるブリッジング ループを防止できます。

STPループは、冗長なトポロジにおいてブロッキング ポートが誤ってフォワーディング ステートに移行すると発生します。通常、BPDU の受信を停止する、物理的に冗長なトポロジ内のポート（ブロッキング ポートとは限らない）が原因で移行が発生します。

ループ ガードをグローバルにイネーブルにしても、デバイスがポイントツーポイント リンクで接続されているスイッチド ネットワークでしか使用できません。ポイントツーポイント リンクでは、下位BPDUを送信するか、リンクをダウンしない限り、代表ブリッジは消えることはありません。ただし、共有リンク上のループ ガードはインターフェイス単位でイネーブルに設定できます。

ループ ガードを使用して、ルート ポートまたは代替/バックアップ ループ ポートが BPDU を受信するかどうかを確認できます。BPDUを受信していたポートでBPDUが受信されなくなると、ループ ガードは、ポート上で BPDU の受信が再開されるまで、そのポートを不整合（ブロッキング）ステートにします。これらのポートでBPDUの受信が再開されると、ポートおよびリンクは再び動作可能として認識されます。この回復は自動的に実行されるので、プロトコルによりポートからループ不整合が排除されると、STP によりポート ステートが判別されます。

ループ ガードは障害を分離し、STPは障害のあるリンクやブリッジを含まない安定したトポロジに収束できます。ループ ガードをディセーブルにすると、すべてのループ不整合ポートはリスニング ステートに移行します

ループ ガードはポート単位でイネーブルにできます。ループ ガードを特定のポートでイネーブルにすると、そのポートが属するすべてのアクティブ インスタンスまたは VLAN にループ ガードが自動的に適用されます。ループ ガードをディセーブルにすると、指定ポートでディセーブルになります。

ルート デバイス上でループ ガードをイネーブルにしても効果はありませんが、ルート デバイスが非ルート デバイスになった場合、保護が有効になります。

ルート ガード

特定のポートでルート ガードをイネーブルにすると、そのポートはルート ポートになることが禁じられます。受信した BPDU によって STP コンバージェンスが実行され、指定ポートがルート ポートになると、そのポートはルート不整合（ブロッキング）状態になります。このポートが優位 BPDU の受信を停止すると、ブロッキングが再度解除されます。次に、STP によって、フォワーディング ステートに移行します。リカバリは自動的に行われます。

インターフェイス上でルートガードをイネーブルにすると、そのインターフェイスが属しているすべての VLAN にルート ガードが適用されます。

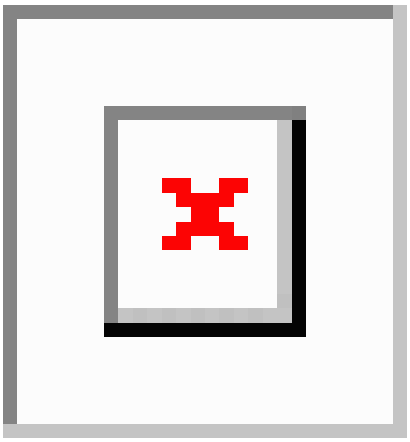
ルートガードを使用すると、ネットワーク内にルートブリッジを強制的に配置できます。ルート ガードは、ルート ガードがイネーブルにされたポートを指定ポートに選出します。通常、ルート ブリッジのポートはすべて指定ポートとなります（ただし、ルート ブリッジの 2 つ以上のポートが接続されている場合はその限りではありません）。ルート ブリッジは、ルートガードがイネーブルにされたポートで上位 BPDU を受信すると、そのポートをルート不整合 STP 状態に移行します。このように、ルートガードはルートブリッジの配置を適用します。

ルート ガードをグローバルには設定できません。

STP 拡張機能の適用

Figure 19: STP 拡張機能を適正に展開したネットワーク

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。



PVST シミュレーション

MST は、ユーザが設定しなくても、Rapid PVST+ と相互運用できます。この相互運用性を提供するのが、PVST シミュレーション機能です。

Note MST をイネーブルにすると、PVST シミュレーションがデフォルトでイネーブルになります。デフォルトでは、デバイス上のすべてのインターフェイスで MST と Rapid PVST+ が相互運用されます。

ただし、MST イネーブル ポートが Rapid PVST+ イネーブル ポートに接続される可能性を防ぐには、MST と Rapid PVST+ 間の接続を制御する必要があります。Rapid PVST+ はデフォルトの STP モードなので、多数の Rapid PVST+ 接続が発生することがあります。

Rapid PVST+ シミュレーションを、ポート単位でディセーブルにするか、デバイス全体でグローバルにディセーブルにすると、MST イネーブル ポートは、Rapid PVST+ イネーブル ポートに接続したことが検出された時点で、ブロッキング ステートに移行します。このポートは、Rapid PVST+/SSTP BPDU の受信が停止されるまで不整合のステートのままになります。そしてポートは、通常の STP 送信プロセスに戻ります。

すべての STP インスタンスのルート ブリッジは、MST または Rapid PVST+ のどちらかの側に属している必要があります。すべての STP インスタンスのルート ブリッジがどちらか一方の側に属していないと、ポートは PVST シミュレーション不整合ステートになります。

Note すべての STP インスタンスのルート ブリッジを、MST 側に配置することを推奨します。

STP のハイ アベイラビリティ

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

Note ハイ アベイラビリティ機能、の詳細については、『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide* 』を参照してください。

STP 拡張機能の前提条件

STP 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。
- STP を設定しておく必要があります。

STP 拡張機能の設定に関するガイドラインおよび制約事項

STP 拡張機能の設定に関するガイドラインと制約事項は次のとおりです。

- **show** コマンド（**internal** キーワード付き）はサポートされていません。
- STP ネットワーク ポートは、スイッチだけに接続してください。
- ホスト ポートは、ネットワーク ポートではなく STP エッジ ポートとして設定する必要があります。
- STP ネットワーク ポート タイプをグローバルにイネーブルにする場合には、ホストに接続しているすべてのポートを手動で STP エッジ ポートとして設定してください。
- レイヤ 2 ホストに接続しているすべてのアクセス ポートおよびトランク ポートを、エッジ ポートとして設定する必要があります。
- Bridge Assurance は、ポイントツーポイントのスパニングツリー ネットワーク ポート上だけで実行されます。この機能は、リンクの両端で設定する必要があります。
- Bridge Assurance は、ネットワーク全体でイネーブルにすることを推奨します。

- すべてのエッジ ポートで BPDU ガードをイネーブルにすることを推奨します。
- グローバルにイネーブルにしたループ ガードは、ポイントツーポイント リンク上でのみ動作します。
- インターフェイス単位でイネーブルにしたループ ガードは、共有リンクおよびポイントツーポイント リンクの両方で動作します。
- ルート ガードを適用したポートは強制的に指定ポートになりますが、ルート ポートにはなりません。ループ ガードは、ポートがルート ポートまたは代替ポートの場合にのみ有効です。ポート上でループ ガードとルート ガードの両方を同時にイネーブルにすることはできません。
- ディセーブル化されたスパニングツリー インスタンスまたは VLAN 上では、ループ ガードは無効です。
- スパニングツリーは、BPDUを送信するチャネル内で最初に動作するポートを常に選択します。このリンクが単方向になると、チャネル内の他のリンクが正常に動作していても、ループ ガードによりチャネルがブロックされます。
- ループ ガードによってブロックされている一連のポートをグループ化してチャネルを形成すると、これらのポートのステート情報はスパニングツリーからすべて削除され、新しいチャネルのポートは指定ロールによりフォワーディング ステートに移行できます。
- チャネルがループ ガードによりブロックされ、チャネルのメンバーが個々のリンク ステータスに戻ると、スパニングツリーからすべてのステート情報が削除されます。チャネルを形成する1つまたは複数のリンクが単一方向リンクである場合も、各物理ポートは指定されたロールを使用して、フォワーディング ステートに移行できます。

（注） 単方向リンク検出（UDLD）アグレッシブ モードをイネーブルにすると、リンク障害を分離できます。UDLD により障害が検出されるまではループが発生することがありますが、ループ ガードでは検出できません。UDLD の詳細については、『*Cisco NX-OS Series NX-OS Interfaces Configuration Guide*』を参照してください。

- 物理ループのあるスイッチ ネットワーク上では、ループ ガードをグローバルにイネーブルにする必要があります。
- 直接の管理制御下にないネットワーク デバイスに接続しているポート上では、ルート ガードをイネーブルにする必要があります。

STP 拡張機能のデフォルト設定

次の表に、STP 拡張機能のデフォルト設定を示します。

Table 14: 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
PVST シミュレーション	有効（Enabled）

STP 拡張機能の設定手順

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

ループ ガードは、共有リンクまたはポイントツーポイント リンク上のインターフェイス単位でイネーブルに設定できます。

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。

Before you begin

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。

- 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。

SUMMARY STEPS

1. **config t**
2. **spanning-tree port type edge default** or **spanning-tree port type network default**
3. **exit**
4. (Optional) **show spanning-tree summary**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree port type edge default** or **spanning-tree port type network default** **Example:** `switch(config)# spanning-tree port type edge default`	• **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

	Command or Action	Purpose
		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。 **Note** レイヤ 2 ホストに接続しているインターフェイスをネットワーク ポートとして設定すると、これらのポートは自動的にブロッキング ステートに移行します。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show spanning-tree summary** **Example:** `switch# show spanning-tree summary`	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	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

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)# exit
switch#
```

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 ポートで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 ポートでのエッジ動作を明示的にイネーブルにします。

Note **spanning-tree port type edge trunk** を入力すると、 コマンド、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。

Before you begin

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。

- 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。

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree port type edge**
4. **exit**
5. (Optional) **show spanning-tree interface** *type slot/port* **ethernet** *x/y*
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *type slot/port*
	Example:
	`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** **Example:** `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**
	Example:
	`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	(Optional) **show spanning-tree interface** *type slot/port* **ethernet** *x/y* **Example:** `switch# show spanning-tree ethernet 1/4`	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	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

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**: このコマンドはネットワーク ポートとしてポートを明示的に設定します。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、Bridge Assurance はこのインターフェイスで実行できません。
- **no spanning-tree port type**：このコマンドは、**spanning-tree port type network default** を定義した場合に、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。 コマンドを使用します。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。

Note 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。

Before you begin

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。

- 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。

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree port type network**
4. **exit**
5. (Optional) **show spanning-tree interface** *type slot/port*
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *type slot/port*
	Example:
	`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** **Example:** `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**
	Example:
	`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	(Optional) **show spanning-tree interface** *type slot/port* **Example:** `switch# show spanning-tree interface ethernet 1/4`	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	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

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。

Note 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。

Before you begin

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。

- 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。

SUMMARY STEPS

1. **config t**
2. **spanning-tree port type edge bpduguard default**
3. **exit**
4. (Optional) **show spanning-tree summary**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree port type edge bpduguard default** **Example:** `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。 **Note** このコマンドは、インターフェイス レベルで動作を変更しますが、show running interface では表示されません。クリア操作のステータスを確認するには、**show spanning-tree summary** コマンドを使用します。

	Command or Action	Purpose

ステップ 3	**exit**
	Example:
	`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	(Optional) **show spanning-tree summary** **Example:** `switch# show spanning-tree summary`	STP の概要を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

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(config)# 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** : インターフェイス上で、BPDU ガードが無条件にイネーブルになります。
- **spanning-tree bpduguard disable** : インターフェイス上で、BPDU ガードが無条件にディセーブルになります。
- **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。

Before you begin

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree bpduguard** {**enable** | **disable**} or **no spanning-tree bpduguard**
4. **exit**
5. (Optional) **show spanning-tree interface** *type slot/port* **detail**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

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

ステップ 3	**spanning-tree bpduguard** {**enable** | **disable**} or **no spanning-tree bpduguard** **Example:** `switch(config-if)# spanning-tree bpduguard enable`	• **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。

ステップ 4	**exit**
	Example:
	`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	(Optional) **show spanning-tree interface** *type slot/port* **detail** **Example:**	STP の概要を表示します。

	Command or Action	Purpose
	`switch# show spanning-tree interface ethernet detail`	
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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。

Caution このコマンドを使用するときは注意してください。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。

Before you begin

この機能を設定する前に、次の点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。

Note 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 ポートにだけ適用されます。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。

SUMMARY STEPS

1. **config t**
2. **spanning-tree port type edge bpdufilter default**
3. **exit**
4. (Optional) **show spanning-tree summary**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree port type edge bpdufilter default** **Example:** `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**
	Example:
	`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	(Optional) **show spanning-tree summary** **Example:** `switch# show spanning-tree summary`	STP の概要を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

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。

Caution **spanning-tree bpdufilter enable** を入力する場合は、慎重に行ってください。 指定されたインターフェイスでコマンドを入力します。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 フィルタ処理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 フィルタ処理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。コマンドを使用します。

Before you begin

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。

Note 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。

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. {|}または **spanning-tree bpdufilter enable disable no spanning-tree bpdufilter**
4. **exit**
5. (Optional) **show spanning-tree summary**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *type slot/port*
	Example:
	`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	{| }または **spanning-tree bpdufilter enable disable no spanning-tree bpdufilter** **Example:** `switch(config-if)# spanning-tree bpdufilter enable`	• **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。

ステップ 4	**exit**
	Example:
	`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	(Optional) **show spanning-tree summary** **Example:** `switch# show spanning-tree summary`	STP の概要を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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。

Note 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。

Before you begin

この機能を設定する前に、次の点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。

SUMMARY STEPS

1. **config t**
2. **spanning-tree loopguard default**
3. **exit**
4. (Optional) **show spanning-tree summary**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	Command or Action	Purpose
ステップ 2	**spanning-tree loopguard default** **Example:** `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**
	Example:
	`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	(Optional) **show spanning-tree summary** **Example:** `switch# show spanning-tree summary`	STP の概要を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

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

Note 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。

Note 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。

Before you begin

この機能を設定する前に、次の点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。

SUMMARY STEPS

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. (Optional) **show spanning-tree interface** *type slot/port* **detail**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *type slot/port*
	Example:
	`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**} **Example:** `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、

	Command or Action	Purpose
		ループ ガードも指定ポートでディセーブルになります。 **Note** 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**
	Example:
	`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*
	Example:
	`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**} **Example:** `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**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 8	(Optional) **show spanning-tree interface** *type slot/port* **detail** **Example:** `switch# show spanning-tree interface ethernet 1/4 detail`	STP の概要を表示します。
ステップ 9	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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 ethernet 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）

Note 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。

SUMMARY STEPS

1. **config t**
2. **no spanning-tree mst simulate pvst global**
3. **exit**
4. (Optional) **show spanning-tree summary**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**no spanning-tree mst simulate pvst global** **Example:** `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

	Command or Action	Purpose
		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**
	Example:
	`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	(Optional) **show spanning-tree summary** **Example:** `switch# show spanning-tree summary`	STP の詳細を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-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。

Example

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)# exit
switch#
```

ポートごとの PVST シミュレーションの設定

Note 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。

SUMMARY STEPS

1. **config t**
2. **interface** {{*type slot/port*} |{**port-channel** *number*}}
3. **spanning-tree mst simulate pvst disable** または **spanning-tree mst simulate pvst** または **no spanning-tree mst simulate pvst**
4. **exit**
5. (Optional) **show spanning-tree interface** *type slot/port* **detail**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** {{*type slot/port*} |{**port-channel** *number*}}
	Example:
	`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 simulate pvst disable** または **spanning-tree mst simulate pvst** または **no spanning-tree mst simulate pvst** **Example:** `switch(config-if)# spanning-tree mst simulate pvst`	• **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。

	Command or Action	Purpose

ステップ 4	**exit**
	Example:
	`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	(Optional) **show spanning-tree interface** *type slot/port* **detail** **Example:** `switch# show spanning-tree interface ethernet 3/1 detail`	STP の詳細を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

Example

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。

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

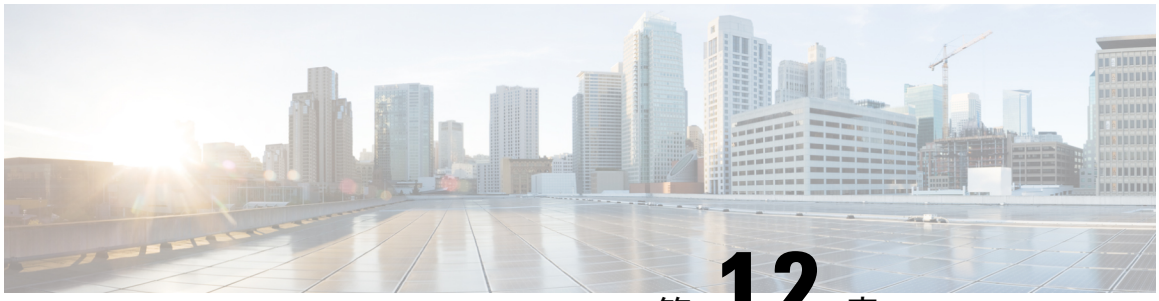
関連項目	マニュアル タイトル
レイヤ2インターフェイス	『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』
NX-OS の基礎	『*Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide*』
高可用性	『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』
システム管理	『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』

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。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.htm



第 12 章

レイヤ2スイッチングのリフレクティブリレーの設定

- リフレクティブリレー802.1Qbgについて （223 ページ）
- リフレクティブ リレーのガイドラインと制約事項, on page 224
- NX-OS CLI を使用したリフレクティブ リレーの設定 （224 ページ）

リフレクティブリレー802.1Qbgについて

Cisco Nexusリリース9.2（1）以降、Cisco Nexus N9K-C93180YC-FXおよびN9K-C93180TC-FXスイッチは、スイッチングオプションのリフレクトリレーをサポートしています。現在のリリースでは、Cisco Nexus N9K-C93180YC-EXおよびN9K-C93180TC-EXスイッチもサポートされています。この機能は IEEE 標準 802.1Qbg のタグレス アプローチです。ポリシーを適用し、必要に応じて、宛先またはターゲットVMサーバ上にトラフィックを送信する外部のスイッチへのすべてのトラフィックを転送します。ローカルスイッチングはありません。ブロードキャストまたはマルチキャスト トラフィックは、リフレクティブ リレーは、各 VM サーバでローカルにパケットのレプリケーションを提供します。

リフレクティブリレーは、スイッチング機能と管理機能に外部スイッチを活用し、サーバリソースを解放してVMをサポートします。リフレクティブリレーは、Cisco Nexusスイッチで設定したポリシーを同じサーバ上のVM間のトラフィックに適用します。

リフレクティブリレーを有効にすると、着信した同じポートからのトラフィックを元に戻すことができます。NX-OS CLIを使用して、レイヤ2物理ポートまたはポートチャネルインターフェイスポリシーでリフレクティブリレーをイネーブルにできます。この機能はデフォルトで無効に設定されています。

用語 仮想イーサネット ポートのためのアグリゲータ 802.1Qbg を説明する (VEPA) が使用されるも機能します。

リフレクティブ リレーのサポート

リフレクティブ リレーには、次のサポートされています。

- Cisco Nexus N9K-C93180YC-EX、N9K-C93180TC-EX、N9K-93180YC-FX、および N9K-C93180TC-FXシリーズスイッチ。
- IEEE 標準 802.1Qbg タグのないアプローチ、リフレクティブ リレーとも呼ばれます。
- 物理ドメイン：仮想ドメインはサポートされません。
- 物理ポートおよびポートチャネル：Cisco Fabric Extender（FEX）およびブレードサーバをサポートしません。リフレクティブリレーはサポートされていないインターフェイスで有効になっていると、障害が発生すると、最後の有効な設定が保持されます。ポートでリフレクティブ リレーを無効にすると、障害をクリアします。

リフレクティブ リレーのガイドラインと制約事項

反射型リレーには、次の設定ガイドラインまたは制限事項があります。

- Cisco Nexus リリース 7.0(3)I7(1) 以降、Cisco Nexus N9K-C93180YC-EX および N9K-C93180TC-EX スイッチはスイッチング オプションおよびリフレクティブ リレーをサポートしています。
- リフレクティブ リレー機能を使用する前に、ARP 抑制を無効にする必要があります。
- Cisco Nexus リリース 9.2(1) 以降、Cisco Nexus N9K-C93180YC-FX および N9K-C93180TC-FX スイッチはスイッチング オプションおよびリフレクティブ リレーをサポートしています。
- Cisco Nexusリリース9.3（2）以降、Cisco Nexus N9K-9336C-FX2スイッチは反射型リレーをサポートします。
- すべてのサーバ側インターフェイスは、リフレクションリレーをサポートするように設定する必要があります。
- Cisco NX-OS リリース 10.2(2)F 以降、仮想イーサネット ポート アグリゲータ（VEPA）機能が Cisco N9K-9332D-GX2B プラットフォーム スイッチでサポートされています。

NX-OS CLI を使用したリフレクティブ リレーの設定

反射型リレーはデフォルトで無効になっています。ただし、ポートまたはポートチャネルでスイッチのレイヤ2インターフェイスポリシーとしてイネーブルにできます。CLI では、NX-OS テンプレートを使用して、複数のポートでリフレクティブ リレーの有効化または individual ports(個々のポート、個別ポート) で有効にすることができます。

手順

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

ステップ 2　interface ethernet 1/2

例：

```
switch(config)# interface ethernet 1/2
switch(config-if)#
```

ポートを有効（オン）にしてください。

ステップ 3　switchport mode virtual-ethernet-bridge

例：

```
switch(config-if)# switchport mode virtual-ethernet-bridge
switch(config-if)#
```

レイヤ2ポートをリフレクティブリレー機能のホストポートとして設定します。

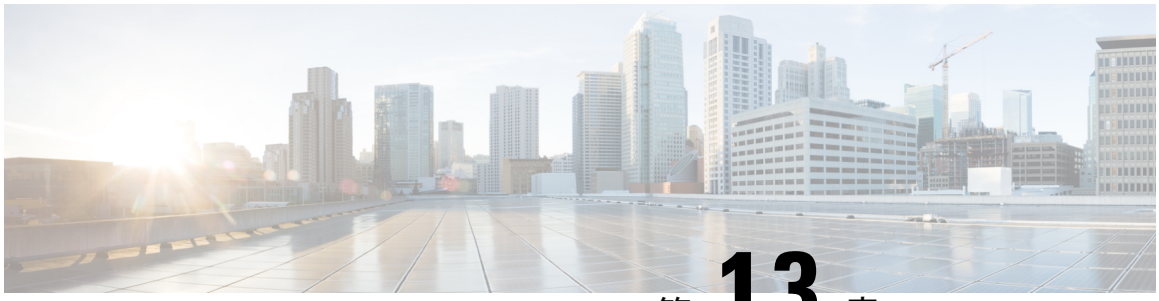
ステップ 4　[no] switchport virtual-ethernet-bridge

例：

```
switch(config-if)# switchport virtual-ethernet-bridge
```

リフレクティブ リレー機能をイネーブルにします。

（注）
リフレクティブリレー機能は、アクセスポートまたはトランクポートでのみサポートされます。



第 13 章

トラフィック ストーム制御の設定

この章では、Cisco NX-OS デバイスに、トラフィック ストーム制御機能を設定する手順について説明します。

この章は、次の項で構成されています。

- トラフィック ストーム制御について, on page 227
- トラフィック ストーム制御のガイドラインと制約事項 （229 ページ）
- トラフィック ストーム制御のデフォルト設定, on page 233
- ワンレベルのしきい値のトラフィック ストーム制御の設定, on page 233
- ツーレベルのしきい値のトラフィック ストーム制御の設定 （235 ページ）
- トラフィック ストーム制御の設定の確認, on page 236
- トラフィック ストーム制御カウンタのモニタリング （237 ページ）
- トラフィック ストーム制御の設定例 , on page 237
- トラフィック ストーム制御のシステム ログの例 （238 ページ）

トラフィック ストーム制御について

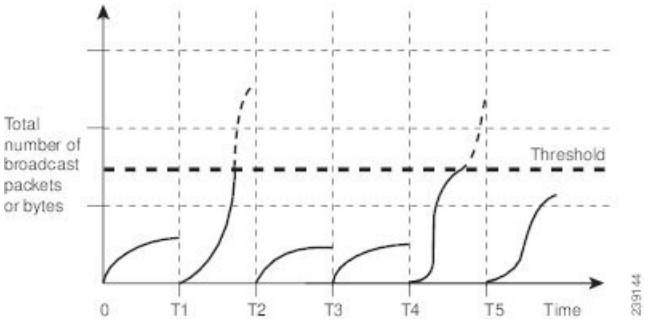
トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御機能を使用すると、物理インターフェイスにおけるブロードキャスト、マルチキャスト、またはユニキャスト トラフィック ストームによって、レイヤ 2 ポート経由の通信が妨害されるのを防げます。

トラフィック ストーム制御（トラフィック抑制ともいう）では、ブロードキャスト、マルチキャスト、ユニキャストの着信トラフィックのレベルを 3.9 ミリ秒間隔でモニターできます。この間、トラフィック レベル（ポートの使用可能合計帯域幅に対するパーセンテージ）が、設定したトラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。

次の表に、指定したインターバルでのレイヤ 2 インターフェイス上のブロードキャスト トラフィック パターンを示します。この例では、トラフィック ストーム制御が T1 と T2 時間の間、

および T4 と T5 時間の間で発生します。これらの間隔中に、ブロードキャスト トラフィックの量が設定済みのしきい値を超過したためです。

Figure 20: ブロードキャストの抑制



トラフィック ストーム制御しきい値の数値と期間の組み合わせにより、トラフィック ストーム制御アルゴリズムがさまざまな粒度で機能します。しきい値が高いほど、通過できるパケット数が多くなります。

Cisco Nexus 9000v デバイスのトラフィック ストーム制御はハードウェアに実装されています。トラフィック ストーム制御は、レイヤ 2 インターフェイスからスイッチング バスに渡されるパケットをモニタします。システムはパケットの宛先アドレスに設定されている Individual/Group ビットを使用して、パケットがユニキャストかブロードキャストかを判断し、3.9 ミリ秒以内の間隔で現在のパケット数を追跡します。パケット数がしきい値に到達したら、後続のパケットをすべて破棄します。

トラフィック ストーム制御では、トラフィック量の計測に帯域幅方式を使用します。制御対象のトラフィックが使用できる、利用可能な合計帯域幅に対するパーセンテージを設定します。パケットは一定間隔で着信するわけではないので、3.9 ミリ秒の間隔はトラフィック ストーム制御の動作に影響を及ぼす可能性があります。

次に、トラフィック ストーム制御の動作がどのような影響を受けるかを示します。

- ブロードキャスト トラフィック ストーム制御をイネーブルにした場合、ブロードキャスト トラフィックが 3.9 ミリ秒のインターバル中に制御レベルを超えると、インターバルが終了するまですべてのブロードキャスト トラフィックがドロップされます。
- ブロードキャストとマルチキャストのトラフィック ストーム制御をイネーブルにした場合、ブロードキャストとマルチキャストの混合トラフィックが 3.9 ミリ秒のインターバル中に制御レベルを超えると、インターバルが終了するまでブロードキャストとマルチキャストのすべてのトラフィックがドロップされます。
- ブロードキャストとマルチキャストのトラフィック ストーム制御をイネーブルにした場合、ブロードキャスト トラフィックが 3.9 ミリ秒のインターバル中に制御レベルを超えると、インターバルが終了するまでブロードキャストとマルチキャストのすべてのトラフィックがドロップされます。
- ブロードキャストとマルチキャストのトラフィック ストーム制御をイネーブルにした場合、マルチキャスト トラフィックが 3.9 ミリ秒のインターバル中に制御レベルを超える

と、インターバルが終了するまでブロードキャストとマルチキャストのすべてのトラフィックがドロップされます。

トラフィックが設定レベルを超過する場合、トラフィック ストーム制御を設定して次のオプションの修正措置を実行することができます。

- シャットダウン：入力トラフィックがポートに対して設定されたトラフィック ストーム制御レベルを超えると、トラフィック ストーム制御がポートを errdisable ステートにします。このポートを再度イネーブルにするために、設定されたインターフェイス上で **shutdown** と **no shutdown**オプションを使用することも、error-disable 検出および回復機能を使用することもできます。error-disable 検出および回復用の **errdisable recovery cause storm-control** コマンドは回復間隔を定義する **errdisable recovery interval** コマンドと一緒に使用することをお勧めします。この間隔は 30 ～ 65535 秒の範囲にすることができます。
- トラップ：入力トラフィックが設定されたトラフィック ストーム制御レベルを超えたときに SNMP トラップを生成するようにトラフィック ストーム制御を設定できます。SNMP トラップアクションはデフォルトでイネーブルになっています。ただし、ストーム制御トラップはデフォルトでレート制限されません。コマンドを使用して、1分あたりに生成されるトラップの数を制御できます。**snmp-server enable traps storm-control trap-rate**

デフォルトで、Cisco NX-OS は、トラフィックが設定済みレベルを超えても是正のための処理を行いません。

トラフィック ストーム制御のガイドラインと制約事項

トラフィック ストーム制御には、次の設定時のガイドラインおよび制約事項があります。

- sFlow も有効になっているインターフェイスでストーム制御を有効にした場合、ストーム制御機能は動作しません。
- ストーム制御 PPS オプションは、Cisco Nexus 9300-FX2 プラットフォーム スイッチでのみサポートされます。
- Cisco Nexus NFE2対応デバイスの場合、ストーム制御CPUを使用してCPUに送信されるARPパケットの数を制御できます。
- ストーム制御は、物理インターフェイス、ポートチャネルインターフェイス、およびブレークアウトインターフェイスで設定できます。
- トラフィック ストーム制御レベルをインターフェイスの帯域幅全体に対する割合として指定します。
  - pps の範囲は 0 ー 200000000 です。
  - 任意で、レベルの小数部を 0 ～ 99 の範囲で指定できます。
  - 100% は、トラフィック ストーム制御がないことを意味します。
  - 0.0% は、すべてのトラフィックを抑制します。

- 9400シリーズラインカードを搭載したCisco Nexus 9500シリーズスイッチ、およびCisco Nexus 9300シリーズスイッチでは、ストーム制御CLIを使用して、帯域幅レベルをポート容量のパーセンテージまたは1秒あたりのパケット数として指定できます。
- Cisco Nexusリリース9.2（1）以降では、ストーム制御パケット/秒を次のように設定すると、エラーマージンが1%を超えます。
  - 60秒未満のトラフィック期間
  - ストーム制御ppsが1000未満
- Cisco Nexusリリース9.2（1）以降では、Cisco Nexus 9336C-FX2、Cisco Nexus 93300YC-FX2、およびCisco Nexus 93240YC-FX2-Zスイッチのポート容量または1秒あたりのパケット数の割合を使用できます。
- Cisco Nexus 9200、9300-EXプラットフォームスイッチ、またはN9K-X9700-FX3ラインカードでVLANのSVIを設定している場合、ストーム制御ブロードキャストはARPトラフィック（ARP要求）に対して機能しません。
- ストーム制御ドロップが個別にカウントされるを防ぐ、ローカル リンクおよびハードウェアの制約事項があります。代わりに、ストーム制御ドロップは discards カウンタの他のドロップとともにカウントされます。
- ハードウェアの制限およびサイズの異なるパケットがカウントされる方式のため、トラフィック ストーム制御レベルの割合は概数になります。着信トラフィックを構成するフレームのサイズに応じて、実際に適用されるパーセンテージ レベルと設定したパーセンテージ レベルの間には、数パーセントの誤差がある可能性があります。
- ハードウェアの制限により、**show interface counters storm-control** の出力は次のとおりです。 コマンドは、ストーム制御が設定され、インターフェイスが実際にARPブロードキャスト トラフィックを抑制している場合、ARP 抑制を表示しません。この制限によって、設定されたアクションがトリガーされない可能性がありますが、入力 ARP ブロードキャストトラフィックは正しくストーム抑制されます。
- ハードウェアの制限により、ストーム制御は、Cisco Nexus GX シリーズプラットフォームスイッチのポート帯域幅の 70% を超える 400G ポートではサポートされません。
- ハードウェアの制限のため、パケット ドロップ カウンタは、トラフィック ストームが原因のパケット ドロップパケット ドロップによって発生その他の破棄された入力フレームとを区別できません。この制限によって、トラフィック ストームが発生していなくても、設定されたアクションがトリガーされる可能性があります。
- ハードウェアの制限により、ストーム抑制パケットの統計情報はアップリンクポートではサポートされません。
- ハードウェアの制限により、ストーム抑制パケット統計情報には、アクティブなSwitched Virtual Interface（SVI）を備えたVLAN上のブロードキャストトラフィックは含まれません。
- 設計上の制限により、設定されたレベルが0.0の場合、ストーム抑制パケットの統計情報は機能しません。これは、すべての着信ストームパケットを抑制することを意味します。

- トラフィックストーム制御は、Cisco Nexus 9300シリーズスイッチおよび9700-EX / FXラインカードを搭載したCisco Nexus 9500シリーズスイッチでサポートされます。
- トラフィックストーム制御は、Cisco N9K-M4PC-CFP2ではサポートされていません。
- トラフィックストーム制御は、FEXインターフェイスではサポートされません。
- トラフィックストーム制御は、未知のユニキャスト、未知のマルチキャスト、ブロードキャスト トラフィックなどの入力トラフィック専用です。

（注） Cisco Nexus 9000シリーズスイッチでは、トラフィックストーム制御は不明なユニキャストトラフィックと不明なユニキャストトラフィックに適用されます。

- 設定されたアクションによってポートチャネルメンバーがエラーディセーブルになった場合、すべての個々のメンバーポートをフラップして、エラーディセーブル状態から回復する必要があります。
- Cisco Nexusリリース9.2（1）のトラフィックストーム制御機能は、N9K-X96136YC-Rラインカードおよび N9K-C9504-FM-Rファブリックモジュールを搭載したCisco Nexus 9500プラットフォームスイッチではサポートされません。
- Cisco Nexusリリース9.3（2）以降では、N9K-X96136YC-R、N9K-X9636C-R、N9K-X9636Q-R、N9K- X9636C-RXラインカード、および N9K-C9504-FM-Rおよび N9K-C9508-FM-Rファブリックモジュール。トラフィックストーム制御カウンタおよびストーム制御アクションはサポートされていません。
- 次のガイドラインと制約事項は、Cisco Nexus 9200 シリーズ スイッチに適用されます。
  - 不明なマルチキャストトラフィックによるトラフィックストーム制御はサポートされていません。
  - ポリサーはバイトベースの統計情報のみをサポートするため、トラフィックストーム制御ではパケットベースの統計情報はサポートされません。
  - トラフィックストーム制御は、copy-to-CPUパケットではサポートされません。
- Cisco NX-OS リリース10.1(2) 以降では、N9K-X9624D-R2 および N9K-C9508-FM-R2 プラットフォーム スイッチで ストーム制御機能がサポートされます。
- Cisco Nexusリリース10.1（2）以降、Cisco Nexus N9300-FXおよびN9300-FX2シリーズスイッチでは、ブロードキャスト、不明なユニキャスト、およびマルチキャスト（BUM）トラフィックの2レベルのしきい値とロギングのサポートを設定できます。各しきい値レベルのトラップまたはシャットダウンアクション。既存のストーム制御設定は、1レベルのしきい値にのみ使用されるようになりました。
- 次のガイドラインと制限事項は、Cisco Nexus 10.1（2）リリースのBUMトラフィック機能の2レベルしきい値およびロギングに適用されます。

- Cisco Nexusリリース10.1（2）の新しいトラフィックストーム制御機能は、Cisco Nexus N9300-FXでは最大62ポート（単一スライスとして）、Cisco Nexus N9300-FX2では合計124ポート（2スライスとして）をサポートします。
- トラフィックストーム制御は、一度に1つのストーム制御モード（1レベルまたは2レベルのしきい値）にあるデバイスのみをサポートします。一度に1レベルのしきい値と2レベルのしきい値ストーム制御モードを混在させることはできません。
- トラフィックストーム制御は、トラフィック統計情報をモニタし、Cisco Nexusリリース10.1（2）からの各レベル（下位および上位）およびトラフィックタイプ（不明なユニキャスト、マルチキャスト、およびブロードキャスト）のシステムログを生成します。
- 2レベルしきい値トラフィックストーム制御機能では、固定サイズ512の新しいTernary Content Addressable Memory（TCAM）リージョンのカービングと、デバイスのリロードが必要です。
- 2レベルしきい値のトラフィックストーム制御は、L2 Netflow機能、つまりconfig layer2スイッチドフローモニタCLIと共存できません。これは、TCAMリソースの制限によるものです。
- トラフィックストーム制御の2レベルしきい値機能は、非IP MCフラッドトラフィック（IPヘッダーのないパケット）およびパケット/秒モードをサポートしません。
- トラフィックストーム制御は、Generic Online Diagnostics（GOLD）パケットおよびサブインターフェイスレベルではサポートされません。
- 以前のリリースで10.1（2）にアップグレードし、2レベルのストーム制御機能を使用する場合は、新しいストーム制御コマンドを使用してスイッチを設定してください。
- バージョン10.1（2）で2レベルストーム制御機能を設定しており、以前のバージョンにダウングレードする場合、新しい機能はダウングレードをサポートしません。ダウングレードするには、設定を削除します。

- Cisco Nexusリリース10.2（1）以降、ストーム制御では、1つのインターフェイスに複数のアクションを設定できません。以前のアクション値が上書きされると、設定されている最新のアクション値が考慮されます。
- Cisco NX-OS リリース 10.2(2)F 以降、ストーム制御機能は Cisco N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。

トラフィック ストーム制御のデフォルト設定

次の表に、トラフィック ストーム制御パラメータのデフォルト設定値を示します。

Table 15: デフォルトのトラフィック ストーム制御パラメータ

パラメータ	デフォルト
トラフィック ストーム制御	無効
しきい値パーセンテージ	100

ワンレベルのしきい値のトラフィック ストーム制御の設定

制御対象のトラフィックがツーレベルしきい値に使用できる、利用可能な合計帯域幅に対するパーセンテージを設定できます。

Note

- トラフィック ストーム制御機能では、トラフィック ストーム制御の動作を 3.9 ミリ秒間隔で変更できます。
- ポートチャネルに storm-control-cpu レートを設定する前に、n9k-arp-acl TCAM リージョンをカービングする必要があります。TCAM リージョン サイズの設定の詳細については、『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』の「*Configuring ACL TCAM Region Sizes*」の章を参照してください。https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-installation-and-configuration-guides-list.html

SUMMARY STEPS

1. **configure terminal**
2. **interface** {**ethernet** *slot*/*port* | **port-channel** *number*}
3. [**no**] **storm-control** {**broadcast** | **multicast** | **unicast**} **level** { *<level-value %>* | **pps** < *pps-value* > }
4. [**no**] **storm-control action trap**
5. [**no**] **storm-control-cpu arp rate**
6. **exit**
7. (Optional) **show running-config interface** {**ethernet** *slot*/*port* | **port-channel** *number*}
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`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。

ステップ 2	**interface** {**ethernet** *slot*/*port* | **port-channel** *number*}
	Example:
	`switch# interface ethernet 1/1`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	[**no**] **storm-control** {**broadcast** | **multicast** | **unicast**} **level** { <*level-value %*> | **pps** < *pps-value* > }
	Example:
	`switch(config-if)# storm-control unicast level 40`
	Example:
	`switch(config-if)# storm-control broadcast level pps 8000`
		インターフェイスを通過するトラフィックのトラフィック ストーム制御を設定します。ポート容量または 1 秒あたりのパケット数の割合として帯域幅レベルを設定することもできます。デフォルトのステートはディセーブルです。

ステップ 4	[**no**] **storm-control action trap** **Example:** `switch(config-if)# storm-control action trap`	トラフィック ストーム制御の制限に達すると、SNMP トラップ（CISCO-PORT-STORM-CONTROL-MIBで定義）を生成します。
ステップ 5	[**no**] **storm-control-cpu arp rate** **Example:** `switch(config-if)# storm-control-cpu arp rate`	ポート チャネルに入る ARP パケットのトラフィック ストーム制御レートを設定します。このレートは、ポートチャネルのメンバー間で均等に分割されます。

ステップ 6	**exit**
	Example:
	`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 7	(Optional) **show running-config interface** {**ethernet** *slot*/*port* | **port-channel** *number*} **Example:** `switch(config)# show running-config interface ethernet 1/1`	トラフィック ストーム制御の設定を表示します。
ステップ 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-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。

ツーレベルのしきい値のトラフィック ストーム制御の設定

制御対象のトラフィックがツーレベルしきい値に使用できる、利用可能な合計帯域幅に対するパーセンテージを設定できます。

手順の概要

1. **system storm control multi-threshold**
2. **hardware access-list tcam region ing-storm-control 512**
3. **configure terminal**
4. **interface** {**ethernet** *slot*/*port* | **port-channel** *number*}
5. [**no**] **storm-control multiunicast** {**level1** *<level-value %>* | **level2** *<level-value %>*}
6. [**no**] **storm-control multi action1** {**trap** | **shutdown**} **action2** {**trap** | **shutdown**}
7. **exit**
8. （任意） **show running-config interface** {**ethernet** *slot*/*port* | **port-channel** *number*}
9. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**system storm control multi-threshold** 例： `switch# system storm control multi-threshold`	グローバル CLI を入力します。このコマンドはツーレベルしきい値を設定するときにのみ必要です。
ステップ 2	**hardware access-list tcam region ing-storm-control 512** 例： `switch# hardware access-list tcam region ing-storm-control 512`	新規 TCAM リージョンは、ツーレベルしきい値向けに固定サイズ 512でカービングされます。 コマンド実行後、デバイスをリロードしてください。

ステップ 3	**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。

ステップ 4	**interface** {**ethernet** *slot*/*port*	**port-channel** *number*}
		例：
		`switch(config)# interface ethernet 1/1`
		`switch(config-if)#`
			インターフェイス設定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 5	[**no**] **storm-control multiunicast** {**level1** <*level-value %*> | **level2** <*level-value %*>} 例： `switch(config-if)# storm-control multi unicast level1 5 level2 10`	ツーレベルしきい値のインターフェイスを通過するトラフィックのトラフィック ストーム制御を設定します。 ポート容量のパーセンテージとして帯域幅レベルを設定することもできます。デフォルトのステートはディセーブルです。
ステップ 6	[**no**] **storm-control multi action1** {**trap** | **shutdown**} **action2** {**trap** | **shutdown**} 例： `switch(config-if)# storm-control multi action1 trap action2 shutdown`	次が生成されます: • SNMP トラップ（CISCO-PORT-STORM-CONTROL-MIB で定義）でストーム制御をモニタします。 • トラフィック ストーム制御が制限に到達すると、シスログ メッセージが生成されます。 ストーム制御しきい値の低/高レベルでトラップおよびシャットダウンアクションを設定することもできます。ただし、ポートの低しきい値（level1）をシャットダウンに設定する場合、ポートの高しきい値（level2）にシャットダウンを設定する必要があります。

ステップ 7	**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 8	（任意） **show running-config interface** {**ethernet** *slot*/*port* | **port-channel** *number*} 例： `switch(config)# show running-config interface ethernet 1/1`	トラフィック ストーム制御の設定を表示します。
ステップ 9	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-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。

トラフィック ストーム制御の設定の確認

トラフィック ストーム制御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 interface	トラフィック ストーム制御の設定を表示します。
show access-list storm-control arp-stats interface [ethernet | **port-channel**] *number*	インターフェイス上の ARP パケットのストーム制御統計情報を表示します。

トラフィック ストーム制御カウンタのモニタリング

トラフィック ストーム制御動作に関して Cisco NX-OS デバイスが維持するカウンタをモニタリングできます。

コマンド	目的
次の行は、ワンレベルのしきい値にのみ適用されます。	
show interface [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control**	トラフィック ストーム制御カウンタを表示します。
次の行は、ツーレベルのしきい値にのみ適用されます。	
show interface [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control multi-threshold**	すべてのインターフェイスに設定されたストーム制御値のリストを表示します。
show interface [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control multi-threshold**	すべてのインターフェイスに設定されたストーム制御値のリストを表示します。
show interface [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control multi-threshold unicast**	level1 と level2 の両方のマルチユニキャストドロップのリストを表示します。
show interface [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control multi-threshold broadcast**	level1 と level2 の両方のマルチ broadcast ドロップのリストを表示します。
show interface [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control multi-threshold multicast**	level1 と level2 の両方のマルチキャストドロップのリストを表示します。

トラフィック ストーム制御の設定例

次に、 ワンレベルしきいイ値のトラフィック ストーム制御の設定例を示します。

```
switch# configure terminal
switch(config)# interface Ethernet1/1
switch(config-if)# storm-control broadcast level 40
switch(config-if)# storm-control multicast level 40
switch(config-if)# storm-control unicast level 40
switch(config)# storm-control-cpu arp rate 150
```

次に、ツーレベルしきい値のトラフィック ストーム制御の設定例を示します。

```
switch# system storm control multi-threshold
switch# hardware access-list tcam region ing-storm-control 512
switch# configure terminal
switch(config)# interface Ethernet1/1
switch(config-if)# storm-control multi broadcast level1 5 level2 10
switch(config-if)# storm-control multi multicast level1 5 level2 10
switch(config-if)# storm-control multi unicast level1 5 level2 10
switch(config-if)# storm-control multi action1 trap action2 shutdown
```

次に、プログラムされた設定レートと、ドロップされた ARP パケットの統計情報を確認する例を示します。

```
switch(config)# sh access-list storm-control-cpu arp-stats
interface port-channel 132
slot  1
=======
------------------------------------------------------------------------
            ARP Policer Entry Statistics
------------------------------------------------------------------------
Interface port-channel132:
----------
Member Interface   Entry-ID  Rate     RedPacket Count     GreenPacket Count
-------------------------------------------------------------------------------
Ethernet1/35        3976        50           0                0
-------------------------------------------------------------------------------

slot  7
=======
------------------------------------------------------------------------
            ARP Policer Entry Statistics
------------------------------------------------------------------------
Interface port-channel132:
----------
Member Interface   Entry-ID  Rate     RedPacket Count     GreenPacket Count
-------------------------------------------------------------------------------
```

トラフィック ストーム制御のシステム ログの例

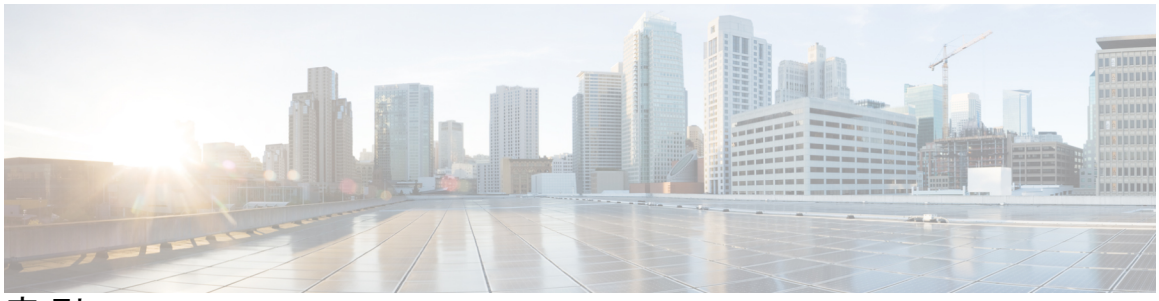
次の例は、1レベルのしきい値を持つトラフィックストーム制御のシステムログを示しています。

- `%ETHPORT-5-STORM_CONTROL_ABOVE_THRESHOLD: Traffic in port Ethernet1/5 exceeds the configured threshold , action - Trap`

次に、2レベルのしきい値を持つトラフィックストーム制御のシステムログの例を示します。

- `%ETHPORT-5-STORM_CONTROL_ABOVE_THRESHOLD: Traffic in port Ethernet1/5 exceeds the configured Broadcast threshold level1[10%], action - Trap`
- `%ETHPORT-5-STORM_CONTROL_ABOVE_THRESHOLD: Traffic in port Ethernet1/5 exceeds the configured Broadcast threshold level1[15%], action - Shutdown`

（注） システムログメッセージには、しきい値を超えた特定のトラフィックタイプと、そのトラフィックタイプがインターフェイスのストーム制御アクションに到達したレベルが含まれます。



索 引

A

abort **161, 165–166, 170**

C

clear spanning-tree counters interface **187**
clear spanning-tree counters **144**
clear spanning-tree detected-protocol interface **186**
clear spanning-tree detected-protocol **143, 186**
clear vlan **54, 98**
clear mac address-table dynamic address **18**
config t **12–13, 18–19, 44–50, 60, 77, 79, 81, 83–87, 89, 91, 94–96, 127–129, 131–142, 159–165, 167–168, 170–173, 175–184, 201, 203–207, 209, 211–214, 216, 218, 220**

F

feature private-vlan **77**
feature vtp **60**

H

ようこそ **169**
hello-time **132, 170**

I

instance **167–168**
interface vlan **83**
インターフェイス **84–87, 89–91, 94–96, 135–137, 142, 175–177, 183–185, 203–206, 212–213, 216, 220**

M

mac-address bpdu source version 2 **107**
mac address-table aging-time **16**
mac address-table static **13**

N

no private-vlan **81**
no vlan **81**

P

primary root **169**
private-vlan mapping **98**

R

リビジョン **164–166**

S

show interface **52–53**
show interface counters storm-control **230, 237**
show interface ethernet counters storm-control **237**
show interface port-channel counters storm-control multi-threshold broadcast **237**
show interface port-channel counters storm-control multi-threshold multicast **237**
show interface port-channel counters storm-control multi-threshold unicast **237**
show interface port-channel counters storm-control multi-threshold **237**
show interface port-channel counters storm-control **237**
show interface private-vlan mapping **98**
show interface switchport **85–86, 88–91, 93–98**
show interface vlan **83–84, 98**
show mac address-table aging-time **16–17**
実行中を表示 **128, 130**
show running-config interface {ethernet | port-channel} **233–236**
show running-config interface **237**
show running-config spanning-tree all **127–128, 159–160, 186**
show running-config spanning-tree **186, 221**
show running-config vlan **51, 54, 98**
show spanning-tree detail vlan **187**
show spanning-tree detail **187**
show spanning-tree interface **135–136, 203–206, 209, 216–217, 220–221**
show spanning-tree mst configuration **162–168, 186**
show spanning-tree mst detail **186**
show spanning-tree mst **170–183, 186, 221**
show spanning-tree pathcost method **136–137**
show spanning-tree summary **186, 201–202, 207–208, 211, 214–215, 218–219, 221**
show spanning-tree vlan **132–134, 138–141, 187**
show spanning-tree **128–129, 131, 142, 144, 184–185**
show system vlan reserved **40**

show vlan counters 54, 98
show vlan private-vlan 79–82, 98
show vlan summary 54
show vlan 44–49, 54
show vtp counters 60–61
show vtp interface 60–61
show vtp password 60–61
show vtp status 47, 49, 54, 60–61
show vtp trunk interface eth a / b 59
show mac address-table 18
show mac address-table static 13
spanning-tree bpdufilter disable 212
spanning-tree bpdufilter enable 212
spanning-tree bpduguard disable 208
spanning-tree bpduguard enable 208
spanning-tree guard 216
spanning-tree link-type 115, 142, 184–185
spanning-tree loopguard default 214–215
spanning-tree mode mst 159–160
spanning-tree mode rapid-pvst 127
spanning-tree mst configuration 161–165, 167–168
spanning-tree mst hello-time 131–132, 169, 178
spanning-tree mst max-age 131–132, 169, 180–181
spanning-tree mst max-hops 182
spanning-tree mst pre-standard 183
spanning-tree mst priority 173
spanning-tree mst root primary 173
spanning-tree mst root secondary 173
spanning-tree mst simulate pvst disable 220
spanning-tree mst simulate pvst 220
spanning-tree mst 170–177
spanning-tree pathcost method 136–137
spanning-tree port type edge bpdufilter default 211–212
spanning-tree port type edge bpduguard default 207
spanning-tree port type edge default 201
spanning-tree port type edge trunk 203
spanning-tree port type edge 203–204
spanning-tree port type network default 201, 205
spanning-tree port type network 205–206
spanning-tree port type normal 203, 205
spanning-tree port type 112
spanning-tree vlan 128–134, 138–141, 169
spanning-tree mst forward-time 131–132, 169, 179–180
state active 47–48
state suspend 47–48
storm-control {broadcast | multicast | unicast} 233–234
storm-control action trap 233–236
storm-control multi unicast 235–236
storm-control-cpu arp rate 233–234
switching-mode store-forward 103–104
switchport 86–87, 91–92, 96
switchport mode private-vlan host 84–85, 94–95
switchport mode private-vlan promiscuous 89–90
switchport mode private-vlan trunk allowed vlan 91–92
switchport mode private-vlan trunk promiscuous 91–92
switchport mode private-vlan trunk secondary 86–87, 96
switchport mode trunk 52–53
switchport private-vlan trunk allowed vlan 86–87, 96–97
switchport private-vlan trunk allowed 74
switchport private-vlan trunk native vlan 86–87, 91–92, 96
switchport vlan mapping 52–53
switchport vlan mapping enable 52–53
system private-vlan fex trunk 94
system vlan long-name 50–51

V

vlan 39, 42, 44–48, 79, 81, 166
vlan configuration 49–50
vtp domain 60–61
vtp password 60–61
vtp version 60–61
vtp file 60–61

い

インスタンス 165

し

remove 80

す

spanning-tree 135–137

ち

diameter 132, 169–170, 172

つ

追加 80

な

名前 47–48, 165–166

翻訳について
このドキュメントは、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。