



Cisco Nexus 3548 Switch NX-OS Layer 2 Switching Configuration Guide, Release 10.6(x)

First Published: 2025-08-13

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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)

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

はじめに xi

対象読者 xi

表記法 xi

Nexus 3548 スイッチ NX-OS ソフトウェアの関連資料 xii

マニュアルに関するフィードバック xiv

通信、サービス、およびその他の情報 xiv

CHAPTER 1

New and Changed Information 1

New and Changed Information 1

CHAPTER 2

概要 3

レイヤ 2 イーサネット スイッチングの概要 3

VLANs 3

スパンニングツリー 4

STP の概要 4

Rapid PVST+ 5

MST 5

STP 拡張機能 5

CHAPTER 3

VLAN の設定 7

VLAN について 7

VLAN の概要 7

VLAN の範囲 9

VLAN の作成、削除、変更 9

VLAN トランッキング プロトコルについて 10

VTP の注意事項と制約事項	10
VLAN の設定	11
VLAN の作成および削除	11
VLAN の設定	12
VLAN へのポートの追加	14
ルーテッド SVI としての VLAN の設定	15
管理 SVI としての VLAN の設定	16
VTP の設定	17
VLAN の設定の確認	19
VLAN の機能履歴	19

CHAPTER 4**プライベート VLAN の設定 21**

プライベート VLAN について	21
プライベート VLAN のプライマリ VLAN とセカンダリ VLAN	23
プライベート VLAN ポート	23
プライマリ、独立、およびコミュニティ プライベート VLAN	24
セカンダリ VLAN とプライマリ プライベート VLAN の関連付け	26
プライベート VLAN 内のブロードキャスト トラフィック	27
プライベート VLAN ポートの分離	28
プライベート VLAN の設定に関する注意事項と制約事項	28
プライベート VLAN の設定	28
プライベート VLAN のイネーブル化	28
プライベート VLAN 上での IGMP スヌーピングのイネーブル化	29
プライベート VLAN としての VLAN の構成	30
セカンダリ VLAN とプライマリ プライベート VLAN の関連付け	31
プライベート VLAN ホスト ポートとしてのインターフェイスの設定	33
プライベート VLAN 無差別ポートとしてのインターフェイスの設定	34
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	35
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	38
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	41
プライベート VLAN 設定の確認	43

CHAPTER 5**アクセス インターフェイスとトランク インターフェイスの設定 45**

アクセス インターフェイスとトランク インターフェイスについて 45

アクセス インターフェイスとトランク インターフェイスの概要 45

IEEE 802.1Q カプセル化の概要 46

アクセス VLAN の概要 47

トランク ポートのネイティブ VLAN ID の概要 48

許可 VLAN の概要 48

ネイティブ 802.1Q VLAN の概要 48

アクセス インターフェイスとトランク インターフェイスの設定 49

LAN インターフェイスをイーサネット アクセス ポートとして設定する 49

アクセス ホスト ポートの設定 50

トランク ポートの設定 51

802.1Q トランク ポートのネイティブ VLAN の設定 52

トランキング ポートの許可 VLAN の設定 53

ネイティブ 802.1Q VLAN の設定 54

インターフェイスの設定の確認 55

CHAPTER 6**Rapid PVST+ の設定 57**

Rapid PVST+ について 57

STP についての概要 57

STP の概要 57

トポロジ形成の概要 58

ブリッジ ID の概要 58

BPDU の概要 60

ルート ブリッジの選定 61

スパニングツリー トポロジの作成 61

Rapid PVST+ の概要 62

Rapid PVST+ の概要 62

Rapid PVST+ BPDU 64

提案と合意のハンドシェイク 65

プロトコル タイマー	66
ポート ロール	66
ポート ステート	68
ポート ロールの同期	70
スパニングツリーの異議メカニズム	72
ポートコスト	72
ポートプライオリティ	73
Rapid PVST+ と IEEE 802.1Q トランク	73
Rapid PVST+ のレガシー 802.1D STP との相互運用	73
Rapid PVST+ の 802.1s MST との相互運用	74
Rapid PVST+ の設定	74
Rapid PVST+ のイネーブル化	75
Rapid PVST+ の VLAN ベースのイネーブル化	76
ルート ブリッジ ID の設定	77
セカンダリ ルート ブリッジの設定	78
Rapid PVST+ のポート プライオリティの設定	80
Rapid PVST+ パスコスト方式およびポート コストの設定	81
VLAN の Rapid PVST+ のブリッジ プライオリティの設定	82
VLAN の Rapid PVST+ の hello タイムの設定	83
VLAN の Rapid PVST+ の転送遅延時間の設定	83
VLAN の Rapid PVST+ の最大経過時間の設定	84
リンク タイプの設定	85
プロトコルの再開	86
Rapid PVST+ 設定の確認	86

CHAPTER 7

マルチ スパニングツリーの設定 89

MST について	89
MST の概要	89
MST 領域	90
MST BPDU	90
MST 設定情報	91

IST、CIST、CST	92
IST、CIST、CST の概要	92
MST 領域内でのスパニングツリーの動作	93
MST 領域間のスパニングツリー動作	93
MST 用語	94
ホップ カウント	95
境界ポート	95
スパニングツリーの異議メカニズム	96
ポート コストとポート プライオリティ	97
IEEE 802.1D との相互運用性	97
Rapid PVST+ の相互運用性と PVST シミュレーションについて	98
MST の設定	98
MST 設定時の注意事項	98
MST の有効化	99
MST コンフィギュレーション モードの開始	100
MST の名前の指定	101
MST 設定のリビジョン番号の指定	102
MST リージョンでの設定の指定	103
VLAN から MST インスタンスへのマッピングとマッピング解除	105
ルートブリッジの設定	106
セカンダリ ルートブリッジの設定	107
ポートのプライオリティの設定	109
ポート コストの設定	110
スイッチ プライオリティの設定	111
hello タイムの設定	112
転送遅延時間の設定	113
最大エージング タイムの設定	114
最大ホップ カウントの設定	114
PVST シミュレーションのグローバル設定	115
ポートごとの PVST シミュレーションの設定	116
リンク タイプの設定	117

プロトコルの再開 118

MST の設定の確認 119

CHAPTER 8

STP 拡張機能の設定 121

概要 121

STP 拡張機能について 121

STP ポート タイプの概要 121

Bridge Assurance の概要 122

BPDU ガードの概要 123

BPDU フィルタリングの概要 123

ループ ガードの概要 124

ルート ガードの概要 125

STP 拡張機能の設定 126

STP 拡張機能の設定における注意事項 126

スパニングツリー ポート タイプのグローバルな設定 126

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 128

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 129

BPDU ガードのグローバルなイネーブル化 130

指定インターフェイスでの BPDU ガードのイネーブル化 131

BPDU フィルタリングのグローバルなイネーブル化 133

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 134

ループ ガードのグローバルなイネーブル化 135

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 136

STP 拡張機能の設定の確認 138

CHAPTER 9

Flex Link の設定 139

Flex Link について 139

プリエンブション 141

マルチキャスト 141

Flex Link の注意事項および制約事項 142

Flex Link のデフォルト設定 143

Flex Link の設定	143
Flex Link プリエンプションの設定	145
Flex Link 設定の確認	147

CHAPTER 10**LLDP の設定 151**

LLDP の設定	151
インターフェイス LLDP の設定	153
LLDP の MIB	155

CHAPTER 11**MAC アドレス テーブルの構成 157**

MAC アドレスに関する情報	157
MAC アドレスの構成	158
スタティック MAC アドレスの設定	158
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	158
MAC テーブルのエージング タイムの設定	160
MAC テーブルからのダイナミック アドレスのクリア	161
MAC 移動ループ検出の設定	161
MAC アドレス設定の確認	162

CHAPTER 12**IGMP スヌーピングの設定 165**

IGMP スヌーピングの情報	165
IGMPv1 および IGMPv2	167
IGMPv3	167
IGMPスヌーピングクエリア	167
IGMP フォワーディング	168
IGMP スヌーピング パラメータの設定	168
IGMP スヌーピング設定の確認	172

CHAPTER 13**トラフィック ストーム制御の設定 175**

トラフィック ストーム制御の概要	175
トラフィック ストーム制御のガイドラインと制約事項	177

トラフィック ストーム制御の設定	178
トラフィック ストーム制御の設定の確認	179
トラフィック ストーム制御の設定例	179
トラフィック ストーム制御のデフォルト設定	180



はじめに

ここでは、*Cisco Nexus 3548* スイッチ *NX-OS* ユニキャスト ルーティング構成ガイドの対象読者、構成、および表記法について説明します。また、関連マニュアルの入手方法についても説明します。

この章は、次の項で構成されています。

- [対象読者](#) (xi ページ)
- [表記法](#) (xi ページ)
- [Nexus 3548 スイッチ NX-OS ソフトウェアの関連資料](#) (xii ページ)
- [マニュアルに関するフィードバック](#) (xiv ページ)
- [通信、サービス、およびその他の情報](#) (xiv ページ)

対象読者

このマニュアルを使用するには、IP およびルーティングのテクノロジーに関する詳しい知識が必要です。

表記法

コマンドの説明では、次の表記法を使用しています。

表記法	説明
太字	コマンドおよびキーワードは太字で示しています。
イタリック体	ユーザーが値を指定する引数は、イタリック体で示しています。
[]	角カッコの中の要素は、省略可能です。
[x y z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。

表記法	説明
string	引用符を付けない一組の文字。 string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

出力例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。



(注) 「注釈」を意味します。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。



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



ヒント 「問題解決に役立つ情報」です。

Nexus 3548 スイッチ NX-OS ソフトウェアの関連資料

Cisco Nexus 3548 スイッチ ソフトウェア全体のマニュアルセットは、次の URL にあります。

http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

リリース ノート

リリース ノートは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps11541/prod_release_notes_list.html

インストール ガイドおよびアップグレード ガイド

インストール ガイドおよびアップグレード ガイドは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps11541/prod_installation_guides_list.html

このカテゴリのマニュアルには、次が含まれます。

- 『Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series Safety Information and Documentation』
- 『Regulatory, Compliance, and Safety Information for the Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series』
- 『Cisco Nexus 3000 Series Hardware Installation Guide』

ライセンス情報

NX-OS の機能ライセンスについては、Cisco NX-OS Licensing Guideを参照してください。次の URL から入手できます：

http://www.cisco.com/en/US/docs/switches/datacenter/sw/nx-os/licensing/guide/b_Cisco_NX-OS_Licensing_Guide.html

コンフィギュレーション ガイド

コンフィギュレーション ガイドは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps11541/products_installation_and_configuration_guides_list.html

このカテゴリのマニュアルには、次が含まれます。

- 『Fundamentals Configuration Guide』
- 『Interfaces Configuration Guide』
- 『Layer 2 Switching Configuration Guide』
- 『Multicast Configuration Guide』
- 『Quality of Service Configuration Guide』
- 『Security Configuration Guide』
- 『System Management Configuration Guide』
- 『Unicast Routing Configuration Guide』
- 『Verified Scalability Guide for Cisco NX-OS』

コマンドリファレンス

コマンドリファレンスは、次の URL で入手できます。

<https://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/products-command-reference-list.html>

エラー メッセージおよびシステム メッセージ

システム メッセージ リファレンス ガイドは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps11541/products_system_message_guides_list.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、nexus3k-docfeedback@cisco.com までご連絡ください。ご協力をよろしくお願いいたします。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によって求めるビジネス成果を得るには、[Cisco Services](#) [英語] にアクセスしてください。
- サービス リクエストを送信するには、[Cisco Support](#) にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco DevNet](#) にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

Cisco バグ検索ツール

[Cisco Bug Search Tool](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。



CHAPTER 1

New and Changed Information

- [New and Changed Information](#), on page 1

New and Changed Information

Table 1: New and Changed Features for Cisco NX-OS Release 10.6(x)

Feature	Description	Changed in Release	Where Documented
NA	No new features added for this release.	10.6(1)F	NA



第 2 章

概要

- [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 3](#)
- [スパニングツリー, on page 4](#)

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、高帯域幅デバイスや多数のユーザによって引き起こされるトラフィックの輻輳を解決するため、各デバイスにドメイン（サーバなど）を割り当てます。

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。1/10 ギガビット イーサネットは、全二重モードだけで動作します。

VLANs

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 に属することができ、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ドされます。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。

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



Note スイッチ間リンク（ISL）トランッキングはサポートされません。

スパニングツリー

ここでは、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。

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、デバイスでは Rapid PVST+ および MST が実行されます。特定の VDC に、Rapid PVST+ または MST のどちらかを使用できます。1 つの VDC では両方は使用できません。Rapid PVST+ はデフォルトの 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 RapidPVST+ 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 ガードは、ポイントツーポイント リンク上の単方向リンク障害が原因で発生するブリッジングループを防止します。

- ルート ガード: ルート ガードは、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を防ぎます。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（ブロッキングされた）状態になります。



第 3 章

VLAN の設定

- [VLAN について（7 ページ）](#)
- [VLAN の設定（11 ページ）](#)

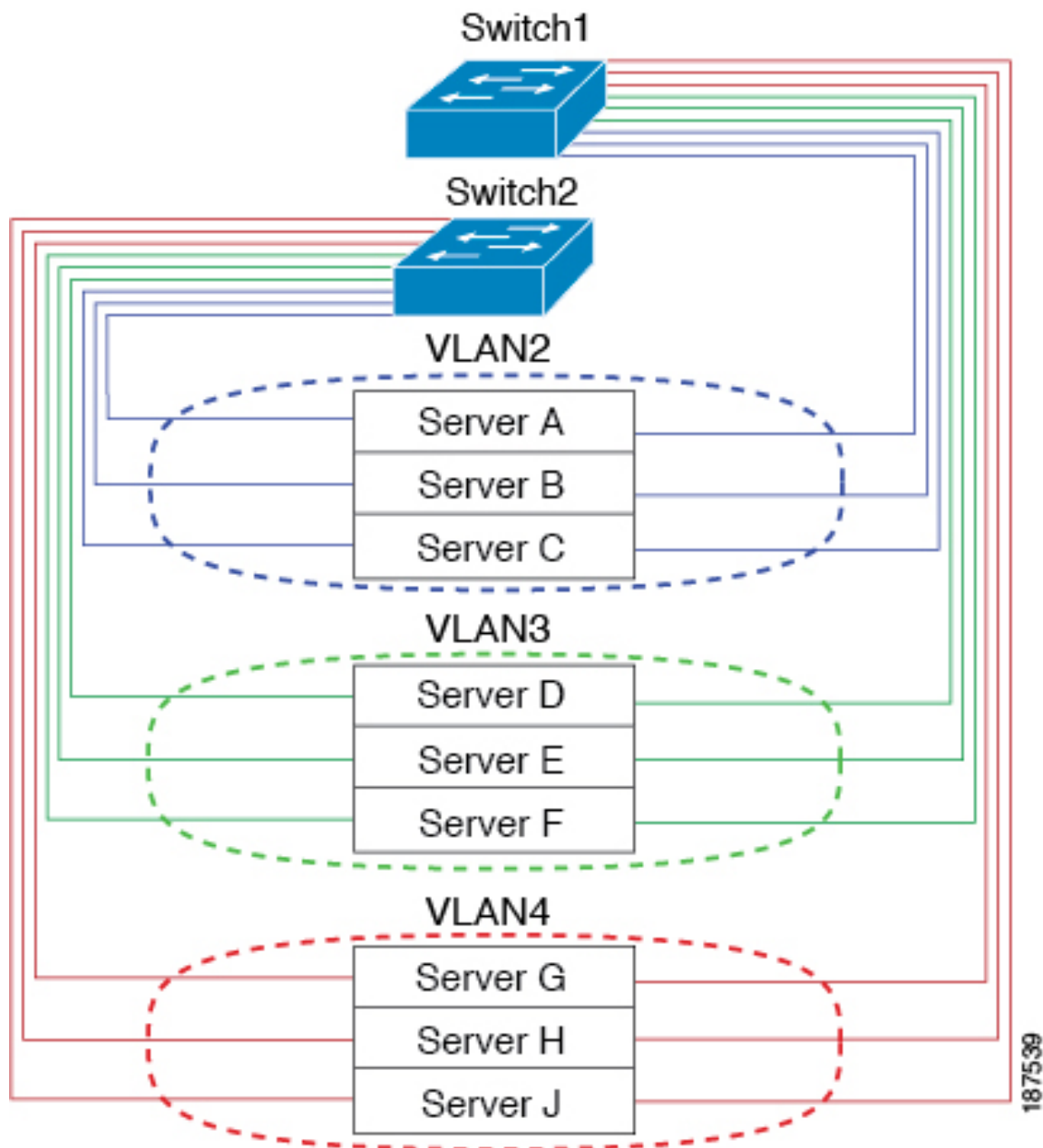
VLAN について

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 に属することができ、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 1: 論理的に定義されたネットワークとしての VLAN



VLANは通常、IPサブネットワーク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 の範囲



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

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

設定制限に関する詳細については、各スイッチに対応する設定制限についての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 2: 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 と 4048 ～ 4093	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。 <ul style="list-style-type: none">• ステータスは必ず、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 ～ 4047 と 4094	内部割り当て	これらの 80 の VLAN と VLAN 4094 は、内部デバイス用に割り当てられています。内部使用のために予約されたブロック内にある VLAN は、作成、削除、および変更はできません。

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。予約グループの VLAN の使用、変更、削除はできません。内部的に割り当てられている VLAN、およびそれに関連した用途は表示できます。

VLAN の作成、削除、変更

VLAN には 1 ～ 4094 の番号が付けられます。スイッチを初めて起動したとき、すべての設定済みポートはデフォルト VLAN に属します。デフォルト VLAN (VLAN1) では、デフォルト値のみ使用されます。デフォルト VLAN では、アクティビティの作成、削除、および一時停止は行えません。

VLAN を作成する際は、その VLAN に番号を割り当てます。VLAN は削除することもできますが、アクティブ動作ステートから一時停止動作ステートに移行することもできます。既存の VLAN ID で VLAN を作成しようとすると、スイッチは VLAN サブモードになりますが、同一の VLAN は再作成しません。

新しく作成した VLAN は、その VLAN にポートが割り当てられるまで使用されません。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
- シャットダウンまたは非シャットダウン

特定の VLAN を削除すると、その VLAN に関連するポートはシャットダウンされ、トラフィックは流れなくなります。ただし、システムではその VLAN の VLAN/ポート マッピングがすべて維持されるため、その VLAN の再イネーブル化や再作成を行うと、その VLAN の元のポートはすべて自動的に回復します。



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す。

VLAN 3968 ~ 4049 および 4094 は内部使用に予約されています。これらの VLAN の変更または使用はできません。

VLAN トランッキング プロトコルについて

VLAN トランッキング プロトコル（VTP）は、ドメイン間で VTP VLAN データベースを同期するための分散 VLAN データベース管理プロトコルです。VTP ドメインは 1 つ以上のネットワーク スイッチで構成されます。これらのネットワーク スイッチは同じ VTP ドメイン名を共有し、トランク インターフェイスで接続されます。

VTP の注意事項と制約事項

VTP 設定時の注意事項と制約事項は次のとおりです。

- 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 をイネーブルにした場合、バージョン 1 またはバージョン 2 のいずれかを設定する必要があります。
- **system vlan long-name** ノブが有効になっている場合、VTP 構成は OFF モードで表示され、ユーザーはモードを透過に変更できます。ただし、モードをサーバーまたはクライアントに変更することはできません。
- **show running-configuration** コマンドを実行しても、1 ~ 1000 の VLAN に関する VLAN 構成情報や VTP 設定情報は表示されません。

- VTP をトークン リング環境で使用している場合は、バージョン 2 を使用する必要があります。
- VTPv3 プルーニングは、Cisco Nexus 9000 スイッチでサポートされています。
- 予約済み VLAN 範囲を変更した後は、**copy running-config startup-config** コマンドを入力してからリロードする必要があります。例：

```
switch(config)# system vlan 2000 reserve
This will delete all configs on vlans 2000-2081. Continue anyway? (y/n) [no] y
```

スイッチのリロード後、VLAN 2000 ～ 2081 は内部使用のために予約されます。そのため、スイッチのリロード前に **copy running-config startup-config** コマンドを入力する必要があります。この範囲内の VLAN を作成することはできません。

- SNMP は CISCO-VTP-MIB オブジェクト上で GET および SET 操作を実行できます。
- VTP サーバ モードおよび VTP クライアント モードはサポートされていません。サポートされているモードは、デフォルト モードである透明モードだけです。
- SNMP では、VTP 機能がイネーブルかどうかは `vlanTrunkPortVtpEnabled` オブジェクトによって示されます。

VLAN の設定

VLAN の作成および削除

デフォルト VLAN およびスイッチによる使用のために内部的に割り当てられている VLAN を除き、すべての VLAN は、作成または削除が可能です。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 にアソシエートされたポートはシャットダウンします。トラフィックは流れなくなり、パケットはドロップされます。



Note 507 を超える VLAN を設定するには、スパニング ツリー プロトコル MST モードを設定する必要があります。スケーラビリティの数値については、[*Cisco Nexus 3548 Switch NX-OS 確認済み 拡張性ガイド*、リリース 6.x (Cisco Nexus 3548 Switch NX-OS Verified Scalability Guide, Release 6.x)] を参照してください。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vlan** {vlan-id | vlan-range}

3. switch(config-vlan)# no vlan {vlan-id | vlan-range}

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# vlan {vlan-id vlan-range}	<p>単独の VLAN またはある範囲に属する複数の VLAN を作成します。</p> <p>VLAN にすでに割り当てられている番号を入力すると、スイッチはその VLAN の VLAN 構成サブモードに移動し、開始します。内部的に割り当てられている VLAN に割り当てられている番号を入力すると、エラーメッセージが返されます。VLAN の範囲を入力し、指定 VLAN の 1 つ以上が、内部的に割り当てられた VLAN の範囲外である場合、コマンドは範囲外の VLAN だけで有効になります。指定できる範囲は 2 ～ 4094 です。VLAN1 はデフォルト VLAN であり、作成や削除はできません。内部使用のために予約されている VLAN の作成や削除はできません。</p>
Step 3	switch(config-vlan)# no vlan {vlan-id vlan-range}	<p>指定した VLAN または VLAN の範囲を削除し、VLAN コンフィギュレーション サブモードを終了します。</p> <p>VLAN1 または内部的に割り当てられている VLAN は削除できません。</p>

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# configure terminal
switch(config)# vlan 15-20
```



Note VLAN 構成サブモードで VLAN の作成と削除を行うこともできます。

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



Note VLAN 名は、短い名前 (最大 32 文字) または長い名前 (最大 128 文字) のいずれかです。最大 128 文字の VLAN ロング ネームを設定するには、**system vlan long-name** コマンドをイネーブルにする必要があります。

- 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. switch# **configure terminal**
2. switch(config)# **vlan** {vlan-id | vlan-range}
3. switch(config-vlan)# **name** vlan-name
4. switch(config-vlan)# **state** {active | suspend}
5. (Optional) switch(config-vlan)# **no shutdown**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# vlan {vlan-id vlan-range}	VLAN コンフィギュレーション サブモードを開始します。VLAN が存在しない場合は、先に指定 VLAN が作成されます。
Step 3	switch(config-vlan)# name vlan-name	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。
Step 4	switch(config-vlan)# state {active suspend}	VLAN のステート（アクティブまたは一時停止）を設定します。VLAN ステートを一時停止（suspended）にすると、その VLAN に関連付けられたポートがシャットダウンし、VLAN のトラフィック転送が停止します。デフォルトステートはactiveです。デフォルト VLAN および VLAN 1006 ~ 4094 のステートを一時停止にすることはできません。

	Command or Action	Purpose
Step 5	(Optional) 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 （つまりイネーブル）です。デフォルト VLAN の VLAN1、または VLAN 1006 ~ 4094 はシャットダウンできません。

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# configure terminal
switch(config)# vlan 5
switch(config-vlan)# name accounting
switch(config-vlan)# state active
switch(config-vlan)# no shutdown
```

VLAN へのポートの追加

VLAN の設定が完了したら、ポートを割り当てます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** {*ethernet slot/port* | **port-channel number**}
3. switch(config-if)# **switchport access vlan** *vlan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface { <i>ethernet slot/port</i> port-channel number }	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。インターフェイスは、物理イーサネット ポートでも EtherChannel でもかまいません。
Step 3	switch(config-if)# switchport access vlan <i>vlan-id</i>	インターフェイスのアクセス モードを指定 VLAN に設定します。

Example

次の例は、VLAN5に参加するようにイーサネットインターフェイスを設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/13
switch(config-if)# switchport access vlan 5
```

ルーテッド SVI としての VLAN の設定

ルーテッド スイッチ仮想インターフェイス（SVI）となるように VLAN を設定できます。

始める前に

- レイヤ 3 ライセンスをインストールします。
- この機能の注意事項および制限事項を必ず理解するようにしてください。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature interface-vlan**
3. switch(config)# **interface-vlan vlan-id**
4. switch(config-if)# **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
Step 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。
Step 2	switch(config)# feature interface-vlan	SVI の作成をイネーブルにします。
Step 3	switch(config)# interface-vlan vlan-id	VLAN インターフェイス（SVI）を作成し、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。
Step 4	switch(config-if)# 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、VLAN をルーテッド SVI として設定する例を示します。

```
switch# configure terminal
switch(config)# feature interface-vlan
switch(config)# interface vlan 5
switch(config-if)# copy running-config startup-config
switch(config-if)#
```

次に、VLAN からルーテッド SVI 機能を削除する例を示します。

```
switch# configure terminal
switch(config)# no interface vlan 5
switch(config-if)# copy running-config startup-config
switch(config-if)#
```

次のタスク

このインターフェイスでルーティング プロトコルを設定できます。

管理 SVI としての VLAN の設定

管理スイッチ仮想インターフェイス（SVI）となるように VLAN を設定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature interface-vlan**
3. switch(config)# **interface-vlan *vlan-id* management**
4. switch(config-if)# **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
Step 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。
Step 2	switch(config)# feature interface-vlan	SVI の作成をイネーブルにします。
Step 3	switch(config)# interface-vlan <i>vlan-id</i> management	VLAN インターフェイス（SVI）を作成し、SVI をインバンド管理に使用するように設定します。
Step 4	switch(config-if)# 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、VLAN を管理 SVI として設定する例を示します。

```
switch# configure terminal
switch(config)# feature interface-vlan
switch(config)# interface vlan 5
switch(config-if)# management
switch(config-if)# copy running-config startup-config
switch(config-if)#
```

次に、SVI から管理機能を削除する例を示します。

```
switch# configure terminal
switch(config)# interface vlan 5
switch(config-if)# no management
switch(config-if)# copy running-config startup-config
switch(config-if)#
```

VTP の設定

[VTP をイネーブルにして設定できます。（You can enable and configure VTP）] VTP をイネーブルにした場合、バージョン 1 またはバージョン 2 のいずれかを設定する必要があります。VTP をトークンリング環境で使用している場合は、バージョン 2 を使用する必要があります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature vtp**
3. switch(config)# **vtp domain** *domain-name*
4. switch(config)# **vtp version** {1 | 2}
5. switch(config)# **vtp file** *file-name*
6. switch(config)# パスワード値 **vtp password**
7. switch(config)# **exit**
8. （任意）switch# **show vtp status**
9. （任意）switch# **show vtp counters**
10. （任意）switch# **show vtp interface**
11. （任意）switch# **show vtp password**
12. （任意）switch# **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
Step 1	switch# configure terminal	グローバル構成モードを開始します。

	コマンドまたはアクション	目的
Step 2	switch(config)# feature vtp	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。
Step 3	switch(config)# vtp domain <i>domain-name</i>	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。
Step 4	switch(config)# vtp version {1 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。
Step 5	switch(config)# vtp file <i>file-name</i>	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。
Step 6	switch(config)# パスワード値 vtp password	VTP 管理ドメイン用のパスワードを指定します。
Step 7	switch(config)# exit	コンフィギュレーションサブモードを終了します。
Step 8	(任意) 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。
Step 9	(任意) 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。
Step 10	(任意) switch# show vtp interface	VTP-enabled インターフェイスのリストを表示します。
Step 11	(任意) switch# show vtp password	管理 VTP ドメイン用のパスワードを表示します。
Step 12	(任意) 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。

例

次に、デバイスの VTP を設定する例を示します。

```
switch# configure terminal
switch(config)# feature vtp
switch(config)# vtp domain accounting
switch(config)# vtp version 2
switch(config)# exit
switch#
```

次の例は、VTP ステータスを表示したものです。スイッチがバージョン 2 をサポート可能であること、およびスイッチが現在バージョン 1 を実行していることがわかります。

```
switch(config)# show vtp status
VTP Status Information
-----
VTP Version                : 2 (capable)
Configuration Revision      : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs    : 502
```



```

VTP Operating Mode           : Transparent
VTP Domain Name             :
VTP Pruning Mode            : Disabled (Operationally Disabled)
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 Digest                  : 0xF5 0xF1 0xEC 0xE7 0x29 0x0C 0x2D 0x01
Configuration last modified by 60.10.10.1 at 0-0-00 00:00:00
VTP version running         : 1

```

VLAN の設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
switch# show running-config vlan [vlan_id vlan_range]	VLAN 情報を表示します。
switch# show vlan [brief id [vlan_id vlan_range] name name summary]	定義済み VLAN の選択した設定情報を表示します。

VLAN の機能履歴

機能名	リリース	機能情報
CISCO-VTP-MIB	5.0(3)U4(1)	この MIB オブジェクトのサポートが追加されました。



第 4 章

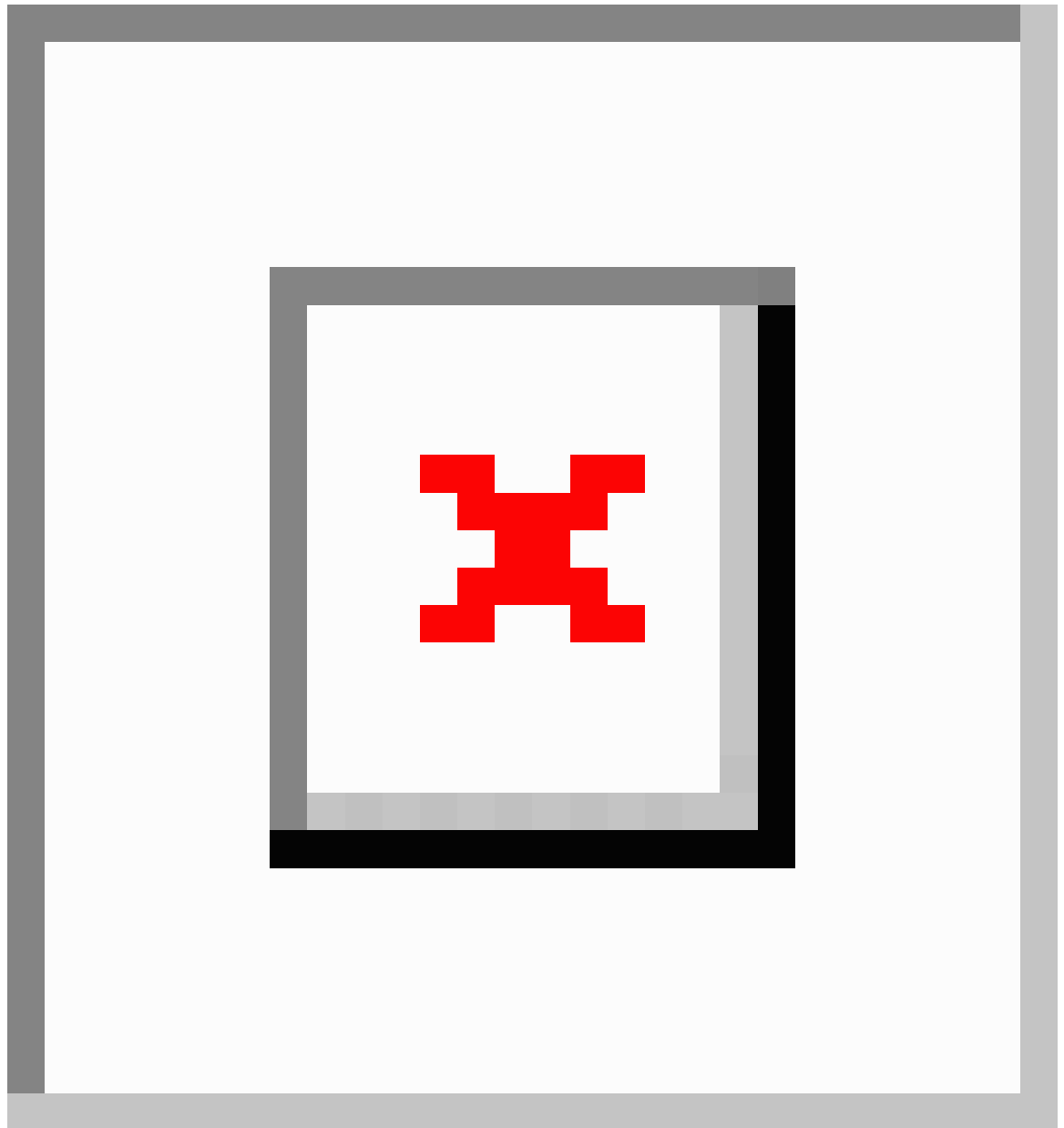
プライベート VLAN の設定

- プライベート VLAN について, on page 21
- プライベート VLAN の設定に関する注意事項と制約事項 (28 ページ)
- プライベート VLAN の設定 (28 ページ)
- プライベート VLAN 設定の確認, on page 43

プライベート VLAN について

プライベート VLAN (PVLAN) では VLAN のイーサネットブロードキャストドメインがサブドメインに分割されるため、スイッチ上のポートを互いに分離することができます。サブドメインは、1つのプライマリ VLAN と 1つ以上のセカンダリ VLAN とで構成されます (次の図を参照)。1つの PVLAN に含まれる VLAN はすべて、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。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、そのプライマリ VLAN 上でアソシエートされている無差別ポートのみと通信できます。コミュニティ VLAN 上のホストは、それぞれのホスト間およびアソシエートされている無差別ポートと通信できますが、他のコミュニティ VLAN にあるポートとは通信できません。

Figure 2: プライベート VLAN ドメイン



Note

VLAN をプライマリまたはセカンダリの PVLAN に変換する場合は、あらかじめその 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 ドメインには、プライマリ VLAN が 1 つのみ含まれています。プライベート VLAN ドメインの各ポートは、プライマリ VLAN のメンバーです。プライマリ VLAN は、プライベート VLAN ドメイン全体です。

セカンダリ VLAN は、同じプライベート VLAN ドメイン内のポート間を分離します。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 レベルで直接かつ相互には通信できません。
- **コミュニティ VLAN:** コミュニティ VLAN 内のポートは相互通信できますが、他のコミュニティ VLAN またはレイヤ 2 レベルの独立 VLAN にあるポートとは通信できません。

プライベート VLAN ポート

PVLAN ポートには、次の 3 種類があります。

- **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、複数のセカンダリ VLAN を関連付けることができるほか、セカンダリ VLAN をまったく関連付けないことも可能です。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。ロード バランシングまたは冗長性を持たせる目的で、これを行う必要が生じる場合があります。無差別ポートとアソシエートされていないセカンダリ VLAN も、含めることができます。

無差別ポートはアクセス ポートとして構成できます。

- **独立ポート:** 独立ポートは、セカンダリ独立 VLAN に属するポートです。このポートは、同じ PVLAN ドメイン内の他のポートから完全に独立しています。ただし、関連付けられている無差別ポートと通信することはできます。PVLAN 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。指定した独立 VLAN には、複数の独立ポートを含めることができます。各ポートは、独立 VLAN にある他のすべてのポートから、完全に隔離されています。

独立ポートはアクセス ポートとして構成できます。

- **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すべてのインターフェイス、および PVLAN ドメイン内のすべての独立ポートから分離されています。

コミュニティ ポートは、アクセス ポートとして設定する必要があります。

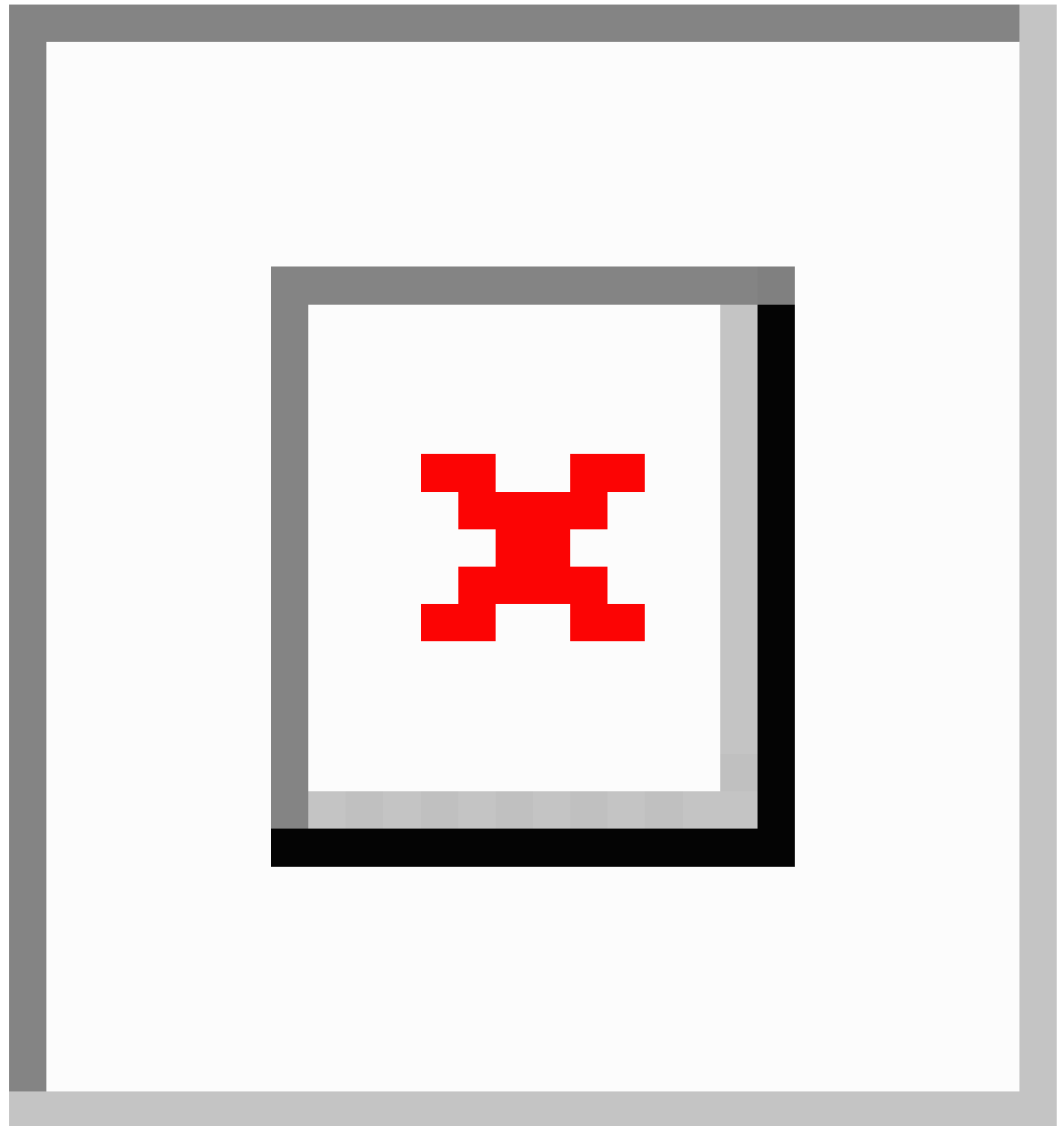
プライマリ、独立、およびコミュニティ プライベート VLAN

プライマリ VLAN および 2 つのタイプのセカンダリ VLAN（独立 VLAN とコミュニティ VLAN）には、次のような特徴があります。

- **プライマリ VLAN:** 独立ポートおよびコミュニティポートであるホストポート、および他の無差別ポートに、無差別ポートからトラフィックを伝送します。
- **独立 VLAN:** ホストから無差別ポートにアップストリームに単方向トラフィックを伝送するセカンダリ VLAN です。1 つの PVLAN ドメイン内で設定できる独立 VLAN は 1 つだけです。独立 VLAN では、複数の独立ポートを使用できます。各独立ポートからのトラフィックも、完全に隔離された状態が維持されます。
- **コミュニティ VLAN:** コミュニティ VLAN は、コミュニティポートから、無差別ポートおよび同じコミュニティにある他のホストポートへ、アップストリームトラフィックを送信するセカンダリ VLAN です。1 つの PVLAN ドメインには、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。

次の図は、PVLAN 内でのトラフィック フローを VLAN およびポートのタイプ別に示したものです。

Figure 3: プライベート VLAN のトラフィック フロー



Note PVLAN 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。プライマリ VLAN で受信したトラフィックによって隔離は行われず、転送は通常の VLAN として実行されます。

無差別アクセス ポートでは、ただ 1 つのプライマリ VLAN と複数のセカンダリ VLAN（コミュニティ VLAN および独立 VLAN）を処理できます。無差別ポートを使用すると、さまざまなデバイスを PVLAN への「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 PVLAN サー

バ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。

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 PVLAN 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。

セカンダリ VLAN とプライマリ プライベート VLAN の関連付け

セカンダリ VLAN をプライマリ VLAN とアソシエートするときには、次の事項に注意してください。

- *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、コミュニティ VALN ID を複数指定できるほか、独立 VLAN ID も 1 つ指定することができます。
- セカンダリ VLAN をプライマリ VLAN に関連付けるには、*secondary-vlan-list* パラメータを入力するか、または *secondary-vlan-list* パラメータを指定して **add** キーワードを使用します。
- セカンダリ VLAN とプライマリ VLAN 間の関連付けを消去するには、*secondary-vlan-list* パラメータを指定して **remove** キーワードを使用します。
- 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 とセカンダリ VLAN のいずれかを削除した場合、関連付けが設定されているポート上では、その VLAN は非アクティブになります。**no private-vlan** コマンドを入力すると、VLAN は通常の VLAN モードに戻ります。その VLAN におけるプライマリとセカンダリ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 PVLAN モードのままです。指定した VLAN を PVLAN モードに再変換すると、関連付けも元の状態に戻ります。

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 PVLAN は失われます。ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN と PVLAN と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、関連付けは復活します。

Before you begin

PVLAN 機能がイネーブルであることを確認します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vlan primary-vlan-id**
3. switch(config-vlan)# **private-vlan association** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}
4. (Optional) switch(config-vlan)# **no private-vlan association**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# vlan <i>primary-vlan-id</i>	PVLAN の設定作業を行うプライマリ VLAN の番号を入力します。
Step 3	switch(config-vlan)# private-vlan association {[add] <i>secondary-vlan-list</i> remove <i>secondary-vlan-list</i> }	セカンダリ VLAN をプライマリ VLAN に関連付けます。セカンダリ VLAN とプライマリ VLAN 間の関連付けを消去するには、 <i>secondary-vlan-list</i> パラメータを指定して remove キーワードを使用します。
Step 4	(Optional) switch(config-vlan)# no private-vlan association	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。

Example

次の例は、コミュニティ VLAN 100 ～ 110 および独立 VLAN 200 をプライマリ VLAN 5 に関連付ける方法を示したものです。

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# private-vlan association 100-110, 200
```

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、プライマリ VLAN で、無差別ポートからすべてのポート（コミュニティ VLAN と独立 VLAN にあるすべてのポートも含む）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。
- 独立ポートからのブロードキャストトラフィックは、独立ポートにアソシエートされているプライマリ VLAN にある無差別ポートにのみ配信されます。
- 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

PVLAN 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。

- 通信を防止するには、エンドステーションに接続されているインターフェイスのうち、選択したインターフェイスを、独立ポートとして設定します。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、サーバ間の通信が防止されます。
- 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 の設定に関する注意事項と制約事項

PVLAN を設定する場合は、次の注意事項に従ってください。

- 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。
- スイッチで 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。
- IGMP は、プライマリ VLAN 上でのみ実行され、すべてのセカンダリ VLAN にプライマリ VLAN の設定が使用されます。
- セカンダリ VLAN 内の IGMP 加入要求は、プライマリ VLAN で受信されたものとして処理されます。
- PVLAN モードで動作しているポートがスイッチにある場合、PVLAN をディセーブルにすることはできません。
- マルチ スパニングツリー（MST）リージョン定義内から **[private-vlan の同期（private-vlan synchronize）]** コマンドを実行すると、プライマリ VLAN と同じ MST インスタンスにセカンダリ VLAN をマップすることができます。
- 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。無差別または隔離された PVLAN トランクは、ホストスイッチでのみサポートされます。

プライベート VLAN の設定

プライベート VLAN のイネーブル化

PVLAN 機能を使用するためには、スイッチ上で PVLAN をイネーブルにする必要があります。



Note PVLAN コマンドは、PVLAN 機能をイネーブルにするまで表示されません。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **feature private-vlan**
3. (Optional) switch(config)# **no feature private-vlan**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# feature private-vlan	スイッチの PVLAN 機能をイネーブルにします。
Step 3	(Optional) switch(config)# no feature private-vlan	スwitchの PVLAN 機能をディセーブルにします。 Note スイッチ上に PVLAN モードで動作しているポートがある場合は、PVLAN をディセーブルにすることはできません。

Example

次の例は、スイッチの PVLAN 機能をイネーブルにする方法を示したものです。

```
switch# configure terminal
switch(config)# feature private-vlan
```

プライベート VLAN 上での IGMP スヌーピングのイネーブル化

Cisco NX-OS リリース 10.2 (2) 以降、プライベート VLAN で IGMP スヌーピングを有効にできます。

手順

	コマンドまたはアクション	目的
Step 1	switch(config)# feature private-vlan	スイッチの PVLAN 機能をイネーブルにします。

	コマンドまたはアクション	目的
Step 2	(任意) switch(config)# no system multicast pvlan route-replication	PVLANにある IGMP スヌーピング機能をイネーブル化します。No オプションは IGMP スヌーピング機能を無効化にします。

例

次に、PVLAN にある IGMP スヌーピング機能をイネーブル化にする例を示します。

```
switch# configure terminal
switch(config)# feature private-vlan
switch(config)# system multicast pvlan route-replication
```

プライベート VLAN としての VLAN の構成

PVLAN を作成するには、まず VLAN を作成したうえで、その VLAN を PVLAN として設定します。

Before you begin

PVLAN 機能がイネーブルであることを確認します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vlan** {vlan-id | vlan-range}
3. switch(config-vlan)# **private-vlan** {community | isolated | primary}
4. (Optional) switch(config-vlan)# **no private-vlan** {community | isolated | primary}

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# vlan {vlan-id vlan-range}	VLAN 設定サブモードにします。
Step 3	switch(config-vlan)# private-vlan {community isolated primary}	VLAN を、コミュニティ PVLAN、独立 PVLAN、またはプライマリ PVLAN として設定します。PVLAN には、プライマリ VLAN を 1 つ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。
Step 4	(Optional) switch(config-vlan)# no private-vlan {community isolated primary}	指定した VLAN から PVLAN 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

	Command or Action	Purpose
		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。

Example

次の例は、VLAN 5 をプライマリ VLAN として PVLAN に割り当てる方法を示したものです。

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# private-vlan primary
```

次の例は、VLAN 100 をコミュニティ VLAN として PVLAN に割り当てる方法を示したものです。

```
switch# configure terminal
switch(config)# vlan 100
switch(config-vlan)# private-vlan community
```

次の例は、VLAN 200 を隔離した VLAN として PVLAN に割り当てる方法を示したものです。

```
switch# configure terminal
switch(config)# vlan 200
switch(config-vlan)# private-vlan isolated
```

セカンダリ VLAN とプライマリ プライベート VLAN の関連付け

セカンダリ VLAN をプライマリ VLAN とアソシエートするときには、次の事項に注意してください。

- *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、コミュニティ VALNID を複数指定できるほか、独立 VLAN ID も 1 つ指定することができます。
- セカンダリ VLAN をプライマリ VLAN に関連付けるには、*secondary-vlan-list* パラメータを入力するか、または *secondary-vlan-list* パラメータを指定して **add** キーワードを使用します。
- セカンダリ VLAN とプライマリ VLAN 間の関連付けを消去するには、*secondary-vlan-list* パラメータを指定して **remove** キーワードを使用します。

- 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 とセカンダリ VLAN のいずれかを削除した場合、関連付けが設定されているポート上では、その VLAN は非アクティブになります。 **no private-vlan** コマンドを入力すると、VLAN は通常の VLAN モードに戻ります。その VLAN におけるプライマリとセカンダリ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 PVLAN モードのままです。指定した VLAN を PVLAN モードに再変換すると、関連付けも元の状態に戻ります。

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 PVLAN は失われます。ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN と PVLAN と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、関連付けは復活します。

Before you begin

PVLAN 機能がイネーブルであることを確認します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vlan primary-vlan-id**
3. switch(config-vlan)# **private-vlan association** {[add] secondary-vlan-list | **remove** secondary-vlan-list}
4. (Optional) switch(config-vlan)# **no private-vlan association**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# vlan primary-vlan-id	PVLAN の設定作業を行うプライマリ VLAN の番号を入力します。
Step 3	switch(config-vlan)# private-vlan association {[add] secondary-vlan-list remove secondary-vlan-list}	セカンダリ VLAN をプライマリ VLAN に関連付けます。セカンダリ VLAN とプライマリ VLAN 間の関連付けを消去するには、 <i>secondary-vlan-list</i> パラメータを指定して remove キーワードを使用します。
Step 4	(Optional) switch(config-vlan)# no private-vlan association	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。

Example

次の例は、コミュニティ VLAN 100 ～ 110 および独立 VLAN 200 をプライマリ VLAN 5 に関連付ける方法を示したものです。

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# private-vlan association 100-110, 200
```

プライベート VLAN ホスト ポートとしてのインターフェイスの設定

PVLAN では、ホスト ポートはセカンダリ VLAN の一部であり、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。PVLAN のホスト ポートを設定する手順には 2 つのステップがあります。1 つ目はポートを PVLAN のホスト ポートとして定義すること、2 つ目はプライマリ VLAN とセカンダリ VLAN のホスト アソシエーションを設定することです。



Note ホスト ポートとして設定したすべてのインターフェイスで BPDU ガードをイネーブルにすることを推奨します。

Before you begin

PVLAN 機能がイネーブルであることを確認します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface type** [*chassis/*]*slot/port*
3. switch(config-if)# **switchport mode private-vlan host**
4. switch(config-if)# **switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*}
5. (Optional) switch(config-if)# **no switchport private-vlan host-association**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface type [<i>chassis/</i>] <i>slot/port</i>	PVLAN のホスト ポートとして設定するポートを選択します。このポートとしては、FEX のポートを選択できます (chassis オプションで指定)。
Step 3	switch(config-if)# switchport mode private-vlan host	選択したポートを PVLAN のホスト ポートとして設定します。
Step 4	switch(config-if)# switchport private-vlan host-association { <i>primary-vlan-id</i> } { <i>secondary-vlan-id</i> }	選択したポートを、PVLAN のプライマリ VLAN とセカンダリ VLAN に関連付けます。セカンダリ VLAN

	Command or Action	Purpose
		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。
Step 5	(Optional) switch(config-if)# no switchport private-vlan host-association	PVLAN の関連付けをポートから削除します。

Example

次の例は、PVLAN のホスト ポートとしてイーサネット ポート 1/12 を設定し、プライマリ VLAN 5 とセカンダリ VLAN 101 にそのポートを関連付ける方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/12
switch(config-if)# switchport mode private-vlan host
switch(config-if)# switchport private-vlan host-association 5 101
```

プライベート VLAN 無差別ポートとしてのインターフェイスの設定

PVLAN ドメインでは、無差別ポートはプライマリ VLAN の一部です。無差別ポートを設定する手順には2つのステップがあります。1つ目はポートを無差別ポートとして定義すること、2つ目はセカンダリ VLAN とプライマリ VLAN とのマッピングを設定することです。

Before you begin

PVLAN 機能がイネーブルであることを確認します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **switchport mode private-vlan promiscuous**
4. switch(config-if)# **switchport private-vlan mapping {primary-vlan-id} {secondary-vlan-list | add secondary-vlan-list | remove secondary-vlan-list}**
5. (Optional) switch(config-if)# **no switchport private-vlan mapping**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface type slot/port	PVLAN の無差別ポートとして設定するポートを選択します。物理インターフェイスが必要です。このポー

	Command or Action	Purpose
		トとして、FEX のポートを選択することはできません。
Step 3	switch(config-if)# switchport mode private-vlan promiscuous	選択したポートを PVLAN の無差別ポートとして設定します。物理イーサネット ポートのみを、無差別ポートとしてイネーブルにできます。
Step 4	switch(config-if)# switchport private-vlan mapping {primary-vlan-id} {secondary-vlan-list add secondary-vlan-list remove secondary-vlan-list}	ポートを無差別ポートとして設定し、プライマリ VLAN と、セカンダリ VLAN の選択リストに、指定したポートをアソシエートします。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかとして設定できます。
Step 5	(Optional) switch(config-if)# no switchport private-vlan mapping	PVLAN から、マッピングをクリアします。

Example

次の例は、プライマリ VLAN 5 およびセカンダリ独立 VLAN 200 に関連付けられた無差別ポートとしてイーサネット インターフェイス 1/4 を設定する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# switchport mode private-vlan promiscuous
switch(config-if)# switchport private-vlan mapping 5 200
```

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 独立トランク 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
Step 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。
Step 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。
Step 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。
Step 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。
Step 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
	<pre>switch(config-if)# switchport private-vlan trunk native vlan 5</pre>	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。
Step 6	<p>switchport private-vlan trunk allowed vlan {add vlan-list all except vlan-list none remove vlan-list}</p> <p>例:</p> <pre>switch(config-if)# switchport private-vlan trunk allowed vlan add 1 switch(config-if)#</pre>	<p>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。</p> <p>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。</p> <p>(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)。</p>
Step 7	<p>[no] switchport private-vlan association trunk {primary-vlan-id [secondary-vlan-id]}</p> <p>例:</p> <pre>switch(config-if)# switchport private-vlan association trunk 10 101 switch(config-if)#</pre>	<p>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。</p> <p>(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。</p> <p>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。</p>

	コマンドまたはアクション	目的
Step 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。
Step 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。
Step 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 secondary
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
Step 1	config t 例: <pre>switch# config t switch(config)#</pre>	コンフィギュレーション モードに入ります。
Step 2	interface <i>{type slot/port}</i> 例: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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。
Step 3	switchport 例: <pre>switch(config-if)# switchport switch(config-if)#</pre>	レイヤ 2 ポートをスイッチ ポートとして設定します。
Step 4	switchport mode private-vlan trunk promiscuous 例: <pre>switch(config-if)# switchport mode private-vlan trunk promiscuous switch(config-if)#</pre>	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 ポートとして設定します。
Step 5	(任意) switchport private-vlan trunk native vlan <i>vlan-id</i> 例: <pre>switch(config-if)# switchport private-vlan trunk native vlan 5</pre>	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
		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。
Step 6	switchport mode private-vlan trunk allowed vlan {add vlan-list all except vlan-list none remove vlan-list} 例: <pre>switch(config-if)# switchport private-vlan trunk allowed vlan add 1 switch(config-if)#</pre>	<p>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。</p> <p>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。</p> <p>(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）。</p>
Step 7	[no]switchport private-vlan mapping trunk primary-vlan-id [secondary-vlan-id] {add secondary-vlan-list remove secondary-vlan-id} 例: <pre>switch(config-if)# switchport private-vlan mapping trunk 4 add 5 switch(config-if)#</pre>	<p>無差別トランク ポートと、プライマリ VLAN および選択した関連するセカンダリ VLAN のリストをマッピングするかマッピングを削除します。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかとして設定できます。トラフィックを通過させるには、プライマリ VLAN とセカンダリ VLAN の間のプライベート VLAN の関連付けが動作する必要があります。各無差別トランク ポートに対し、最大 16 個のプライベート VLAN のプライマリとセカンダリのペアをマッピングできます。作業しているプライマリ VLAN それぞれに対してコマンドを再入力する必要があります。</p> <p>または</p> <p>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。</p>
Step 8	exit 例: <pre>switch(config-if)# exit switch(config)#</pre>	<p>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。</p>

	コマンドまたはアクション	目的
Step 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。
Step 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 2 add 3
switch(config-if)# switchport private-vlan mapping trunk 4 add 5
switch(config-if)# switchport private-vlan mapping trunk 1 add 20
switch(config-if)# exit
switch(config)#
```

プライマリ 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



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 7000 Series NX-OS インターフェイス構成ガイド]（Cisco Nexus 7000 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。
- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。VDC が異なっても同じ VLAN 名と ID を使用できるので、正しい VDC で作業していることを確認する必要があります。
- セカンダリ VLAN のマッピング先となる正しいプライマリ VLAN レイヤ 3 インターフェイスで作業をしていること。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	config t Example: switch# config t 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
Step 2	interface vlan <i>primary-vlan-ID</i> 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。
Step 3	次のいずれかのコマンドを入力します。	
	オプション	説明
	private-vlan mapping {[add] <i>secondary-vlan-list</i> remove <i>secondary-vlan-list</i>}	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。

	Command or Action		Purpose
	オプション	説明	
	no private-vlan mapping	セカンダリ VLAN とプライマリ VLAN 間のレイヤ 3 インターフェイスへのマッピングを消去します。	
	Example: switch(config-if) # private-vlan mapping 100-105, 109		
Step 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。
Step 5	(Optional) show interface vlan <i>primary-vlan-id</i> 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。
Step 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 設定の確認

PVLAN の設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
switch# show feature	スイッチでイネーブル化されている機能を表示します。

コマンド	目的
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。
switch# show vlan private-vlan [type]	PVLAN のステータスを表示します。

次の例は、PVLAN 設定の表示方法を示したものです。

```
switch# show vlan private-vlan
Primary Secondary Type Ports
-----
5 100 community
5 101 community Eth1/12, Eth100/1/1
5 102 community
5 110 community
5 200 isolated Eth1/2

switch# show vlan private-vlan type
Vlan Type
-----
5 primary
100 community
101 community
102 community
110 community
200 isolated
```

次の例は、イネーブル化されている機能の表示方法を示したものです（出力については一部割愛してあります）。

```
switch# show feature
Feature Name Instance State
-----
fcsp 1 enabled
...
interface-vlan 1 enabled
private-vlan 1 enabled
udld 1 disabled
...
```



第 5 章

アクセスインターフェイスとトランクインターフェイスの設定

- [アクセス インターフェイスとトランク インターフェイスについて \(45 ページ\)](#)
- [アクセス インターフェイスとトランク インターフェイスの設定 \(49 ページ\)](#)
- [インターフェイスの設定の確認, on page 55](#)

アクセス インターフェイスとトランク インターフェイスについて

アクセス インターフェイスとトランク インターフェイスの概要

イーサネット インターフェイスは、次のように、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。

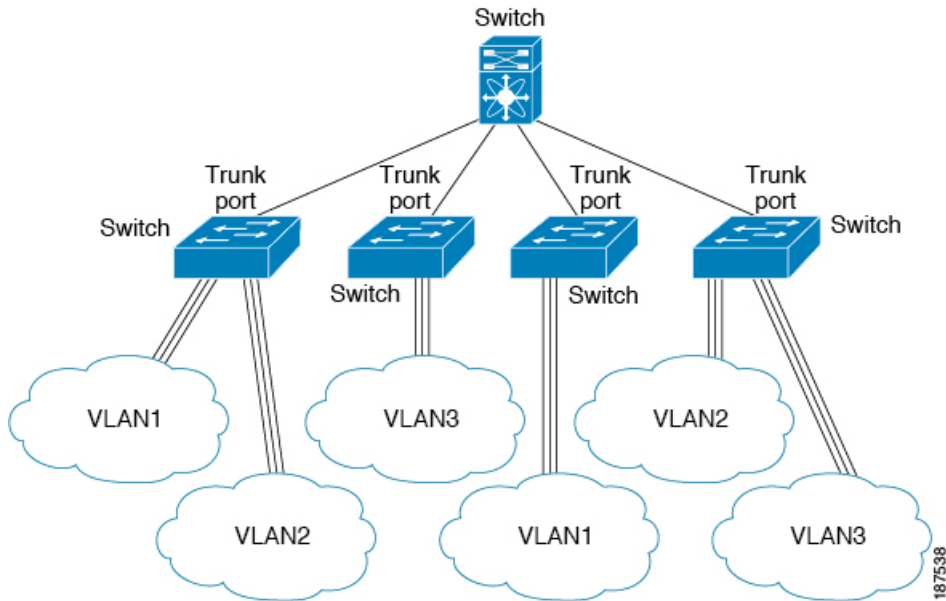
- アクセス ポートはインターフェイス上に設定された1つのVLAN だけに対応し、1つのVLAN のトラフィックだけを伝送します。
- トランク ポートはインターフェイス上に設定された2つ以上のVLAN に対応しているため、複数のVLAN のトラフィックを同時に伝送できます。



Note Cisco NX-OS では、IEEE 802.1Q タイプの VLAN トランク カプセル化だけをサポートしています。

次の図は、ネットワークにおけるトランク ポートの使い方を示したものです。トランク ポートは、2つ以上のVLAN のトラフィックを伝送します。

Figure 4: トランキング環境におけるデバイス



複数の VLAN に対応するトランク ポートでトラフィックが正しく送信されるようにするため、デバイスでは IEEE 802.1Q カプセル化（タギング）方式が使用されます。

アクセスポートでのパフォーマンスを最適化するには、そのポートをホストポートとして設定します。ホストポートとして設定されたポートは、自動的にアクセスポートとして設定され、チャネルグループ化はディセーブルになります。ホストポートを使用すると、指定ポートがパケットの転送を開始するための所要時間を短縮できます。



Note ホストポートとして設定できるのは端末だけです。端末以外のポートをホストとして設定しようとするとエラーになります。

アクセスポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元の MAC アドレスを学習せずにドロップします。



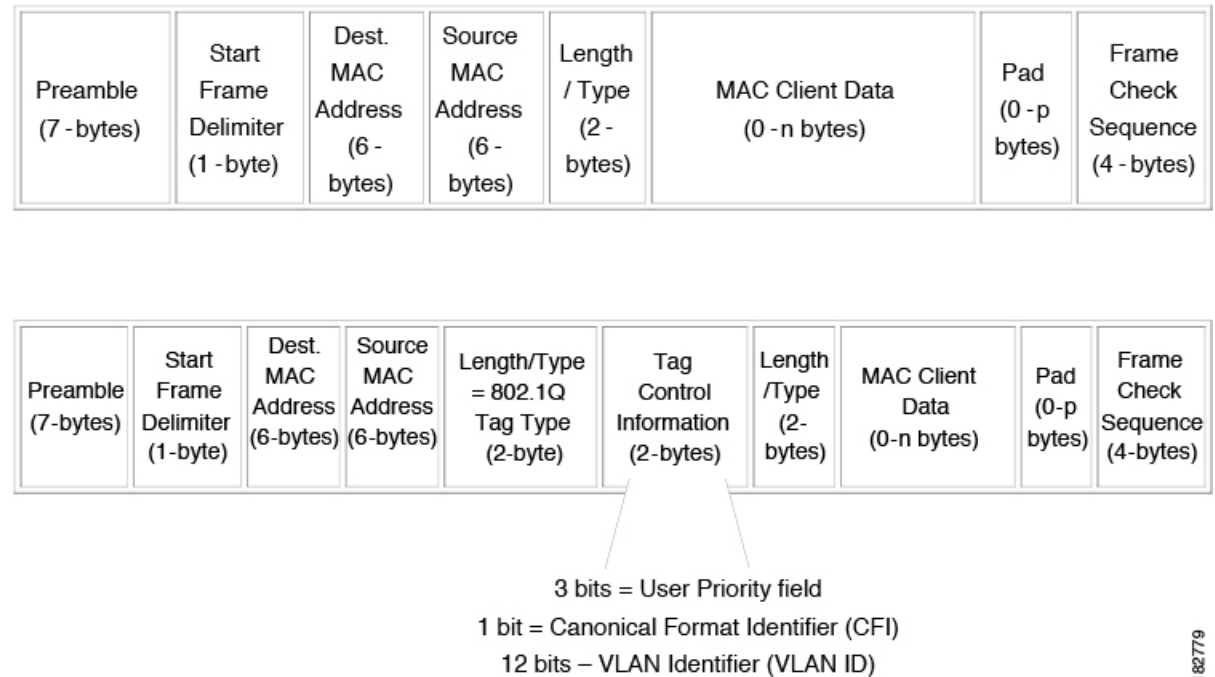
Note イーサネットインターフェイスはアクセスポートまたはトランクポートとして動作できますが、両方のポートタイプとして同時に動作することはできません。

IEEE 802.1Q カプセル化の概要

トランクは、デバイスと他のネットワークデバイス間のポイントツーポイントリンクです。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。

複数の VLAN に対応するトランク ポートでトラフィックが正しく送信されるようにするため、デバイスでは IEEE 802.1Q カプセル化（タギング）方式が使用されます。このタグには、そのフレームおよびパケットが属する特定の VLAN に関する情報が含まれます。タグ方式を使用すると、複数の異なる VLAN 用にカプセル化されたパケットが、同じポートを通過しても、各 VLAN のトラフィックを区別することができます。また、VLAN タグのカプセル化を使用すると、同じ VLAN 上のネットワークを経由するエンドツーエンドでトラフィックを転送できます。

Figure 5: 802.1Q タグが含まれているヘッダーと含まれていないヘッダー



182779

アクセス VLAN の概要

アクセス モードでポートを設定すると、そのインターフェイスのトラフィックを伝送する VLAN を指定できます。アクセス モードのポート（アクセス ポート）用に VLAN を設定しないと、そのインターフェイスはデフォルトの VLAN（VLAN1）のトラフィックだけを伝送します。

VLAN のアクセス ポート メンバーシップを変更するには、新しい VLAN を指定します。VLAN をアクセス ポートのアクセス VLAN として割り当てるには、まず、VLAN を作成する必要があります。アクセス ポート上のアクセス VLAN を、まだ作成されていない VLAN に変更すると、システムはそのアクセス ポートをシャット ダウンします。



Note

アクセス ポートまたはトランク ポートで VLAN を変更すると、インターフェイスがフラップします。ただし、ポートが vPC の一部である場合は、最初にセカンダリ vPC のネイティブ VLAN を変更してから、プライマリ vPC に変更します。

アクセス ポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元の MAC アドレスを学習せずにドロップします。

トランク ポートのネイティブ VLAN ID の概要

トランク ポートは、タグなしのパケットと 802.1Q タグ付きのパケットを同時に伝送できます。デフォルトのポート VLAN ID をトランク ポートに割り当てると、すべてのタグなしトラフィックが、そのトランク ポートのデフォルトのポート VLAN ID で伝送され、タグなしトラフィックはすべてこの VLAN に属するものと見なされます。この VLAN のことを、トランク ポートのネイティブ VLAN ID といいます。ネイティブ VLAN ID とは、トランク ポート上でタグなしトラフィックを伝送する VLAN のことです。

トランク ポートは、デフォルトのポート VLAN ID と同じ VLAN が設定された出力パケットをタグなしで送信します。他のすべての出力パケットは、トランク ポートによってタグ付けされます。ネイティブ VLAN ID を設定しないと、トランク ポートはデフォルト VLAN を使用します。



Note ネイティブ VLAN ID 番号は、トランクの両端で一致していなければなりません。

許可 VLAN の概要

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックを送受信します。各トランク上では、すべての VLAN ID が許可されます。この包括的なリストから VLAN を削除することによって、特定の VLAN からのトラフィックが、そのトランクを通過するのを禁止できます。トランク経由でトラフィックを伝送したい VLAN を後でリストに戻すこともできます。

デフォルト VLAN のスパニングツリープロトコル (STP) トポロジを区切るには、許可 VLAN のリストから VLAN1 を削除します。この分割を行わないと、VLAN1 (デフォルトでは、すべてのポートでイネーブル) が非常に大きな STP トポロジを形成し、STP の収束時に問題が発生する可能性があります。VLAN1 を削除すると、そのポート上で VLAN1 のデータトラフィックはすべてブロックされますが、制御トラフィックは通過し続けます。

ネイティブ 802.1Q VLAN の概要

802.1Q トランク ポートを通過するトラフィックのセキュリティを高めるため、**vlan dot1q tag native** コマンドが導入されました。この機能により、802.1Q トランク ポートから送信されるすべてのパケットが必ずタグ付けされるとともに、タグなしのパケットが 802.1Q トランク ポートで受信されないようにすることができるようになりました。

この機能がない場合、802.1Q トランク ポートで受信されたタグ付き入力フレームは、許可 VALN のリストに含まれる限り受信が許可され、それらのタグは維持されます。タグなしフレームについては、トランク ポートのネイティブ VLAN ID でタグ付けされたうえで、それ以降の処理が行われます。出力フレームは、その VLAN タグが 802.1Q トランク ポートで許可される範囲内に属する場合に限って受信されます。フレームの VLAN タグが、トランク ポートのネイティブ VLAN のタグと一致した場合、その VLAN タグは取り除かれ、フレームはタグなしで送信されます。

この動作は、ハッカーがフレームを別の VLAN へジャンプさせる「VLAN ホッピング」に利用される可能性があります。また、タグなしパケットを 802.1Q トランク ポートへ送信することにより、トラフィックをネイティブ VLAN の一部にすることもできます。

こうした問題を解決するため、**vlan dot1q tag native** コマンドでは次のような機能を実行できるようになっています。

- 入力側では、タグなしのデータ トラフィックをすべてドロップする。
- 出力側では、すべてのトラフィックをタグ付けする。ネイティブ VLAN に属するトラフィックは、ネイティブ VLAN ID でタグ付けされます。

この機能は、すべての直接接続されたイーサネット インターフェイスおよびポート チャネル インターフェイスでサポートされます。



(注) コマンドをイネーブルにするには、グローバル コンフィギュレーション モードで **vlan dot1q tag native** コマンドを入力します。

アクセスインターフェイスとトランクインターフェイスの設定

LAN インターフェイスをイーサネットアクセスポートとして設定する

イーサネット インターフェイスはアクセス ポートとして設定できます。アクセス ポートは、パケットを、1 つのタグなし VLAN 上だけで送信します。管理者は、そのインターフェイスで伝送する VLAN トラフィックを指定します。アクセスポートの VLAN を指定しないと、そのインターフェイスは、デフォルト VLAN だけのトラフィックを伝送します。デフォルトの VLAN は VLAN 1 です。

VLAN をアクセス VLAN として指定するには、その VLAN が存在しなければなりません。システムは、存在しないアクセス VLAN に割り当てられたアクセス ポートをシャット ダウンします。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *{{type slot/port}}* | **port-channel number**}
3. switch(config-if)# **switchport mode** *{access | trunk}*
4. switch(config-if)# **switchport access vlan** *vlan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface {{type slot/port} {port-channel number}}	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。
Step 3	switch(config-if)# switchport mode {access trunk}	トランキングなし、タグなしの単一 VLAN イーサネット インターフェイスとして、インターフェイスを設定します。アクセス ポートは、1 つの VLAN のトラフィックだけを伝送できます。デフォルトでは、アクセス ポートは VLAN1 のトラフィックを伝送します。異なる VLAN のトラフィックを伝送するようにアクセス ポートを設定するには、 switchport access vlan を使用します
Step 4	switch(config-if)# switchport access vlan vlan-id	このアクセスポートでトラフィックを伝送する VLAN を指定します。このコマンドを入力しないと、アクセス ポートは VLAN1 だけのトラフィックを伝送します。このコマンドを使用して、アクセス ポートがトラフィックを伝送する VLAN を変更できます。

Example

次に、指定された VLAN のみのトラフィックを送受信するイーサネットアクセスポートとしてインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/10
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
```

アクセス ホスト ポートの設定

スイッチポートホストを使用することにより、アクセスポートをスパンニングツリーエッジポートにすることが可能であり、BPDU フィルタリングおよび BPDU ガードを同時にイネーブルにすることができます。

Before you begin

設定を行うインターフェイスが適切であることを確認します。対象となるインターフェイスは、エンドステーションに接続されている必要があります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **switchport host**

DETAILED STEPS

Procedure		
	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface type slot/port	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。
Step 3	switch(config-if)# switchport host	Sets the interface to spanning-tree port type edge, turns on BPDU Filtering and BPDU Guard. Note このコマンドは、ホストに接続されたスイッチポートに対してのみ使用してください。

Example

次に、EtherChannel がディセーブルにされたイーサネット アクセス ホスト ポートとしてインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/10
switch(config-if)# switchport host
```

トランク ポートの設定

イーサネット ポートをトランク ポートとして設定できます。トランク ポートは、ネイティブ VLAN のタグなしパケット、および複数の VLAN のカプセル化されたタグ付きパケットを伝送します。



Note Cisco NX-OS は、IEEE 802.1Q カプセル化だけをサポートしています。

SUMMARY STEPS

1. switch# **configure terminal**

2. switch(config)# **interface** {*type slot/port* | **port-channel number**}
3. switch(config-if)# **switchport mode** {**access** | **trunk**}

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface { <i>type slot/port</i> port-channel number }	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。
Step 3	switch(config-if)# switchport mode { access trunk }	インターフェイスをイーサネット トランク ポートとして設定します。トランク ポートは、同じ物理リンクで 1 つ以上の VLAN 内のトラフィックを伝送できます（各 VLAN はトランッキングが許可された VLAN リストに基づいています）。デフォルトでは、トランク インターフェイスはすべての VLAN のトラフィックを伝送できます。特定のトランク上で特定の VLAN だけを許可するように指定するには、 switchport trunk allowed vlan コマンドを使用します。

Example

次の例は、インターフェイスをイーサネット トランク ポートとして設定する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport mode trunk
```

802.1Q トランク ポートのネイティブ VLAN の設定

このパラメータを設定しないと、トランク ポートは、デフォルト VLAN をネイティブ VLAN ID として使用します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** {*type slot/port* | **port-channel number**}
3. switch(config-if)# **switchport trunk native vlan** *vlan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface { <i>type slot/port</i> port-channel number }	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。
Step 3	switch(config-if)# switchport trunk native vlan vlan-id	802.1Q トランクのネイティブ VLAN を設定します。指定できる範囲は 1 ～ 4094 です（ただし、内部使用に予約されている VLAN は除きます）。デフォルト値は VLAN 1 です。

Example

次の例は、イーサネット トランク ポートに対してネイティブ VALN を設定する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport trunk native vlan 5
```

トランキング ポートの許可 VLAN の設定

特定のトランク ポートで許可されている VLAN の ID を指定できます。

指定トランク ポートの許可 VLAN を設定する前に、正しいインターフェイスを設定していること、およびそのインターフェイスがトランクであることを確認してください。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** {*type slot/port* | **port-channel number**}
3. switch(config-if)# **switchport trunk allowed vlan** {*vlan-list all* | **none** [**add** | **except** | **none** | **remove** {*vlan-list*}]}

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。

	Command or Action	Purpose
Step 2	switch(config)# interface { <i>type slot/port</i> port-channel number }	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。
Step 3	switch(config-if)# switchport trunk allowed vlan { <i>vlan-list all</i> <i>none</i> [<i>add</i> <i>except</i> <i>none</i> <i>remove</i> { <i>vlan-list</i> }]}	<p>トランク インターフェイスの許可 VLAN を設定します。デフォルトでは、トランク インターフェイス上のすべての VLAN（1 ～ 3967 および 4048 ～ 4094）が許可されます。VLAN 3968 ～ 4047 は、内部利用のためにデフォルトで予約されている VLAN です。この VLAN グループは設定できません。デフォルトでは、すべてのトランク インターフェイスですべての VLAN が許可されます。</p> <p>Note 内部で割り当て済みの VLAN を、トランク ポート上の許可 VLAN として追加することはできません。内部で割り当て済みの VLAN を、トランク ポートの許可 VLAN として登録しようとする、メッセージが返されます。</p>

Example

次の例は、イーサネット トランク ポートの許可 VLAN のリストにいくつかの VLAN を追加する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport trunk allow vlan 15-20
```

ネイティブ 802.1Q VLAN の設定

通常は、ネイティブ VLAN ID で 802.1Q トランクを設定します。これによって、その VLAN 上のすべてのパケットからタギングが取り除かれます。この設定は、すべてのタグなしトラフィックと制御トラフィックが Cisco Nexus デバイスを通過できるようにします。ネイティブ VLAN ID の値と一致する 802.1Q タグを持つ、スイッチに着信するパケットも、同様にタギングが取り除かれます。

ネイティブ VLAN でのタギングを維持し、タグなしトラフィックをドロップするには、**vlan dot1q tag native** コマンドを入力します。スイッチによって、ネイティブ VLAN で受信したトラフィックがタグ付けされ、802.1Q タグが付けられたフレームのみが許可され、ネイティブ VLAN のタグなしトラフィックを含むすべてのタグなしトラフィックはドロップされます。

vlan dot1q tag native コマンドがイネーブルになっていても、トランク ポートのネイティブ VLAN のタグなし制御トラフィックは引き続き許可されます。



(注) **vlan dot1q tag native** コマンドはグローバル ベースでイネーブルになります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vlan dot1q tag native [tx-only]**
3. (任意) switch(config)# **no vlan dot1q tag native [tx-only]**
4. (任意) switch# **show vlan dot1q tag native**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# vlan dot1q tag native [tx-only]	Cisco Nexus デバイス 上のすべてのトランク ポートのすべてのネイティブ VLAN の dot1q (IEEE 802.1Q) タギングをイネーブルにします。デフォルトでは、この機能は無効になっています。
Step 3	(任意) switch(config)# no vlan dot1q tag native [tx-only]	スイッチ上の全トランッキング ポートを対象に、そのネイティブ VLAN すべてに対して dot1q (IEEE 802.1Q) タギングをイネーブルにします。
Step 4	(任意) switch# show vlan dot1q tag native	ネイティブ VLAN のタギングのステータスを表示します。

例

次に、スイッチ上の 802.1Q タギングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# vlan dot1q tag native
switch(config)# exit
switch# show vlan dot1q tag native
vlan dot1q native tag is enabled
```

インターフェイスの設定の確認

アクセスおよびトランク インターフェイス設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
switch# show interface	インターフェイス設定を表示します。
switch# show interface switchport	すべてのイーサネット インターフェイス（アクセス インターフェイスとトランク インターフェイスを含む）の情報を表示します。
switch# show interface brief	インターフェイス設定情報を表示します。



第 6 章

Rapid PVST+ の設定

- [Rapid PVST+ について, on page 57](#)
- [Rapid PVST+ の設定, on page 74](#)
- [Rapid PVST+ 設定の確認, on page 86](#)

Rapid PVST+ について

Rapid PVST+ プロトコルは、VLAN 単位で実装される IEEE 802.1w 標準（高速スパン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 802.1D 標準と相互運用されます。

Rapid PVST+ は、デフォルト VLAN（VLAN1）と、ソフトウェアで新たに作成された新しい VLAN でデフォルトでイネーブルになります。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

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、「スパンニングツリー」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 についての概要

STP の概要

イーサネットネットワークが適切に動作するには、任意の 2 つのステーション間のアクティブパスは 1 つだけでなければなりません。

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 アルゴリズムでは、スイッチドネットワーク中で、ループのない最適のパスが計算されます。LAN ポートでは、定期的な間隔で、ブリッジプロトコルデータユニット（BPDU）と呼ばれる STP フレームの送受信が実行されます。

スイッチはこのフレームを転送しませんが、このフレームを使って、ループの発生しないパスを実現します。

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あると、エンドステーションがメッセージを重複して受信したり、複数の LAN ポートでエンドステーションの MAC アドレスをスイッチが認識してしまうことがあります。このような状態になるとブロードキャストストームが発生し、ネットワークが不安定になります。

STP では、ルートブリッジでツリーを定義し、ルートからネットワーク内のすべてのスイッチへ、ループのないパスを定義します。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。

スイッチの 2 つの LAN ポートで同じ MAC アドレスを認識することでループが発生している場合は、STP ポートのプライオリティとポート パス コストの設定により、フォワーディング ステートになるポートと、ブロッキング ステートになるポートが決定されます。

トポロジ形成の概要

スパニングツリーを構成している、拡張 LAN のスイッチはすべて、BPDU を交換することによって、ネットワーク内の他のスイッチについての情報を収集します。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witch 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。
- 冗長なインターフェイスをバックアップステートにする（スイッチドネットワークの任意の箇所からルート スwitch に到達するために必要としないパスをすべて STP ブロック ステートにする）ことにより、スイッチドネットワークのループをすべて解除します。

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。

- 各スイッチにアソシエートされている、スイッチの一意なスイッチ識別情報である MAC アドレス
- 各インターフェイスにアソシエートされているルートのパス コスト
- 各インターフェイスにアソシエートされているポートの識別情報

スイッチドネットワークでは、ルート スwitch 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 では、BPDU を使用して、スイッチドネットワークのルート スwitch やルート ポート、および、各スイッチドセグメントのルート ポートや指定ポートが選定されます。

ブリッジ ID の概要

それぞれのスイッチの各 VLAN には固有の 64 ビットブリッジ ID があります。この ID は、ブリッジプライオリティ値、拡張システム ID（IEEE 802.1t）、STP MAC アドレス割り当てから構成されます。

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。



Note Cisco NX-OS 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 はディセーブルにできません。

拡張システム ID を伴わない

12 ビットの拡張システム ID フィールドは、ブリッジ ID の一部です。

Figure 6: 拡張システム ID 付きのブリッジ ID



スイッチは 12 ビットの拡張システム ID を常に使用します。

システム ID の拡張は、ブリッジ ID と組み合わせられ、VLAN の一意の識別情報として機能します。

Table 3: 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 拡張システム ID と MAC アドレス削減は、ソフトウェア上で常にイネーブルです。

任意のスイッチの MAC アドレス削減がイネーブルの場合、不要なルートブリッジの選定とスパニングツリートポロジの問題を避けるため、他のすべての接続スイッチでも、MAC アドレス削減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。スイッチのブリッジ ID (最小の優先ルートブリッジを特定するために、スパニングツリーアルゴリズムによって使用される) は、4096 の倍数を指定します。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

同じスパンニングツリー ドメインにある別のブリッジで MAC アドレス削減機能が実行されていない場合、そのブリッジのブリッジ ID と、MAC アドレス削減機能で指定されている値のいずれかが一致する可能性があり、その場合はそのブリッジがルートブリッジとして機能することになります。

BPDU の概要

スイッチは STP インスタンス全体にブリッジプロトコルデータ ユニット (BPDU) を送信します。各スイッチにより、コンフィギュレーション BPDU が送信され、スパンニングツリー トポロジの通信が行われ、計算されます。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。

- 送信するスイッチによりルートブリッジが特定される、スイッチの一意なブリッジ ID
- ルートまでの STP パス コスト
- 送信側ブリッジのブリッジ ID
- メッセージ エージ
- 送信側ポートの 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

スイッチにより Rapid PVST+ BPDU フレームが送信されるときには、フレームの送信先の VLAN に接続されているすべてのスイッチで、BPDU を受信します。スイッチで BPDU を受信するときに、スイッチによりフレームは送信されませんが、フレームにある情報を使用して BPDU が計算されます。トポロジが変更される場合は、BPDU の送信が開始されます。

BPDU 交換によって次の処理が行われます。

- 1 つのスイッチがルートブリッジとして選択されます。
- ルートブリッジへの最短距離は、パスコストに基づいてスイッチごとに計算されます。
- LAN セグメントごとに指定ブリッジが選択されます。これは、ルートブリッジに最も近いスイッチで、そのスイッチを介してフレームがルートに転送されます。
- ルートポートが選択されます。これはブリッジからルートブリッジまでの最適パスを提供するポートです。
- 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

各 VLAN では、ブリッジ識別子の数値が最も小さいスイッチが、ルートブリッジとして選択されます。すべてのスイッチがデフォルトのプライオリティ（32768）で設定されている場合、その VLAN で最小の MAC アドレスを持つスイッチが、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。

ブリッジのプライオリティの値を変更すると、スイッチがルートブリッジとして選定される可能性を変更することになります。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。

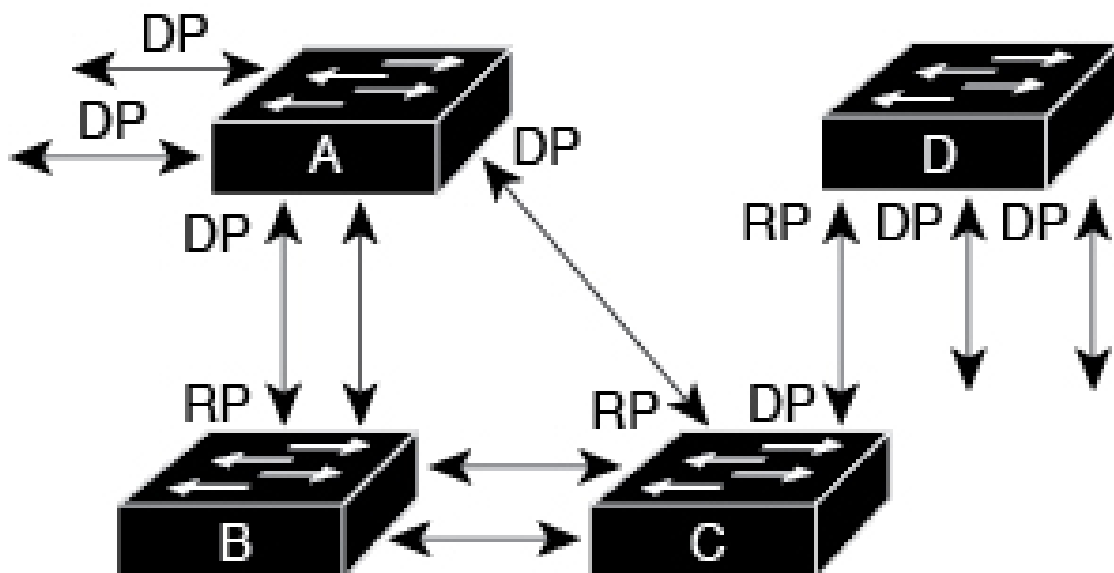
STP ルートブリッジは論理的に、ネットワークで各スパニングツリートポロジの中心です。ネットワークの任意の箇所からルートブリッジに到達するために必要ではないすべてのパスは、STP ブロッキングモードになります。

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 では、この情報を使用して、STP インスタンス用のルートブリッジを選定し、ルートブリッジに導くルートポートを選択し、各セグメントの指定ポートを特定します。

スパニングツリートポロジの作成

次の図では、スイッチ A がルートブリッジに選定されます。これは、すべてのスイッチ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。任意のスイッチのプライオリティを高くする（数値を小さくする）ことでそのスイッチがルートブリッジになるようにします。これにより STP が強制的に再計算され、そのスイッチをルートとする新しいスパニングツリートポロジが形成されます。

Figure 7: スパニングツリー トポロジ



RP = Root Port
DP = Designated Port

187026

スパニングツリー トポロジがデフォルトのパラメータに基づいて算出された場合、スイッチドネットワークの送信元エンドステーションから宛先エンドステーションまでのパスが最適にならない場合があります。たとえば、現在のルートポートよりも数値の大きいポートに高速リンクを接続すると、ルートポートが変更される場合があります。最高速のリンクをルートポートにすることが重要です。

たとえば、スイッチ B の 1 つのポートが光ファイバリンクであり、同じスイッチの別のポート（シールドなしツイストペア（UTP）リンク）がルートポートになっていると仮定します。ネットワークトラフィックを高速の光ファイバリンクに流した方が効率的です。光ファイバポートの STP ポートプライオリティをルートポートよりも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+ の概要

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 RapidPVST+ 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 Rapid PVST+ は、スイッチでのデフォルト STP モードです。

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）。



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。STP にある各指定ポートまたは各ルートポートにより、デフォルトで、2 秒ごとに BPDUs が送信されます。トポロジの指定ポートまたはルートポートで、hello メッセージが 3 回連続失われた場合、または、最大経過時間の期限が切れた場合、ポートでは、すべてのプロトコル情報がテーブルにただちにフラッシュされます。ポートでは、3 つの BPDUs が失われるか、最大経過時間の期限が切れた場合、直接のネイバールートまたは指定ポートへの接続が失われたと見なされます。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。スイッチは PVID を自動的に確認します。

Rapid PVST+ により、ネットワーク デバイス、スイッチ ポート、または LAN の障害の直後に、接続が迅速に回復されます。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 スイッチにあるエッジポートとしてポートを設定する場合、エッジポートでは、フォワーディングステートにただちに移行します（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。

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



Note ホストに接続されているすべてのポートを、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+ により新しいルートポートが選択された場合、古いポートがブロックされ、新しいルートポートがただちに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、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 BPD 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) BPD 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により、TC フラグがオンに設定された状態で BPD が送信されます。BPD 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。

- すべての非エッジルートポートと指定ポートで、必要に応じ、hello タイムの 2 倍の値で TC While タイマーが開始されます。
- 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。



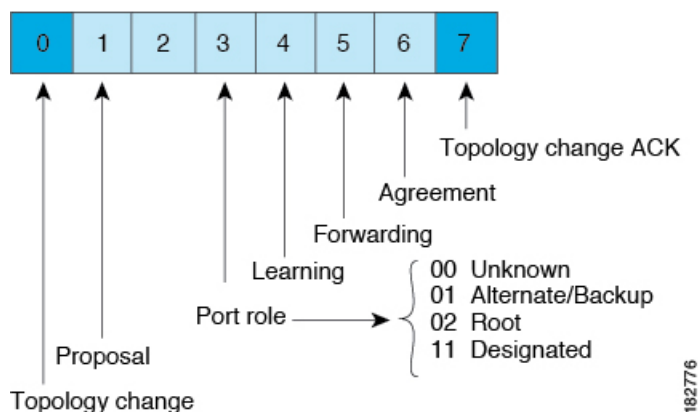
Note スイッチが、レガシー 802.1D STP を実行しているスイッチと相互に動作しているときにのみ、TCA フラグが使用されます。

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+ BPD

Rapid PVST+ と 802.1w では、フラグバイトの 6 ビットすべてを使用して、BPD の送信元のポートのロールおよびステートと、提案や合意のハンドシェイクが追加されます。次の図に、Rapid PVST+ の BPD フラグの使用法を示します。

Figure 8: BPD の Rapid PVST+ フラグ バイト

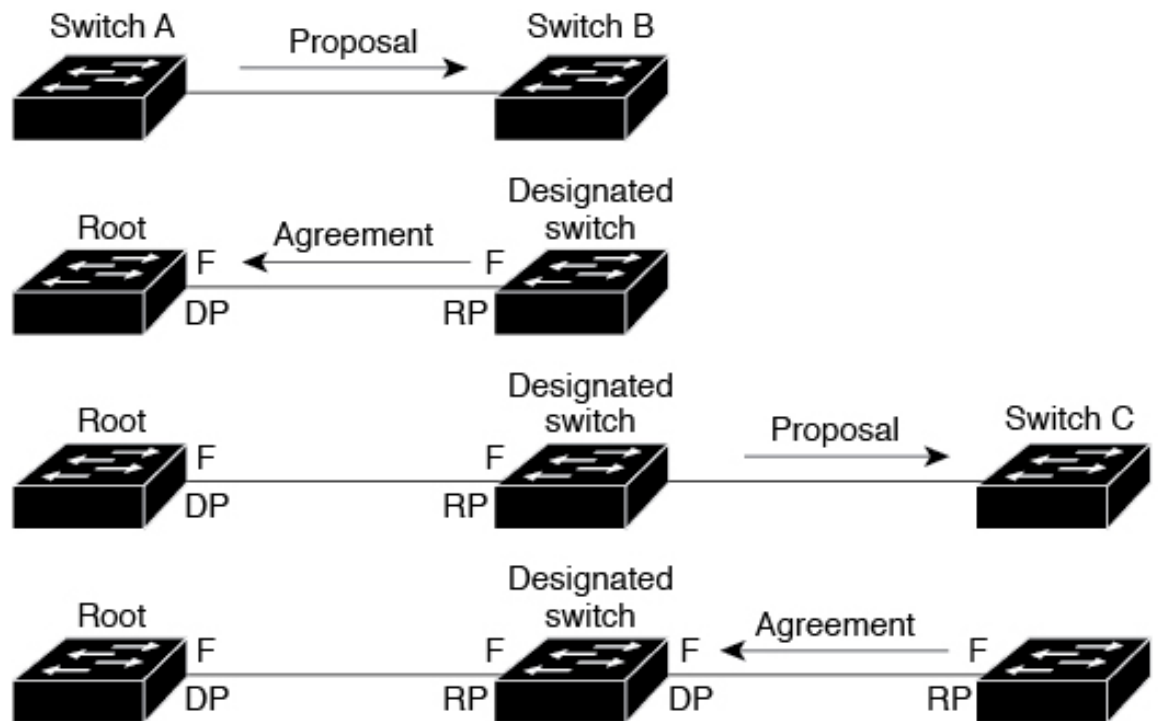


もう一つの重要な変更点は、Rapid PVST+ BPDU がタイプ 2、バージョン 2 であることで、これにより、スイッチでは、接続されているレガシー（802.1D）ブリッジを検出できるようになります。802.1D の BPDU は、バージョン 0 です。

提案と合意のハンドシェイク

次の図のように、スイッチ A は、ポイントツーポイントリンクを介してスイッチ B に接続され、すべてのポートがブロッキングステートになります。スイッチ A のプライオリティ値がスイッチ B のプライオリティ値より小さい数値である場合、

Figure 9: 高速コンバージェンスの提案と合意のハンドシェイク



スイッチ A はスイッチ B に提案メッセージ（提案フラグが設定されたコンフィギュレーション BPDU）を送信し、スイッチ A 自身が指定スイッチになることを提案します。

スイッチ B は、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ブロッキングステートにします。さらに、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 ですべての非エッジポートがブロックされ、ス

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ため、ネットワークではループが形成されることはありません。

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。このハンドシェイク処理の繰り返しごとに、さらに 1 つのネットワーク デバイスがアクティブなトポロジに参加します。ネットワークの収束のたびに、この提案と合意のハンドシェイクが、ルートからスパニングツリーの末端に向かって進みます。

スイッチは、ポート デュプレックス モードからリンク タイプを認識します。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。

spanning-tree link-type インターフェイス コンフィギュレーション コマンドを入力すると、デュプレックス設定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。

この提案合意ハンドシェイクが開始されるのは、非エッジ ポートがブロッキング ステートからフォワーディング ステートに移行するときだけです。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 4: Rapid PVST+ プロトコル タイマー

変数	説明
ハロー タイマー	各スイッチから他のスイッチに 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、バックアップとして使用されます。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スイッチで保存される時間を決めます。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、最も高いプライオリティ（最小プライオリティ値）を持つスイッチ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。

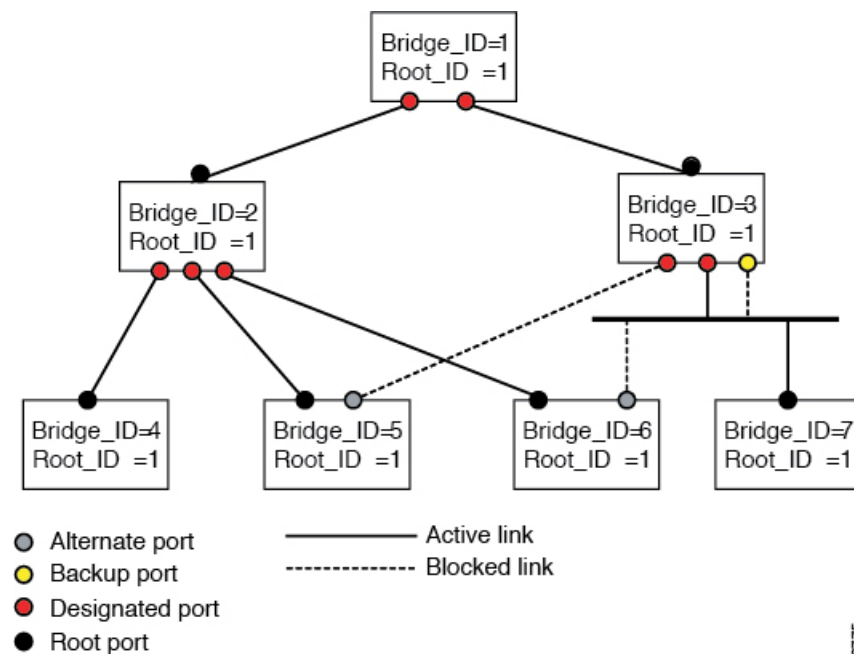
- ルートポート：スイッチによりパケットがルートブリッジに転送されるときに、最適のパス（最小コスト）を用意します。

- 指定ポート: 指定スイッチに接続します。指定スイッチでは、LANからルートブリッジにパケットが転送されるときに、発生するパス コストが最小になります。指定スイッチが LAN に接続するポートのことを指定ポートと呼びます。
- 代替ポート: 現在のルートポート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。代替ポートにより、トポロジにある別のスイッチへのパスが確保されます。
- バックアップ ポート: 指定ポートが提供した、スパニング ツリーのリーフに向かうパスのバックアップとして機能します。バックアップ ポートが存在できるのは、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されている場合、または1つのスイッチに共有 LAN セグメントへの接続が2つ以上ある場合です。バックアップ ポートにより、スイッチに対する別のパスがトポロジ内で確保されます。
- 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、RapidPVST+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。

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 ポートのロールを持つポートは、アクティブなトポロジから除外されます（次の図を参照）。

Figure 10: 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



ポート ステート

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の変化が発生します。スパニングツリー トポロジで LAN ポートが非伝搬ステートからフォワーディング ステートに直接移行する際、一時的にデータがループすることがあります。ポートは新しいトポロジ情報がスイッチド LAN 経由で伝播されるまで待機し、それからフレーム転送を開始する必要があります。

Rapid PVST+ または MST を使用しているソフトウェア上の各 LAN ポートは、次の 4 つのステートの 1 つで終了します。

- **ブロッキング:** LAN ポートはフレーム転送に参加しません。
- **ラーニング:** LAN ポートは、フレーム転送への参加を準備します。
- **フォワーディング:** LAN ポートはフレームを転送します。
- **ディセーブル:** LAN ポートは STP に参加せず、フレームを転送しません。

RapidPVST+をイネーブルにすると、ソフトウェアのすべてのポート、VLAN、ネットワークは、電源投入時にブロッキング ステートからラーニングの移行ステートに進みます。各 LAN ポートは、適切に設定されていれば、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 アルゴリズムにより LAN ポートがフォワーディング ステートになると、次の処理が発生します。

- ラーニングステートに進む必要があることを示すプロトコル情報を待つ間、LAN ポートはブロッキングステートになります。
- LAN ポートは転送遅延タイマーの期限が切れるのを待ち、ラーニングステートに移行し、転送遅延タイマーを再開します。
- ラーニングステートでは、LAN ポートはフォワーディングデータベースのエンドステーション位置情報をラーニングする間、フレームの転送をブロックし続けます。
- LAN ポートは転送遅延タイマーの期限が切れるのを待って、フォワーディングステートに移行します。このフォワーディングステートでは、ラーニングとフレーム転送が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 ステートにある LAN ポートはフレームを転送しません。

ブロッキング ステートの LAN ポートでは、次の処理が実行されます。

- 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 LAN ポートではラーニングがないため、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。
- ネットワーク管理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 ステートにある LAN ポートは、フレームの MAC アドレスをラーニングすることによって、フレーム転送の準備をします。LAN ポートは、ブロッキング ステートからラーニング ステートになります。

ラーニング ステートの LAN ポートでは、次の処理が実行されます。

- 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。
- ネットワーク管理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 ステートにある LAN ポートでは、フレームを転送します。LAN ポートは、ラーニング ステートからフォワーディング ステートになります。

フォワーディング ステートの LAN ポートでは、次の処理が実行されます。

- 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。
- ネットワーク管理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 ステートにある LAN ポートは、フレーム転送または STP は行いません。ディセーブル ステートの LAN ポートは、実質的に動作が停止しています。

ディセーブルの LAN ポートでは、次の処理が実行されます。

- 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、ポートおよびそれに対応してアクティブ トポロジに含められる、可能性のある動作と Rapid PVST+ のステートのリストを示します。

Table 5: 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	×
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

スイッチ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、強制的に、すべての他のポートと新しいルート情報との同期をとります。

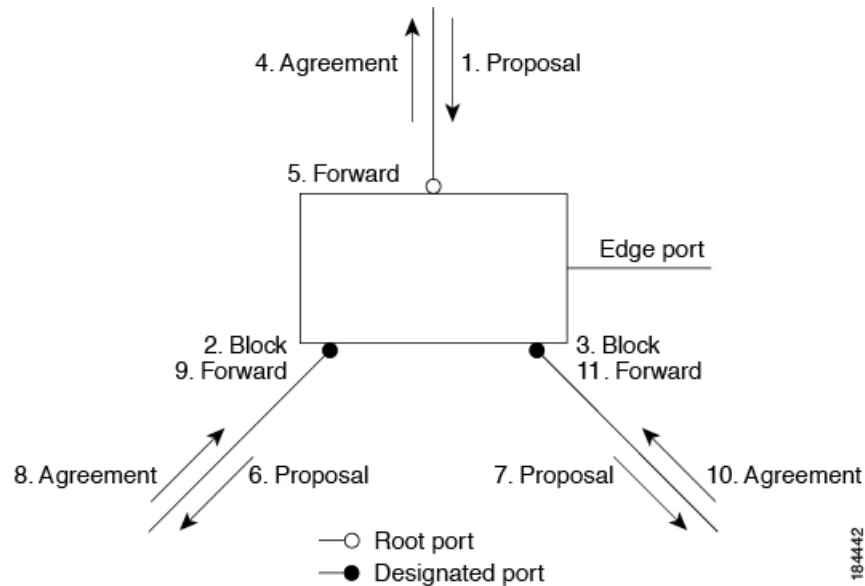
他のすべてのポートが同期化されると、スイッチはルート ポートで受信した優位のルート情報に同期化されます。次のいずれかが当てはまる場合、スイッチ上の個々のポートで同期がとられます。

- 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。

すべてのポートで同期がとられた後で、スイッチから、ルートポートに対応する指定スイッチへ、合意メッセージが送信されます。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が、そのポートのロールについての合意に存在する場合、Rapid PVST+により、ポートステートがただちにフォワーディングステートに移行します。この一連のイベントを次の図に示します。

Figure 11: 高速コンバージェンス中のイベントのシーケンス



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、選択されている場合、Rapid PVST+ は残りすべてのポートを同期させます。

受信した BPDU が提案フラグの設定された Rapid PVST+ BPDU の場合、スイッチは残りすべてのポートを同期させたあと、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。

スパニングツリーの異議メカニズム

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。

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グループを解決できるからです。

次の図に、ブリッジング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 規格の BPDU には、送信側ポートのロールと状態が含まれます。この情報により、送信する上位 BPDU に対してスイッチ B が反応しないこと、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）、ブリッジンググループが防止されます。ブロックは、STP の矛盾として示されます。

Figure 12: 単方向リンク障害の検出



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、ロング型（32 ビット）のパスコスト方式を使用するようにスイッチを設定することもできます。この場合、1 ～ 200,000,000 の範囲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。

STP ポートのパスコストのデフォルト値は、メディア速度と LAN インターフェイスのパスコストの計算方式によって決まります。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。

Table 6: 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 ギガビット イーサネット	4	20,000

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 ギガビットイーサネット	2	2,000

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

アクセス ポートでは、ポート 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

ループが発生し、複数のポートに同じパス コストが割り当てられている場合、RapidPVST+ では、フォワーディング ステートにする LAN ポートの選択時に、ポートのプライオリティを考慮します。RapidPVST+ 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、RapidPVST+ 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、RapidPVST+ 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。プライオリティの範囲は 0 ～ 224（デフォルトは 128）で、32 ずつ増加させて設定できます。LAN ポートがアクセスポートとして設定されているときはポートのプライオリティ値が使用され、LAN ポートがトランク ポートとして設定されているときは VLAN ポートのプライオリティ値が使用されます。

Rapid PVST+ と IEEE 802.1Q トランク

Cisco スイッチを 802.1Q トランクで接続しているネットワークでは、スイッチは、トランクの VLAN ごとに STP のインスタンスを 1 つ維持します。ただし、非 Cisco 802.1Q スイッチでは、トランクのすべての VLAN に対して維持する STP のインスタンスは 1 つだけです。

802.1Q トランクで Cisco スイッチを非 Cisco スイッチに接続している場合は、Cisco スイッチにより、トランクの 802.1Q VLAN の STP インスタンスが、非 Cisco 802.1Q スイッチの STP インスタンスと組み合わせられます。ただし、Cisco スイッチで維持されている VLAN ごとの STP 情報はすべて、非シスコ 802.1Q スイッチのクラウドによって分けられます。Cisco スイッチを分ける非 Cisco 802.1Q クラウドは、スイッチ間の単一のトランク リンクとして扱われます。

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 プロトコルを実行中のスイッチと相互に動作させることができます。スイッチが BPDU バージョン 0 を受信すると、802.1D を実行中の機器と相互に動作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、提案フラグがオンに設定された 802.1w BPDU バージョン 2 の場合、スイッチは残りすべてのポートを同期

させたあと、合意メッセージを送信します。受信した BPDU が 802.1D BPDU バージョン 0 の場合は、スイッチは提案フラグを設定せずに、ポートの転送遅延タイマーを開始します。新しいルートポートでは、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。

スイッチは、次のように、レガシー 802.1D スイッチと相互動作します。

- 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 スイッチとの相互運用のため、Cisco NX-OS では、TCN BPDU を処理し、生成します。
- 受信応答: 802.1w スイッチでは、802.1D スイッチから指定ポート上に TCN メッセージを受信すると、TCA ビットを設定し、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 スイッチに接続され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）がアクティブの場合、TCA がセットされたコンフィギュレーション BPDU を受信すると、TC While タイマーはリセットされます。

動作のこの方式は、802.1D スイッチでのみ必要です。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 スイッチとの下位互換性のために、802.1w は、802.1D コンフィギュレーション BPDU と TCN BPDU をポート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な間、スイッチ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。

ポート移行遅延タイマーの期限切れ後にスイッチで 802.1D BPDU を受信した場合は、802.1D スイッチに接続していると思われて、802.1D BPDU のみを使用して開始します。ただし、802.1w スイッチが、ポート上で 802.1D BPDU を使用中で、タイマーの期限切れ後に 802.1w BPDU を受信すると、タイマーが再起動され、ポート上の 802.1w BPDU を使用して開始されます。



Note

すべてのスイッチでプロトコルを再ネゴシエーションするには、Rapid PVST+ を再起動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。

Rapid PVST+ の設定

Rapid PVST+ プロトコルには 802.1w 規格が適用されていますが、Rapid PVST+ は、ソフトウェアのデフォルト STP 設定です。

Rapid PVST+ は VLAN ごとにイネーブルにします。STP のインスタンスが VLAN ごとに維持されます（STP をディセーブルにした VLAN を除く）。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

スイッチ上で Rapid PVST+ をイネーブルにすると、指定されている VLAN 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。MST と Rapid PVST+ は同時には実行できません。



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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mode rapid-pvst**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# spanning-tree mode rapid-pvst	<p>スイッチで 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。</p> <p>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。</p>

Example

次の例は、スイッチで Rapid PVST+ をイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mode rapid-pvst
```



Note STP はデフォルトでイネーブルのため、設定結果を参照するために **show running-config** 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 ベースのイネーブル化

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. switch# **configure terminal**
2. switch(config)# **spanning-tree** *vlan-range*
3. (Optional) switch(config)# **no spanning-tree** *vlan-range*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# spanning-tree <i>vlan-range</i>	VLAN ごとに Rapid PVST+（デフォルト STP）をイネーブルにします。 <i>vlan-range</i> の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。
Step 3	(Optional) switch(config)# no spanning-tree <i>vlan-range</i>	指定 VLAN で Rapid PVST+ をディセーブルにします。 Caution VLAN のすべてのスイッチおよびブリッジでスパニングツリーがディセーブルになっていない場合は、VLAN でスパニングツリーをディセーブルにしないでください。VLAN の一部のスイッチおよびブリッジでスパニングツリーをディセーブルにして、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

	Command or Action	Purpose
		<p>なるので、この処理によって予想外の結果となる場合があります。</p> <p>VLAN に物理ループが存在しないことを確認せずに、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、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。</p>

Example

次に、VLAN で STP をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5
```

ルートブリッジIDの設定

Rapid PVST+ では、STP のインスタンスはアクティブな VLAN ごとに管理されます。VLAN ごとに、最小のブリッジ ID を持つスイッチが、その VLAN のルートブリッジとして選定されます。

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

spanning-tree vlan *vlan_ID* root コマンドを入力すると、各 VLAN で現在ルートになっているブリッジのブリッジプライオリティがスイッチによって確認されます。スイッチは指定した VLAN のブリッジプライオリティを 24576 に設定します（このスイッチがその VLAN のルートになる値）。指定した VLAN のいずれかのルートブリッジに 24576 より小さいブリッジプライオリティが設定されている場合は、スイッチはその VLAN のブリッジプライオリティを、最小のブリッジプライオリティより 4096 だけ小さい値に設定します。



Note

ルートブリッジになるために必要な値が 1 より小さい場合は、**spanning-tree vlan *vlan_ID* root** このコマンドは機能しません。



Caution

STP の各インスタンスのルートブリッジは、バックボーンスイッチまたはディストリビューションスイッチでなければなりません。アクセススイッチは、STP のプライマリ ルートとして設定しないでください。

キーワード **diameter** を入力し、ネットワーク直径（ネットワーク内の任意の 2 つのエンドステーション間での最大ブリッジ ホップ数）を指定します。ネットワーク直径を指定すると、ソフト

ウェアはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に選びます。その結果、STP のコンバージェンスに要する時間が大幅に短縮されます。自動的に算出された hello タイムを無効にするには、**hello-time** キーワードを入力します。



Note ルートブリッジとして設定されているスイッチでは、hello タイム、転送遅延時間、最大エージング タイムを、**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、および **spanning-tree mst max-age** の各コンフィギュレーション コマンドを使用して手動で設定しないでください。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree vlan** *vlan-range* **root primary** [**diameter** *dia* [**hello-time** *hello-time*]]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 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。
Step 2	switch(config)# spanning-tree vlan <i>vlan-range</i> root primary [diameter <i>dia</i> [hello-time <i>hello-time</i>]]	ソフトウェアスイッチをプライマリ ルートブリッジとして設定します。 <i>vlan-range</i> の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。 <i>dia</i> のデフォルトは 7 です。 <i>hello-time</i> は 1 ～ 10 秒で、デフォルト値は 2 秒です。

Example

次の例は、VLAN のルート スイッチとしてスイッチを設定する方法を示しています。

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

セカンダリ ルート ブリッジの設定

ソフトウェアスイッチをセカンダリ ルートとして設定しているときに、STP ブリッジのプライオリティをデフォルト値（32768）から変更しておく、プライマリ ルートブリッジに障害が発生した場合に、そのスイッチが、指定した VLAN のルートブリッジになります（ネットワークの他のスイッチで、デフォルトのブリッジプライオリティ 32768 が使用されているとします）。STP により、ブリッジプライオリティが 28672 に設定されます。

キーワード **diameter** を入力し、ネットワーク直径（ネットワーク内の任意の2つのエンドステーション間での最大ブリッジ ホップ数）を指定します。ネットワーク直径を指定すると、ソフトウェアはその直径を持つネットワークに最適な **hello** タイム、転送遅延時間、および最大エージング タイムを自動的に選びます。その結果、STP のコンバージェンスに要する時間が大幅に短縮されます。自動的に算出された **hello** タイムを無効にするには、**hello-time** キーワードを入力します。

複数のスイッチに対して同様に設定すれば、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ているスイッチでは、**hello** タイム、転送遅延時間、最大エージング タイムを、**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、および **spanning-tree mst max-age** の各グローバル コンフィギュレーション コマンドを使用して手動で設定しないでください。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree vlan *vlan-range* root secondary [*diameter dia* [*hello-time hello-time*]]**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# spanning-tree vlan <i>vlan-range</i> root secondary [<i>diameter dia</i> [<i>hello-time hello-time</i>]]	ソフトウェアスイッチをセカンダリ ルートブリッジとして設定します。 <i>vlan-range</i> の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。 <i>dia</i> のデフォルトは 7 です。 <i>hello-time</i> は 1 ～ 10 秒で、デフォルト値は 2 秒です。

Example

次の例は、VLAN のセカンダリ ルート スイッチとしてスイッチを設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 root secondary diameter 4
```

Rapid PVST+ のポート プライオリティの設定

Rapid PVST+ に最初を選択させる 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。

LAN ポートがアクセス ポートとして設定されているときはポートのプライオリティ値が使用され、LAN ポートがトランク ポートとして設定されているときは VLAN ポートのプライオリティ値が使用されます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **spanning-tree [vlan vlan-list] port-priority priority**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface type slot/port	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。
Step 3	switch(config-if)# spanning-tree [vlan vlan-list] port-priority priority	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。 <i>priority</i> の値は 0 ～ 224 の範囲です。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。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。

Example

次の例は、イーサネット インタフェースのアクセス ポートのプライオリティを設定する方法を示しています。

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

このコマンドを使用できるのは、物理イーサネット インターフェイスに対してだけです。

Rapid PVST+ パスコスト方式およびポート コストの設定

アクセス ポートでは、ポートごとにポート コストを割り当てます。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、ショート型またはロング型のいずれかのパス コスト方式を使用できます。この方式は、インターフェイスまたはコンフィギュレーションサブモードのいずれかで設定できます。デフォルトのパス コスト方式は、ショート型です。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree pathcost method {long | short}**
3. switch(config)# **interface type slot/port**
4. switch(config-if)# **spanning-tree [vlan vlan-id] cost [value | auto]**

DETAILED STEPS

Procedure		
	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# spanning-tree pathcost method {long short}	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。
Step 3	switch(config)# interface type slot/port	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。
Step 4	switch(config-if)# spanning-tree [vlan vlan-id] cost [value auto]	<p>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。</p> <ul style="list-style-type: none"> • ショート型: 1 ～ 65535 • ロング型: 1 ～ 200000000 <p>Note このパラメータは、アクセスポートのインターフェイス別、およびトランク ポートの VLAN 別に設定します。</p>

	Command or Action	Purpose
		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。

Example

この例は、イーサネットインターフェイスのアクセス ポート コストを設定する方法を示しています。

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

このコマンドを使用できるのは、物理イーサネットインターフェイスに対してだけです。

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。



Note

この設定を使用するときは注意が必要です。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、ブリッジプライオリティを変更することを推奨します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree vlan *vlan-range* priority *value***

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# spanning-tree vlan <i>vlan-range</i> priority <i>value</i>	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。

Example

次の例は、VLAN のブリッジプライオリティを設定する方法を示します。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 priority 8192
```

VLAN の Rapid PVST+ の hello タイムの設定

VLAN では、Rapid PVST+ の hello タイムを設定できます。

**Note**

この設定を使用するときは注意が必要です。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. switch# **configure terminal**
2. switch(config)# **spanning-tree vlan** *vlan-range* **hello-time** *hello-time*

DETAILED STEPS**Procedure**

	Command or Action	Purpose
Step 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。
Step 2	switch(config)# spanning-tree vlan <i>vlan-range</i> hello-time <i>hello-time</i>	VLAN の hello タイムを設定します。hello タイムの値には 1 ～ 10 秒を指定できます。デフォルト値は 2 秒です。

Example

次の例は、VLAN の hello タイムの値を設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 hello-time 7
```

VLAN の Rapid PVST+ の転送遅延時間の設定

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. switch# **configure terminal**
2. switch(config)# **spanning-tree vlan *vlan-range* forward-time *forward-time***

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 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。
Step 2	switch(config)# spanning-tree vlan <i>vlan-range</i> forward-time <i>forward-time</i>	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。

Example

次の例は、VLAN の転送遅延時間を設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 forward-time 21
```

VLAN の Rapid PVST+ の最大経過時間の設定

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. switch# **configure terminal**
2. switch(config)# **spanning-tree vlan *vlan-range* max-age *max-age***

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	コンフィギュレーション モードに入ります。
Step 2	switch(config)# spanning-tree vlan <i>vlan-range</i> max-age <i>max-age</i>	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。

Example

次の例は、VLAN の最大経過時間を設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree vlan 5 max-age 36
```

リンク タイプの設定

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 スイッチの 1 つのポートに、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、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 に戻ります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **spanning-tree link-type {auto | point-to-point | shared}**

DETAILED STEPS

Procedure		
	Command or Action	Purpose
Step 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。
Step 2	switch(config)# interface type slot/port	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。
Step 3	switch(config-if)# spanning-tree link-type {auto point-to-point shared}	リンク タイプを、ポイントツーポイントリンクまたは共有リンクに設定します。デフォルト値はスイッチ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 に戻ります。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。

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

このコマンドを使用できるのは、物理イーサネットインターフェイスに対してだけです。

プロトコルの再開

レガシー ブリッジに接続されている場合、Rapid PVST+ を実行しているブリッジは、そのポートの1つに 802.1D BPDU を送信できます。ただし、STP プロトコルの移行では、レガシー スイッチが指定スイッチではない場合、レガシー スイッチがリンクから削除されたかどうかを認識できません。スイッチ全体または指定し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開する（強制的に隣接スイッチと再ネゴシエーションさせる）ことができます。

コマンド	目的
switch# clear spanning-tree detected-protocol [interface interface [<i>interface-num</i> <i>port-channel</i>]]	スイッチのすべてのインターフェイスまたは指定インターフェイスで Rapid PVST+ を再起動します。

次の例は、イーサネット インターフェイスで Rapid PVST+ を再起動する方法を示しています。

```
switch# clear spanning-tree detected-protocol interface ethernet 1/8
```

Rapid PVST+ 設定の確認

Rapid PVST+ の設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
show running-config spanning-tree [all]	現在のスパンニングツリー設定を表示します。
show spanning-tree [<i>options</i>]	最新のスパンニングツリー設定について、指定した詳細情報を表示します。

次の例は、スパンニングツリーのステータスの表示方法を示しています。

```
switch# show spanning-tree brief

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32768
             Address     001c.b05a.5447
```

```
Cost          2
Port          131 (Ethernet1/3)
Hello Time    2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address       000d.ec6d.7841
Hello Time    2 sec Max Age 20 sec Forward Delay 15 sec
Interface     Role Sts Cost      Prio.Nbr Type
-----
Eth1/3        Root FWD 2        128.131 P2p Peer (STP)
```




第 7 章

マルチ スパニングツリーの設定

- [MST について（89 ページ）](#)
- [MST の設定（98 ページ）](#)
- [MST の設定の確認, on page 119](#)

MST について

MST の概要



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。

MST は、複数の VLAN を 1 つのスパニングツリー インスタンスにマップします。各インスタンスのスパニングツリー トポロジは、他のスパニングツリー インスタンスの影響を受けません。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、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のため、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。

MST の使用中は、MAC アドレスの削減が常にイネーブルに設定されます。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+）

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 802.1s では MST が定義されて、IEEE 802.1Q に組み込まれました。



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 領域

スイッチが MSTI に参加できるようにするには、同一の MST 設定情報でスイッチの設定に整合性を持たせる必要があります。

同じ MST 設定の相互接続スイッチの集まりが MST リージョンです。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。

各スイッチがどの MST リージョンに属するかは、MST コンフィギュレーションによって制御されます。この設定には、領域の名前、バージョン番号、MST VLAN とインスタンスの割り当てマップが含まれます。

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。

各リージョンは、最大 65 の MST インスタンス (MSTI) までサポートします。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。

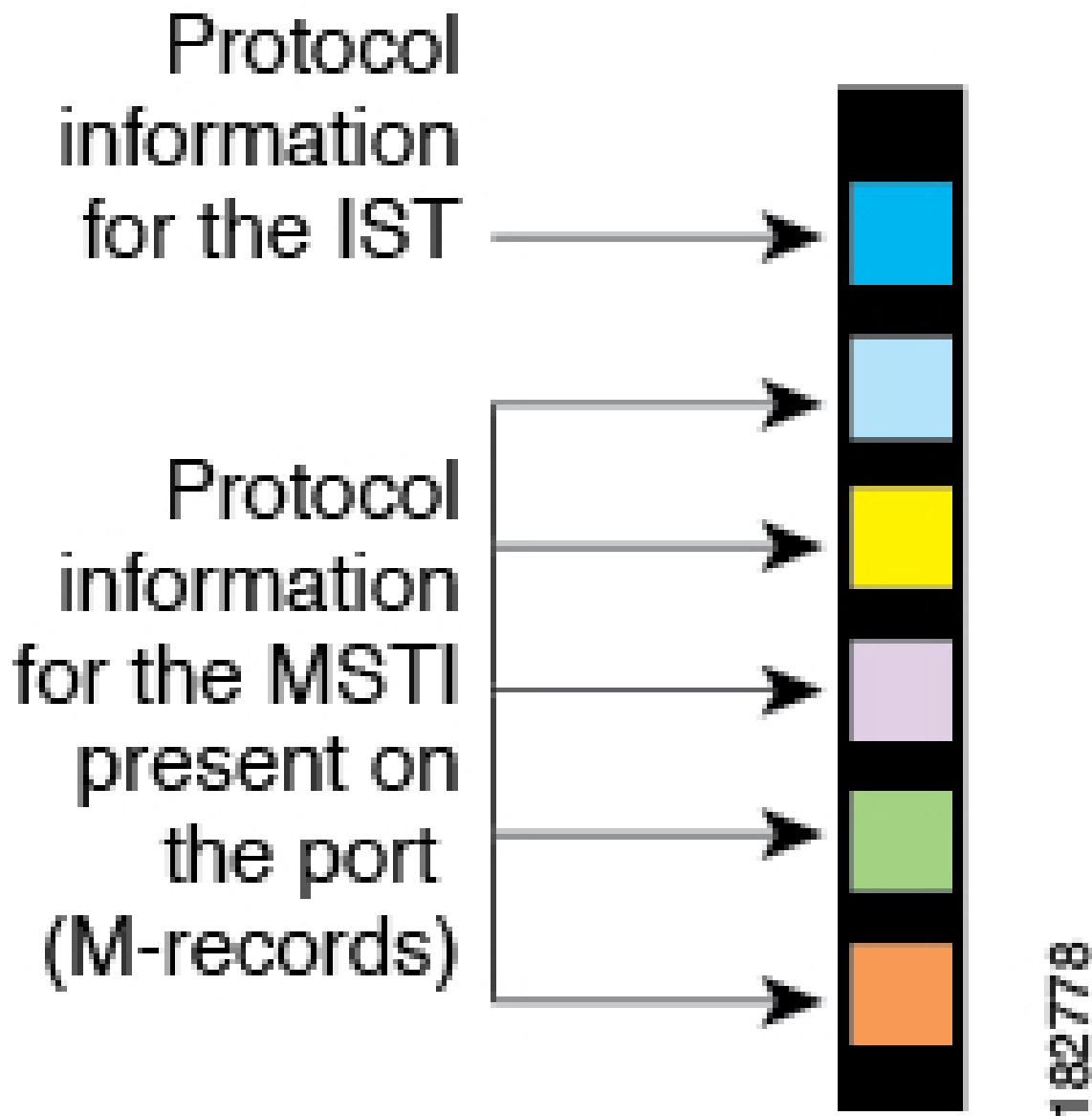


Note ネットワークを、非常に多数の領域に分けることは推奨しません。

MST BPDU

1 つの領域に含まれる MST BPDU は 1 つだけで、その BPDU により、領域内の各 MSTI について M レコードが保持されます (次の図を参照)。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 にはすべてのインスタンスに関する情報が保持されるため、MSTI をサポートするために処理する必要がある BPDU の数は、非常に少なくなります。

Figure 13: MSTI の M レコードが含まれる MST BPDUs



MST 設定情報

単一の MST 領域内にあるすべてのスイッチで 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 設定の次の 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。

- **MST 設定テーブル:** 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 4094 の各 VLAN を該当のインスタンスにアソシエートします。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。

**Caution**

VLAN/MSTI マッピングを変更すると、MST は再起動されます。

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。

- 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 の各規格をサポートするスイッチで実行されているスパニングツリーアルゴリズムによって形成されています。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 1 つのリージョン内のすべての MSTP スイッチを接続します。IST が収束すると、IST のルートは CIST リージョナルルートになります。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 スイッチの 1 つが CIST リージョナルルートとして選択されます。

MST スイッチが初期化されると、スイッチ自体を識別する BPDU が、CIST のルートおよび CIST リージョナルルートとして送信されます。このとき、CIST ルートと CIST リージョナルルートへのパス コストは両方ゼロに設定されます。また、スイッチはすべての MSTI を初期化し、これらすべての MSTI のルートであることを示します。現在ポートに格納されている情報よりも上位の MST 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）をスイッチが受信すると、CIST リージョナルルートとしての主張を撤回します。

MST リージョンには、初期化中に多くのサブリージョンが含まれて、それぞれに独自の CIST リージョナルルートが含まれることがあります。スイッチは、同一リージョンのネイバーから優位 IST 情報を受信すると、古いサブリージョンを離れ、本来の CIST リージョナルルートを含む新しいサブリージョンに加わります。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 リージョン内のすべてのスイッチが同じ CIST リージョナルルートを承認する必要があります。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

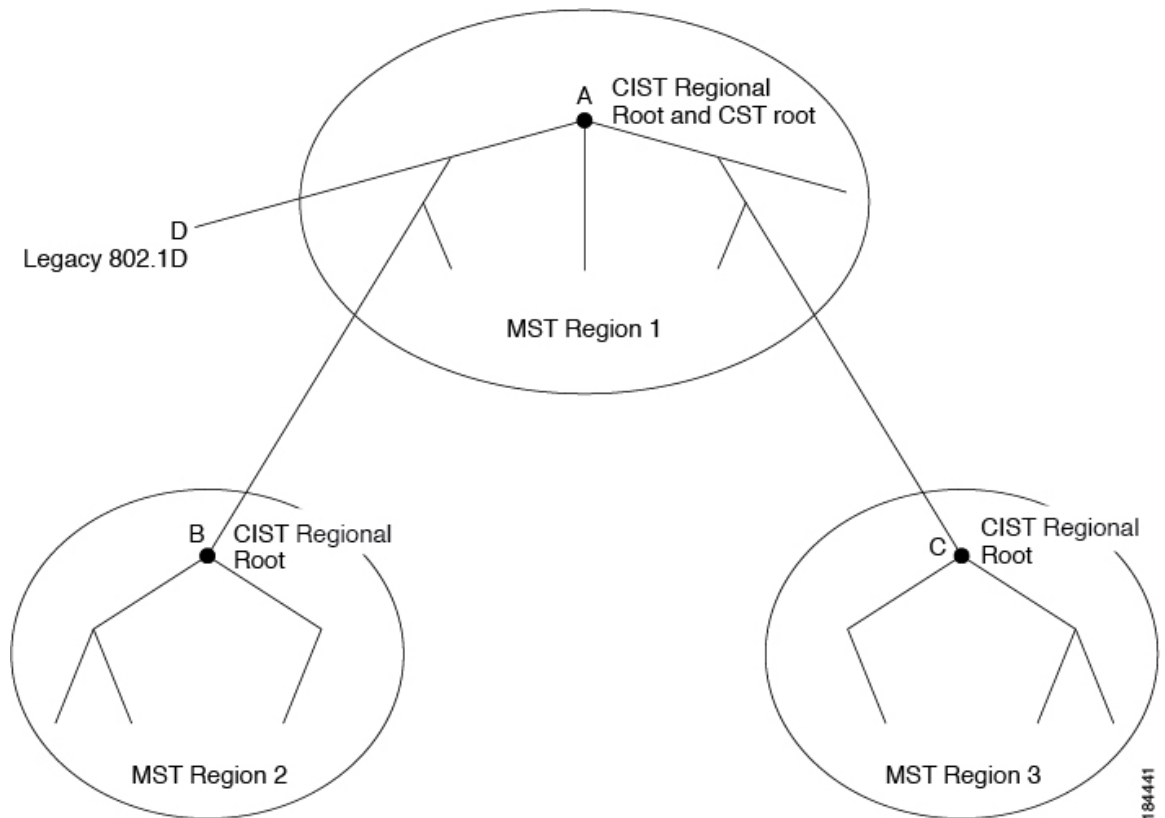
ネットワーク内に複数の領域、または 802.1w や 802.1D STP インスタンスがある場合、MST はネットワーク内のすべての MST 領域、すべての 802.1w と 802.1D STP スイッチを含む CST を確立して、維持します。MSTI は、リージョンの境界にある IST と組み合わせり、CST になります。

IST は、リージョン内のすべての MSTP スイッチに接続し、スイッチド ドメイン全体を網羅する CIST のサブツリーとして見なされます。サブツリーのルートは CIST リージョナルルートです。MST リージョンは、隣接する STP スイッチや MST リージョンからは仮想スイッチとして認識されます。

次の図に、3 つの MST 領域と 802.1D (D) がある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）、およびバージョン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。

Figure 14: MST リージョン、CIST リージョナルルート、CST ルート



BPDU を送受信するのは CST インスタンスのみです。MSTI は、そ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、隣接スイッチと相互作用して、最終的なスパニングツリー トポロジを計算します。このプロセスのため、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 スイッチは、802.1D 専用スイッチと通信する場合、バージョン 3 BPDU または 802.1D STP BPDU を使用します。MST スイッチは、MST スイッチと通信する場合、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わ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。MST リージョンは、CIST に対する唯一のスイッチのように見えます。CIST 外部ルートパスコストは、これらの仮想スイッチとリージョンに属していないスイッチ間を計算して出したルート パス コストです。
- CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。または、CIST リージョナルルートがそのリージョンで CIST ルートに最も近いスイッチになります。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、メッセージエージング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) を常々に送信します。スイッチがこの BPDU を受信すると、受信 BPDU の残存ホップ カウントから 1 だけ差し引いた値を残存ホップ カウントとする BPDU を生成し、これを伝播します。このホップ カウントが 0 になると、スイッチはその BPDU を廃棄し、ポート用に維持されていた情報を期限切れにします。

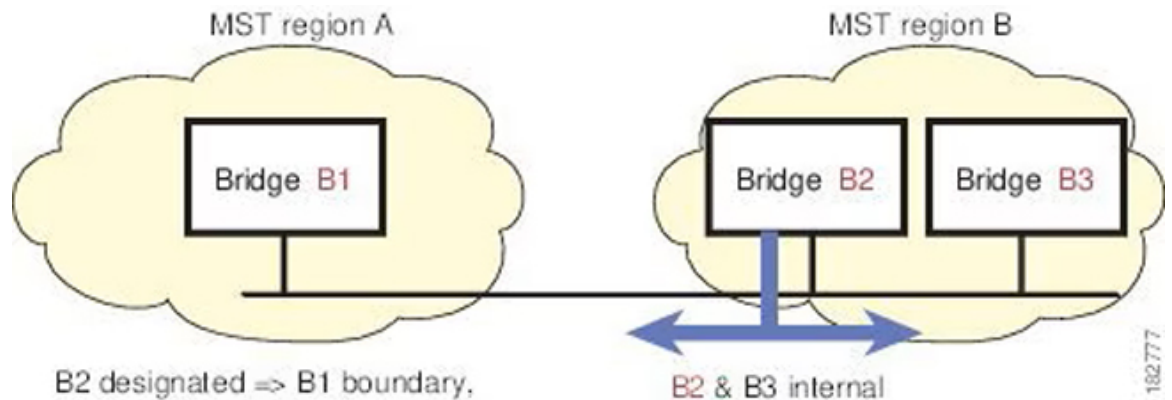
BPDU の 802.1w 部分に格納されているメッセージ有効期間および最大エージング タイムの情報は、領域全体で同じです (IST の場合のみ)。同じ値が、境界にある領域の指定ポートによって伝播されます。

スイッチ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として最大エージング タイムを設定します。

境界ポート

境界ポートは、ある領域を別の領域に接続するポートです。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。この定義により、領域の内部にある 2 つのポートが、異なる領域に属すポートとセグメントを共有できるため、ポートで内部メッセージと外部メッセージの両方を受信できる可能性があります (次の図を参照)。

Figure 15: 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。

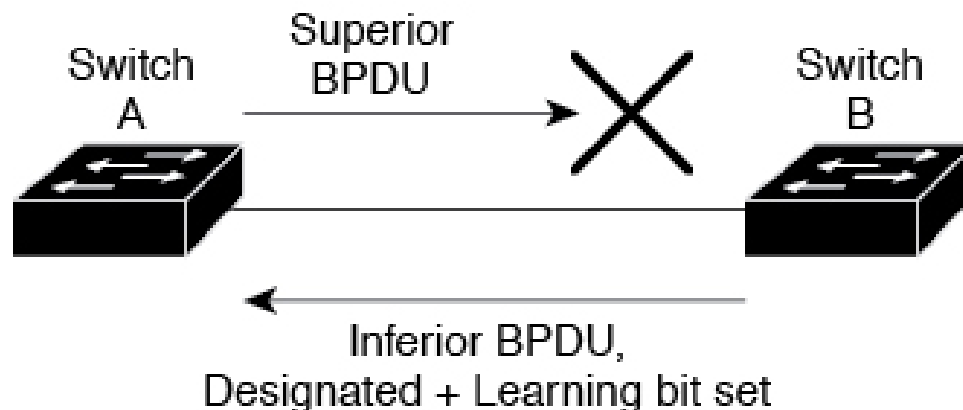
スパニングツリーの異議メカニズム

現在、この機能は、IEEE MST 規格にはありませんが、規格準拠の実装に含まれています。ソフトウェアは、受信した BPDUs 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。

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グループを解決できるからです。

次の図に、ブリッジング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 BPDUs は失われます。Rapid PVST+ (802.1w) には、送信側ポートのロール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 BPDUs 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）、ブリッジンググループが防止されます。ブロックは、STP の矛盾として示されます。

Figure 16: 単一方向リンク障害の検出



184440

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。

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

ポート コストを設定すると、選択されるポートが影響を受けます。



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 が実行されるスイッチでは、802.1D STP スイッチとの相互運用を可能にする、内蔵プロトコル移行機能がサポートされます。このスイッチで、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 スイッチは、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、スイッチは、802.1D BPDU を受信しなくなった場合でも、自動的に MSTP モードには戻りません。これは、802.1D スイッチが指定スイッチではない場合、802.1D スイッチがリンクから削除されたかどうかを検出できないためです。さらにスイッチは、接続先スイッチがリージョンに加入した場合であっても、引き続きポートに境界の役割を指定する可能性があります。

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 802.1D 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 スイッチは、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 に接続され、その指定スイッチは、単一スパニングツリー スイッチか、MST 設定が異なるスイッチのいずれかです。



Note MST は、MST ポート上で先行標準 MSTP を受信するたびに、シスコの先行標準マルチ スパニングツリー プロトコル（MSTP）と相互に動作します。明示的な設定は必要ありません。

Rapid PVST+ の相互運用性と PVST シミュレーションについて

MST は、ユーザが設定しなくても、Rapid PVST+ と相互運用できます。PVST シミュレーション機能により、このシームレスな相互運用が可能になっています。



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。つまり、スイッチ上のすべてのインターフェイスは、デフォルトで、MST と Rapid PVST+ との間で相互動作します。

ただし、MST と Rapid PVST+ との接続を制御し、MST 対応ポートを Rapid PVST+ 対応ポートに誤って接続するのを防止することが必要な場合もあります。Rapid PVST+ はデフォルト STP モードのため、Rapid PVST+ がイネーブルな多数の接続が検出されることがあります。

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、スイッチ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、ブロックング ステートに移行します。このポートは、Rapid PVST+/SSTP BPDU を受信しなくなるまで不整合ステートのままですが、そのあとは標準 STP のステート移行を再開します。

MST の設定

MST 設定時の注意事項

MST を設定する場合は、次の注意事項に従ってください。

- MST 設定モードの場合、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モードを終了するには、**abort** コマンドを入力します。
- 行った変更内容をすべてコミットして MST コンフィギュレーションモードを終了するには、**exit** コマンドを入力します。

MST の有効化

MST はイネーブルにする必要があります。デフォルトは Rapid PVST+ です。



Caution

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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch# **configure terminal**
3. switch(config)# **spanning-tree mode mst**
4. (Optional) switch(config)# **no spanning-tree mode mst**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch# configure terminal	コンフィギュレーション モードに入ります。
Step 3	switch(config)# spanning-tree mode mst	スイッチ上で MST をイネーブルにします。
Step 4	(Optional) switch(config)# no spanning-tree mode mst	スイッチ上の MST がディセーブルにされ、Rapid PVST+ に戻ります。

Example

次の例は、スイッチで MST をイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mode mst
```



Note STP はデフォルトでイネーブルのため、設定結果を参照するために **show running-config** 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。

MST コンフィギュレーション モードの開始

スイッチ上で、MSTの名前、VLANからインスタンスへのマッピング、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。

同じ MST リージョンにある複数のスイッチには、同じ MST の名前、VLAN からインスタンスへのマッピング、MST リビジョン番号を設定しておく必要があります。



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。

MST コンフィギュレーション モードで作業している場合、**exit** コマンドと **abort** コマンドとの違いに注意してください。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst configuration**
3. switch(config-mst)# **exit** or switch(config-mst)# **abort**
4. (Optional) switch(config)# **no spanning-tree mst configuration**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# spanning-tree mst configuration	システム上で、MST コンフィギュレーション モードを開始します。次の MST コンフィギュレーション パラメータを割り当てるには、MST コンフィギュレーション モードを開始しておく必要があります。 <ul style="list-style-type: none"> • MST 名 • インスタンスから VLAN へのマッピング • MST リビジョン番号

	Command or Action	Purpose
Step 3	switch(config-mst)# exit or switch(config-mst)# abort	終了または中断します。 <ul style="list-style-type: none"> • exit コマンドは、すべての変更をコミットして MST コンフィギュレーションモードを終了します。 • abort コマンドは、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モードを終了します。
Step 4	(Optional) switch(config)# 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。 <ul style="list-style-type: none"> • 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。

MST の名前の指定

ブリッジに領域名を設定できます。同じ MST リージョンにある複数のブリッジには、同じ MST の名前、VLAN からインスタンスへのマッピング、MST リビジョン番号を設定しておく必要があります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst configuration**
3. switch(config-mst)# **name name**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# spanning-tree mst configuration	MST コンフィギュレーションサブモードを開始します。

	Command or Action	Purpose
Step 3	switch(config-mst)# name <i>name</i>	MST 領域の名前を指定します。 <i>name</i> ストリングには 32 文字まで使用でき、大文字と小文字が区別されます。デフォルトは空の文字列です。

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# configure terminal
switch(config)# spanning-tree mst configuration
switch(config-mst)# name accounting
```

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。同じ MST リージョンにある複数のブリッジには、同じ MST の名前、VLAN からインスタンスへのマッピング、MST リビジョン番号を設定しておく必要があります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst configuration**
3. switch(config-mst)# **revision** *name*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 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。
Step 2	switch(config)# spanning-tree mst configuration	MST コンフィギュレーションサブモードを開始します。
Step 3	switch(config-mst)# revision <i>name</i>	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。

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# configure terminal
```

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

MST リージョンでの設定の指定

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

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 を処理する必要があります。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. switch# **configure terminal**
2. switch(config)# **spanning-tree mst configuration**
3. switch(config-mst)# **instance** *instance-id* **vlan** *vlan-range*
4. switch(config-mst)# **name** *name*
5. switch(config-mst)# **revision** *name*

DETAILED STEPS

Procedure		
	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# spanning-tree mst configuration	MST コンフィギュレーションサブモードを開始します。
Step 3	switch(config-mst)# instance <i>instance-id</i> vlan <i>vlan-range</i>	<p>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。</p> <ul style="list-style-type: none">• <i>instance-id</i> の範囲は 1 ～ 4094 です。• vlan <i>vlan-range</i> の範囲は 1 ～ 4094 です。 <p>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。</p> <p>VLAN の範囲を指定するにはハイフンを入力します。たとえば VLAN 1 ～ 63 を MST インスタンス 1 にマッ</p>

	Command or Action	Purpose
		<p>ピングするには、 instance 1 vlan 1-63 コマンドを入力します。</p> <p>一連の VLAN を指定するにはカンマを入力します。たとえば VLAN 10、20、30 を MST インスタンス 1 にマッピングするには、 instance 1 vlan 10, 20, 30 コマンドを入力します。</p>
Step 4	switch(config-mst)# name <i>name</i>	インスタンス名を指定します。 <i>name</i> スtringには32文字まで使用でき、大文字と小文字が区別されます。
Step 5	switch(config-mst)# revision <i>name</i>	設定リビジョン番号を指定します。範囲は0～65535です。

Example

デフォルトに戻すには、次のように操作します。

- デフォルトの MST リージョン設定に戻すには、 **no spanning-tree mst configuration** コンフィギュレーション コマンドを入力します。
- VLAN インスタンスマッピングをデフォルトの設定に戻すには、 **no instance instance-id vlan vlan-range MST** コンフィギュレーション コマンドを使用します。
- デフォルトの名前に戻すには、 **no name MST** コンフィギュレーション コマンドを入力します。
- デフォルトのリビジョン番号に戻すには、 **no revision MST** コンフィギュレーション コマンドを入力します。
- Rapid PVST+を再度イネーブルにするには、 **no spanning-tree mode** または **spanning-tree mode rapid-pvst** グローバルコンフィギュレーションコマンドを入力します。

次の例は、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、領域に **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)# spanning-tree mst configuration
switch(config-mst)# instance 1 vlan 10-20
switch(config-mst)# name region1
switch(config-mst)# revision 1
switch(config-mst)# show pending
Pending MST configuration
Name          [region1]
```

```

Revision 1
Instances configured 2
Instance Vlans Mapped
-----
0        1-9,21-4094
1        10-20
-----

```

VLAN から MST インスタンスへのマッピングとマッピング解除



Caution

VLAN/MSTI マッピングを変更すると、MST は再起動されます。



Note

MSTI はディセーブルにできません。

同じ MST リージョンにある複数のブリッジには、同じ MST の名前、VLAN からインスタンスへのマッピング、MST リビジョン番号を設定しておく必要があります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst configuration**
3. switch(config-mst)# **instance** *instance-id* **vlan** *vlan-range*
4. switch(config-mst)# **no instance** *instance-id* **vlan** *vlan-range*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# spanning-tree mst configuration	MST コンフィギュレーションサブモードを開始します。
Step 3	switch(config-mst)# instance <i>instance-id</i> vlan <i>vlan-range</i>	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。 <ul style="list-style-type: none"> • <i>instance-id</i> 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。

	Command or Action	Purpose
		<ul style="list-style-type: none"> • <i>vlan-range</i> の範囲は 1 ～ 4094 です。 <p>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。</p>
Step 4	switch(config-mst)# 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。

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# configure terminal
switch(config)# spanning-tree mst configuration
switch(config-mst)# instance 3 vlan 200
```

ルートブリッジの設定

スイッチは、ルートブリッジになるよう設定できます。



Note 各 MSTI のルートブリッジは、バックボーンスイッチまたはディストリビューションスイッチである必要があります。アクセススイッチは、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。

MSTI 0（または IST）でのみ使用可能な **diameter** キーワードを入力し、ネットワーク直径（ネットワーク内の任意の 2 つのエンドステーション間での最大ホップ数）を指定します。ネットワークの直径を指定すると、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、および最大エージングタイムをスイッチが自動的に設定するので、コンバージェンスの所要時間を大幅に短縮できます。自動的に算出された **hello** タイムを無効にするには、**hello** キーワードを入力します。



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

SUMMARY STEPS

1. switch# **configure terminal**

2. switch(config)# **spanning-tree mst instance-id root {primary | secondary} [diameter dia [hello-time hello-time]]**
3. (Optional) switch(config)# **no spanning-tree mst instance-id root**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# spanning-tree mst instance-id root {primary secondary} [diameter dia [hello-time hello-time]]	<p>次のように、ルートブリッジとしてスイッチを設定します。</p> <ul style="list-style-type: none"> • <i>instance-id</i> 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。 • <i>diameter net-diameter</i> には、2 つのエンドステーション間にホップの最大数を設定します。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。 • <i>hello-time seconds</i> には、ルートブリッジが設定メッセージを生成する時間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。
Step 3	(Optional) switch(config)# 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。

Example

次の例は、MSTI 5 のルートスイッチとしてスイッチを設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst 5 root primary
```

セカンダリ ルート ブリッジの設定

このコマンドは、複数のスイッチに対して実行し、複数のバックアップルートブリッジを設定できます。 **spanning-tree mst root primary** 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. switch# **configure terminal**
2. switch(config)# **spanning-tree mst instance-id root {primary | secondary} [diameter dia [hello-time hello-time]]**
3. (Optional) switch(config)# **no spanning-tree mst instance-id root**

DETAILED STEPS

Procedure		
	Command or Action	Purpose
Step 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。
Step 2	switch(config)# spanning-tree mst instance-id root {primary secondary} [diameter dia [hello-time hello-time]]	<p>次のように、セカンダリ ルートブリッジとしてスイッチを設定します。</p> <ul style="list-style-type: none"> • <i>instance-id</i> 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。 • <i>diameter net-diameter</i> には、2 つのエンドステーション間にホップの最大数を設定します。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。 • <i>hello-time seconds</i> には、ルートブリッジが設定メッセージを生成する時間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。
Step 3	(Optional) switch(config)# 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。

Example

次の例は、MSTI 5 のセカンダリ ルート スイッチとしてスイッチを設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst 5 root secondary
```

ポートの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。最初を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、最後を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. switch# **configure terminal**
2. switch(config)# **interface** {{type slot/port} | {port-channel number}}
3. switch(config-if)# **spanning-tree mst instance-id port-priority priority**

DETAILED STEPS

Procedure		
	Command or Action	Purpose
Step 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。
Step 2	switch(config)# interface {{type slot/port} {port-channel number}}	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。
Step 3	switch(config-if)# spanning-tree mst instance-id port-priority priority	<p>次のように、ポートのプライオリティを設定します。</p> <ul style="list-style-type: none"> • <i>instance-id</i> 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。 • <i>priority</i> 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。 <p>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。</p>

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# configure terminal
```

```
switch(config)# interface ethernet 3/1
switch(config-if)# spanning-tree mst 3 port-priority 64
```

このコマンドを使用できるのは、物理イーサネットインターフェイスに対してだけです。

ポートコストの設定

MSTパスコストのデフォルト値は、インターフェイスのメディア速度から算出されます。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. switch# **configure terminal**
- 2. switch(config)# **interface** {{type slot/port} | {port-channel number}}
- 3. switch(config-if)# **spanning-tree mst instance-id cost** [cost | auto]

DETAILED STEPS

Procedure		
	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface {{type slot/port} {port-channel number}}	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。
Step 3	switch(config-if)# spanning-tree mst instance-id cost [cost auto]	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。

	Command or Action	Purpose
		<ul style="list-style-type: none"> • <i>cost</i> の範囲は 1 ～ 200000000 です。デフォルト値は <i>auto</i> 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。

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# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# spanning-tree mst 4 cost 17031970
```

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のプライオリティは、指定されたポートがルートブリッジとして選択されるように設定できます。



Note

このコマンドの使用には注意してください。ほとんどの場合、スイッチのプライオリティを変更するには、**spanning-tree mst root primary** および **spanning-tree mst root secondary** のグローバル コンフィギュレーション コマンドの使用を推奨します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst instance-id priority priority-value**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 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。
Step 2	switch(config)# spanning-tree mst instance-id priority priority-value	<p>次のように、スイッチのプライオリティを設定します。</p> <ul style="list-style-type: none"> • <i>instance-id</i> 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

	Command or Action	Purpose
		<p>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。</p> <ul style="list-style-type: none"> • priority には、4096 単位で 0 ～ 61440 の値を指定します。デフォルトは 32768 です。小さい値を設定すると、スイッチがルート スイッチとして選択される可能性が高くなります。 <p>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。</p>

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# configure terminal
```

```
switch(config)# spanning-tree mst 5 priority 4096
```

hello タイムの設定

hello タイムを変更することによって、スイッチ上のすべてのインスタンスについて、ルートブリッジにより設定メッセージを生成する間隔を設定できます。



Note このコマンドの使用には注意してください。多くの状況では、**spanning-tree mst instance-id root primary** および **spanning-tree mst instance-id root secondary** コンフィギュレーション コマンドを入力して hello タイムを変更することを推奨します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst hello-time seconds**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 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。

	Command or Action	Purpose
Step 2	switch(config)# spanning-tree mst hello-time seconds	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、スイッチがアクティブであることを意味します。 <i>seconds</i> の範囲は 1 ～ 10 で、デフォルトは 2 秒です。

Example

次の例は、スイッチの hello タイムを 1 秒に設定する方法を示しています。

```
switch# configure terminal
```

```
switch(config)# spanning-tree mst hello-time 1
```

転送遅延時間の設定

スイッチ上のすべての MST インスタンスには、1 つのコマンドで転送遅延タイマーを設定できます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst forward-time seconds**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 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。
Step 2	switch(config)# spanning-tree mst forward-time seconds	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。 <i>seconds</i> の範囲は 4 ～ 30 で、デフォルトは 15 秒です。

Example

次の例は、スイッチの転送遅延時間を 10 秒に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst forward-time 10
```

最大エージング タイムの設定

最大経過時間タイマーは、スイッチが、再設定を試行する前に、スパニングツリー設定メッセージの受信を待つ秒数です。

スイッチ上のすべての MST インスタンスには、1つのコマンドで最大経過時間タイマーを設定できます（最大経過時間は IST にのみ適用されます）。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst max-age seconds**

DETAILED STEPS

Procedure		
	Command or Action	Purpose
Step 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。
Step 2	switch(config)# spanning-tree mst max-age seconds	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。最大経過時間は、スイッチが、再設定を試行する前に、スパニングツリー設定メッセージの受信を待つ秒数です。 <i>seconds</i> の範囲は 6 ～ 40 で、デフォルトは 20 秒です。

Example

次の例は、スイッチの最大エージング タイマーを 40 秒に設定する方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst max-age 40
```

最大ホップ カウントの設定

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。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。ホップカウントは、メッセージ エージング情報と同じ結果になります（再設定を開始）。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst max-hops hop-count**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# spanning-tree mst max-hops hop-count	BPDU を廃棄してポート用に保持していた情報を期限切れにするまでの、リージョンでのホップ数を設定します。hop-count の有効範囲は 1 ～ 255 で、デフォルト値は 20 ホップです。

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# configure terminal
switch(config)# spanning-tree mst max-hops 40
```

PVST シミュレーションのグローバル設定

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 コマンドを入力すると、インターフェイス コマンドモードの実行中に、スイッチ全体の PVST シミュレーション設定を変更できます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no spanning-tree mst simulate pvst global**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# no spanning-tree mst simulate pvst global	Rapid PVST+ モードで実行中の接続スイッチと自動的に相互動作する状態から、スイッチ上のすべての

	Command or Action	Purpose
		インターフェイスをディセーブルにできます。スイッチ上のすべてのインターフェイスは、デフォルトで、Rapid PVST+ と MST との間でシームレスに動作します。

Example

次の例は、RapidPVST+を実行している接続スイッチと自動的に相互運用することを防止するようにスイッチを設定する方法を示しています。

```
switch# configure terminal
switch(config)# no spanning-tree mst simulate pvst global
```

ポートごとの PVST シミュレーションの設定

MST は、Rapid PVST+ とシームレスに相互動作します。ただし、デフォルト STP モードとして MST が実行されていないスイッチへの誤った接続を防ぐため、この自動機能をディセーブルにする必要が生じる場合があります。RapidPVST+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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *{{type slot/port}}* | **{port-channel number}}**
3. switch(config-if)# **spanning-tree mst simulate pvst disable**
4. switch(config-if)# **spanning-tree mst simulate pvst**
5. switch(config-if)# **no spanning-tree mst simulate pvst**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface <i>{{type slot/port}}</i> {port-channel number}}	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。

	Command or Action	Purpose
Step 3	switch(config-if)# spanning-tree mst simulate pvst disable	Rapid PVST+ モードで実行中の接続スイッチと自動的に相互動作する状態から、指定したインターフェイスをディセーブルにします。 スイッチ上のすべてのインターフェイスは、デフォルトで、Rapid PVST+ と MST との間でシームレスに動作します。
Step 4	switch(config-if)# spanning-tree mst simulate pvst	指定したインターフェイスで、MST と Rapid PVST+ との間のシームレスな動作を再度イネーブルにします。
Step 5	switch(config-if)# 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、設定したスイッチ全体で MST と Rapid PVST+ との間で相互動作するように設定します。

Example

次の例は、MST を実行していない接続スイッチと自動的に相互運用することを防止するように指定インターフェイスを設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree mst simulate pvst disable
```

リンク タイプの設定

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。

リモートスイッチの 1 つのポートに、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、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 に戻されます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **spanning-tree link-type {auto | point-to-point | shared}**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	コンフィギュレーション モードに入ります。
Step 2	switch(config)# interface <i>type slot/port</i>	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。
Step 3	switch(config-if)# spanning-tree link-type {auto point-to-point shared}	リンク タイプを、ポイントツーポイントまたは共有に設定します。システムでは、スイッチ接続からデフォルト値を読み込みます。半二重リンクは共有で、全二重リンクはポイントツーポイントです。リンク タイプが共有の場合、STP は 802.1D に戻ります。デフォルトは 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。

Example

次の例は、リンク タイプをポイントツーポイントとして設定する方法を示しています。

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

プロトコルの再開

MST ブリッジは、レガシー BPDU または別のリージョンと関連付けられた MST BPDU を受信すると、ポートがリージョンの境界に位置していることを検出できます。ただし、STP プロトコルの移行では、レガシー スイッチが指定スイッチではない場合、IEEE 802.1D のみが実行されているレガシー スイッチが、リンクから削除されたかどうかを認識できません。スイッチ全体または指定し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開する（強制的に隣接スイッチと再ネゴシエーションさせる）には、このコマンドを入力します。

SUMMARY STEPS

1. switch# **clear spanning-tree detected-protocol** [interface *interface* [interface-num | port-channel]]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# clear spanning-tree detected-protocol [interface <i>interface</i> [interface-num port-channel]]	スイッチ全体または指定したインターフェイスで、MST を再開します。

Example

次の例は、スロット 2、ポート 8 のイーサネット インターフェイスで MST を再起動する方法を示しています。

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

MST の設定の確認

MST の設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
show running-config spanning-tree [all]	現在のスパニングツリー設定を表示します。
show spanning-tree mst [options]	現在の MST 設定の詳細情報を表示します。

次に、現在の MST 設定を表示する例を示します。

```
switch# show spanning-tree mst configuration
```

```
% Switch is not in mst mode
```

```
Name      [mist-attempt]
```

```
Revision 1      Instances configured 2
```

```
Instance Vlans mapped
```

```
-----
0          1-12,14-41,43-4094
1          13,42
```




第 8 章

STP 拡張機能の設定

• 概要, on page 121

概要

シスコでは、スパニングツリー プロトコル (STP) に、収束をより効率的に行うための拡張機能を追加しました。場合によっては、同様の機能が IEEE 802.1w 高速スパニングツリー プロトコル (RSTP) 標準にも組み込まれている可能性がありますが、シスコの拡張機能を使用することを推奨します。これらの拡張機能はすべて、RPVST+ およびマルチ スパニングツリー プロトコル (MST) と組み合わせて使用できます。

使用可能な拡張機能には、スパニングツリー ポート タイプ、Bridge Assurance、ブリッジプロトコルデータユニット (BPDU) ガード、BPDU フィルタリング、ループ ガード、ルート ガードがあります。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 拡張機能について

STP ポート タイプの概要

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。インターフェイスが接続されているデバイスのタイプによって、スパニングツリーポートを上記いずれかのポートタイプに設定できます。

スパニングツリー エッジポート

エッジポートは、ホストに接続されるポートであり、アクセスポートとトランクポートのどちらにもなります。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經由することなく、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）。

ホストに接続されているインターフェイスは、STPブリッジプロトコルデータユニット（BPDU）を受信してはなりません。



Note 別のスイッチに接続されているポートをエッジポートとして設定すると、ブリッジンググループが発生する可能性があります。

スパニングツリー ネットワーク ポート

ネットワークポートは、スイッチまたはブリッジにだけ接続されます。**Bridge Assurance** がグローバルにイネーブルになっている間にポートをネットワークポートとして設定すると、そのポートで **Bridge Assurance** がイネーブルになります。



Note ホストまたは他のエッジデバイスに接続されている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すると、そ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。

スパニングツリー標準ポート

標準ポートは、ホスト、スイッチ、またはブリッジに接続できます。これらのポートは、標準スパニングツリーポートとして機能します。

デフォルトのスパニングツリー インターフェイスは標準ポートです。

Bridge Assurance の概要

Bridge Assurance を使用すると、ネットワーク内でブリッジング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、単方向リンク障害や、スパニングツリーアルゴリズムを実行しなくなってもデータトラフィックの転送を続けているデバイスなどからネットワークを保護できます。



Note **Bridge Assurance** は、Rapid PVST+ および MST だけでサポートされています。従来の 802.1D スパニングツリーではサポートされていません。

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。

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。

BPDU ガードの概要

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。正しい設定では、LAN エッジインターフェイスは BPDU を受信しません。エッジインターフェイスが BPDU を受信すると、無効な設定（未認証のホストまたはスイッチへの接続など）を知らせるシグナルが送信されます。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 ガードは、無効な設定があると確実に応答を返します。無効な設定をした場合は、当該 LAN インターフェイスを手動でサービス状態に戻す必要があるからです。



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 フィルタリングの概要

BPDU フィルタリングを使用すると、スイッチが特定のポートで BPDU を送信または受信するのを禁止できます。

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ッ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、ブリッジンググループに陥る可能性があります。というのは、そうしたポートは受信した 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。

ポートがデフォルトで BPDU フィルタリングに設定されていない場合は、エッジ設定によって BPDU フィルタリングが影響を受けることはありません。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 7: 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	有効	有効	イネーブルポートは 10 以上の BPDU を送信します。このポートは、BPDU を受信すると、スパニングツリー標準ポート状態に戻り、BPDU フィルタリングはディセーブルになります。
デフォルト	有効	無効	無効
デフォルト	無効	イネーブル化 / ディ セーブル化	無効
無効	イネーブル化 / ディ セーブル化	イネーブル化 / ディ セーブル化	無効
有効	イネーブル化 / ディ セーブル化	イネーブル化 / ディ セーブル化	イネーブル Caution BPDU は送信されませんが、受信した場合には、通常の STP の動作が開始されません。BPDU の使用に当たっては、十分注意してください。

ループ ガードの概要

ループ ガードは、次のような原因によってネットワークでループが発生するのを防ぎます。

- ネットワーク インターフェイスの誤動作
- CPU の過負荷
- BPDU の通常転送を妨害する要因

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。こうした移行は通常、物理的に冗長なトポロジ内のポートの1つ（ブロッキングポートとは限らない）がBPDUの受信を停止すると起こります。

ループガードは、デバイスがポイントツーポイントリンクによって接続されているスイッチドネットワークでだけ役立ちます。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。



Note ループガードは、ネットワークおよび標準のスパニングツリーポートタイプ上だけでイネーブルにできます。

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を受信しないポートを検出すると、ループガードは、そのポートを不整合状態（ブロッキングステート）に移行します。このポートは、再度BPDUの受信を開始するまで、ブロッキングステートのままです。不整合状態のポートはBPDUを送信しません。このようなポートがBPDUを再度受信すると、ループガードはそのループ不整合状態を解除し、STPによってそのポート状態が確定されます。こうしたリカバリは自動的に行われます。

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 ガードの概要

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の送信を停止すると、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。

特定のインターフェイス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するすべてのVLANにルートガード機能が適用されます。

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。



Note ルート ガードはすべてのスパニングツリー ポート タイプ（標準、エッジ、ネットワーク）でイネーブルにできます。

STP 拡張機能の設定

STP 拡張機能の設定における注意事項

STP 拡張機能を設定する場合は、次の注意事項に従ってください。

- ホストに接続されたすべてのアクセス ポートとトランク ポートをエッジ ポートとして設定します。
- 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。
- ループ ガードは、スパニングツリー エッジ ポートでは動作しません。
- ポイントツーポイントリンクに接続していないポートでループガードをイネーブルにはできません。
- ルートガードがイネーブルになっている場合、ループガードをイネーブルにはできません。

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割り当ては、そのポートが接続されているデバイスのタイプによって次のように決まります。

- エッジ：エッジ ポートは、ホストに接続されるポートであり、アクセス ポートとトランク ポートのどちらかです。
- ネットワーク：ネットワーク ポートは、スイッチまたはブリッジだけに接続されます。
- 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。標準ポートは、任意のタイプのデバイスに接続できます。

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

STP が設定されていること。

インターフェイスに接続されているデバイスのタイプに合わせてポートが正しく設定されていること。

SUMMARY STEPS

1. `switch# configure terminal`

2. switch(config)# spanning-tree port type edge default
3. switch(config)# spanning-tree port type network default

DETAILED STEPS

Procedure		
	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# spanning-tree port type edge default	すべてのインターフェイスをエッジポートとして設定します。このコマンドの使用は、すべてのポートがホスト/サーバに接続されていることが前提になります。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。
Step 3	switch(config)# spanning-tree port type network default	<p>すべてのインターフェイスをスパニングツリー ネットワークポートとして設定します。このコマンドの使用は、すべてのポートがスイッチまたはブリッジに接続されていることが前提になります。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。</p> <p>Note ホストに接続され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、そ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。</p>

Example

次に、ホストに接続されたアクセスポートおよびトランクポートをすべて、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# configure terminal
switch(config)# spanning-tree port type edge default
```

次に、スイッチまたはブリッジに接続されたポートをすべて、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# configure terminal
switch(config)# spanning-tree port type network default
```

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:** このコマンドを実行すると、アクセス ポート上のエッジ動作が明示的にイネーブルにされます。
- **spanning-tree port type edge trunk:** このコマンドを実行すると、トランク ポート上のエッジ動作が明示的にイネーブルにされます。



Note **spanning-tree port type edge trunk** コマンドを入力すると、そのポートは、アクセス モードであってもエッジポートとして設定されます。

- **spanning-tree port type normal:** このコマンドを実行すると、ポートは標準スパニングツリーポートとして明示的に設定されますが、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されません。
- **no spanning-tree port type:** このコマンドを実行すると、**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、エッジ動作が暗黙にイネーブルにされます。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 disable** コマンドと同じです。

Before you begin

STP が設定されていること。

インターフェイスがホストに接続されていること。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **spanning-tree port type edge**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。

	Command or Action	Purpose
Step 2	switch(config)# interface <i>type slot/port</i>	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。
Step 3	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 ステートを經由することなく、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。

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# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree port type edge
```

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:** このコマンドを実行すると、指定したポートが明示的にネットワーク ポートとして設定されます。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** — このコマンドを実行すると、ポートが明示的に標準スパニングツリー ポートとして設定されます。このインターフェイス上では Bridge Assurance は動作しません。
- **no spanning-tree port type:** このコマンドを実行すると、**spanning-tree port type network default** コマンドをグローバル コンフィギュレーションモードで定義した場合に、ポートが暗黙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されます。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

ホストに接続されているポートをネットワーク ポートとして設定すると、そ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。

Before you begin

STP が設定されていること。

インターフェイスがスイッチまたはルータに接続されていること。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** type slot/port
3. switch(config-if)# **spanning-tree port type network**

DETAILED STEPS**Procedure**

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface type slot/port	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。インターフェイスには、物理イーサネット ポートを指定できます。
Step 3	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。

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# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree port type network
```

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

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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree port type edge bpduguard default**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	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。

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# configure terminal
```

```
switch(config)# spanning-tree port type edge bpduguard default
```

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:** インターフェイスで BPDU ガードを無条件でイネーブルにします。
- **spanning-tree bpduguard disable:** インターフェイスで BPDU ガードを無条件でディセーブルにします。

- **no spanning-tree bpduguard**: 動作中のエッジ ポート インターフェイスに **spanning-tree port type edge bpduguard default** コマンドが設定されている場合、そのインターフェイスで BPDU ガードをイネーブルにします。

Before you begin

STP が設定されていること。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. switch(config-if)# **spanning-tree bpduguard {enable | disable}**
4. (Optional) switch(config-if)# **no spanning-tree bpduguard**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface <i>type slot/port</i>	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。
Step 3	switch(config-if)# spanning-tree bpduguard {enable disable}	指定したスパン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、BPDU ガードは、物理イーサネット インターフェイスではディセーブルです。
Step 4	(Optional) switch(config-if)# no spanning-tree bpduguard	<p>インターフェイス上で BPDU ガードをディセーブルにします。</p> <p>Note 動作中のエッジ ポート インターフェイスで、spanning-tree port type edge bpduguard default コマンドを入力した場合、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。</p>

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# configure terminal
switch (config)# interface ethernet 1/4
```

```
switch(config-if) # spanning-tree bpduguard enable
switch(config-if) # no spanning-tree bpduguard
```

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にされたエッジポートは、BPDUを受信すると、エッジポートとしての動作ステータスを失い、通常の STP 状態遷移を再開します。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には注意してください。誤って使用すると、ブリッジンググループが発生するおそれがあります。



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。

Before you begin

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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree port type edge bpdupfilter default**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# spanning-tree port type edge bpdupfilter 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。

Example

次に、すべての動作中のスパンニングツリー 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# configure terminal
switch(config)# spanning-tree port type edge bpdupfilter default
```

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、トランッ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

指定インターフェイスで **spanning-tree bpdupfilter enable** コマンドを入力する場合は注意してください。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、ブリッジンググループに陥る可能性があります。というのは、そうしたポートは受信した 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。

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 bpdupfilter enable:** インターフェイス上の BPDU フィルタリングを無条件にイネーブルにします。
- **spanning-tree bpdupfilter disable:** インターフェイス上の BPDU フィルタリングを無条件にディセーブルにします。
- **no spanning-tree bpdupfilter:** 動作中のエッジ ポート インターフェイスに **spanning-tree port type edge bpdupfilter 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。



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。

Before you begin

STP が設定されていること。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **spanning-tree bpdupfilter {enable | disable}**
4. (Optional) switch(config-if)# **no spanning-tree bpdupfilter**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface type slot/port	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。
Step 3	switch(config-if)# spanning-tree bpdupfilter {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。
Step 4	(Optional) switch(config-if)# no spanning-tree bpdupfilter	<p>インターフェイス上で BPDU フィルタリングをディセーブルにします。</p> <p>Note 動作中のエッジポートインターフェイスに spanning-tree port type edge bpdupfilter 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。</p>

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# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpdupfilter enable
```

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

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. switch# **configure terminal**
2. switch(config)# **spanning-tree loopguard default**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	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。

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# configure terminal
switch(config)# spanning-tree loopguard default
```

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

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。

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を禁止されます。ループガードは、単方向リンクを発生させる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。

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

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. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. switch(config-if)# **spanning-tree guard** {**loop** | **root** | **none**}

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface <i>type slot/port</i>	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。
Step 3	switch(config-if)# spanning-tree guard { loop root none }	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。 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。

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# configure terminal
```

```
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree guard root
```

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、次のコマンドを使用します。

コマンド	目的
show running-config spanning-tree [all]	スイッチ上でスパニングツリーの最新ステータスを表示します。
show spanning-tree [options]	最新のスパニングツリー設定について、指定した詳細情報を表示します。



第 9 章

Flex Link の設定

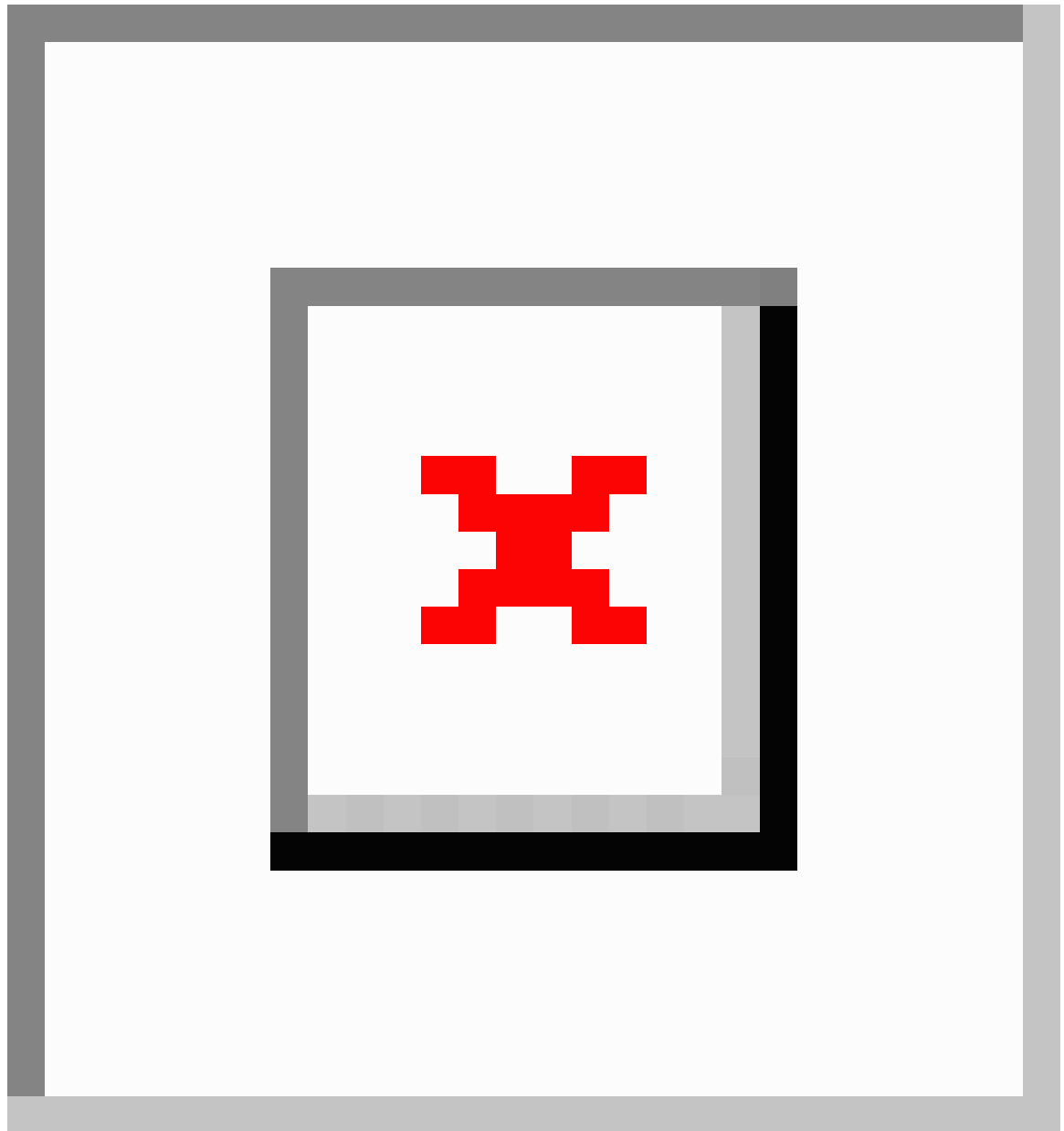
- [Flex Link について（139 ページ）](#)
- [Flex Link の注意事項および制約事項（142 ページ）](#)
- [Flex Link のデフォルト設定（143 ページ）](#)
- [Flex Link の設定（143 ページ）](#)
- [Flex Link プリエンプションの設定（145 ページ）](#)
- [Flex Link 設定の確認（147 ページ）](#)

Flex Link について

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、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ます。この機能は、スパニングツリー プロトコル（STP）の代替ソリューションです。STP をディセーブルにしても、基本的リンク冗長性を保つことができます。Flex Link は、通常、お客様がスイッチで STP を実行しない場合のサービス プロバイダーまたは企業ネットワークに設定されます。スイッチが STP を実行中の場合は、STP がすでにリンクレベルの冗長性またはバックアップを提供しているため、Flex Link は不要です。

別のレイヤ 2 インターフェイスを Flex Link またはバックアップリンクとして割り当てることで、1 つのレイヤ 2 インターフェイス（アクティブリンク）に Flex Link を構成できます。Flex Link インターフェイスは、同じスイッチ上に設定できます。リンクの 1 つがアップでトラフィックを転送しているときは、もう一方のリンクがスタンバイモードで、このリンクがシャットダウンした場合にトラフィックの転送を開始できるように準備しています。どの時点でも、1 つのインターフェイスのみがリンクアップ状態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。デフォルトでは、Flex Link は構成されておらず、バックアップ インターフェイスは定義されていません。STP は Flex Link インターフェイスでディセーブルです。

図 17: Flex Link の設定例



Flex Link の構成例では、スイッチ A と B はダウンリンク スイッチです。スイッチ A と B の中のポート 1 と 2 は、アップリンク スイッチ C と D に接続されています。これらのスイッチは Flex Link として構成されているので、どちらかのインターフェイスがトラフィックを転送し、もう一方のインターフェイスはスタンバイモードになります。トラフィックを転送しているインターフェイスが現用系インターフェイスです。スイッチ A にあるポート 1 がアクティブ インターフェイスである場合、ポート 1 とスイッチ D 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 インターフェイス）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。

Flex Link はレイヤ 2 ポートおよびポート チャネルだけでサポートされ、VLAN またはレイヤ 3 ポートではサポートされません。STP、VPC、レイヤー 2 マルチパスなどの他のタイプの冗長性が不要または望ましくないスイッチ トポロジにリンク冗長性を提供します。

プリエンブション

オプションで、現用系インターフェイスを指定するプリエンブション メカニズムを設定できます。たとえば、Flex Link ペアをプリエンブションモードで設定することにより、ピア ポートより帯域幅の大きいポートが動作を再開し、ポートが 60 秒後に転送を開始してピア ポートがスタンバイとなります。これを行うには、`preemption mode bandwidth` および `delay` コマンドを入力します。

プライマリ（転送）リンクがダウンすると、ネットワーク管理ステーションが通知を受けます。スタンバイ リンクがダウンすると、通知されます。

プリエンブションは、次の 3 つのモードで設定できます。

- 強制 - 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。
- 帯域幅 - 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。
- オフ - プリエンブションはありません。機能している最初のインターフェイスが転送モードになります。

また、別のインターフェイスに代わって現用インターフェイスをプリエンブションする前に、プリエンブション遅延を指定した時間（秒単位）で設定することもできます。これにより、スイッチの切り替え前にアップストリーム スwitch の対応スイッチが STP フォワーディング ステートに移行されます。

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。

Flex Link の注意事項および制約事項

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 インターフェイスで、スパン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。
- 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。
- 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。

- 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。



(注) Flex Link は、Nexus 3500 シリーズ スイッチでのみサポートされます。Nexus 3000 または Nexus 3100 シリーズ スイッチでは Flex Link を構成できません。

Flex Link のデフォルト設定

表 8: Flex Link のデフォルト パラメータの設定

パラメータ	定義
Multicast Fast-Convergence	ディセーブル
プリエンブション モード	消灯
プリエンブション遅延	35 秒

Flex Link 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。

手順の概要

1. switch# **configure terminal**
2. switch(config) # **feature flexlink**
3. switch(config) # **interface** {*ethernet slot/port* | *port-channel channel-no* }
4. switch(config-if) # **switchport backup interface** {*ethernet slot/port* | *port-channel channel-no*} [**multicast fast-convergence**]
5. (任意) switch(config-if) # **end**
6. (任意) switch# **show interface switchport backup**
7. (任意) switch# **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
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config) # feature flexlink	Flex Link をイネーブルにします。
Step 3	switch(config) # 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。 指定できるポートチャネルは 1 ～ 48 です。
Step 4	switch(config-if) # 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。 <ul style="list-style-type: none"> • 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。
Step 5	(任意) switch(config-if) # end	特権 EXEC モードに戻ります。
Step 6	(任意) switch# show interface switchport backup	設定を確認します。
Step 7	(任意) switch# 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 Link のペアにプリエンプション スキームを構成できます。

始める前に

Flex Link 機能をイネーブル化します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet slot/port**
3. switch(config-if)# **switchport backup interface ethernet slot/port**
4. switch(config-if)# **switchport backup interface ethernet slot/port preemption mode [bandwidth | forced | off]**
5. switch(config-if)# **switchport backup interface ethernet slot/port preemption delay delay-time**
6. （任意）switch(config-if)# **end**
7. （任意）switch# **show interface switchport backup**
8. （任意）switch# **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
Step 1	<code>switch# configure terminal</code>	グローバル構成モードを開始します。
Step 2	<code>switch(config)# interface ethernet slot/port</code>	<p>イーサネット 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。</p> <p>インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）です。</p> <p>スロット / ポートの範囲は 1 ～ 48 です。</p>
Step 3	<code>switch(config-if)# switchport backup interface ethernet slot/port</code>	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。
Step 4	<code>switch(config-if)# switchport backup interface ethernet slot/port preempt mode [bandwidth forced off]</code>	<p>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。</p> <ul style="list-style-type: none"> • 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。 <p>Flex Link インターフェイス ペアのプリエンプションメカニズムとを構成します。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。</p> <ul style="list-style-type: none"> • 帯域幅: より大きい帯域幅のインターフェイスが常に現用系 インターフェイスとして動作します。 • 強制: 現用系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。 • オフ: 現用系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。
Step 5	<code>switch(config-if)# switchport backup interface ethernet slot/port preempt delay delay-time</code>	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

	コマンドまたはアクション	目的
		す。デフォルトのプリエンプション遅延は 35 秒です。 (注) 遅延時間の設定は、forced モードおよび bandwidth モードでのみ有効です。
Step 6	(任意) switch(config-if)# end	特権 EXEC モードに戻ります。
Step 7	(任意) switch# show interface switchport backup	設定を確認します。
Step 8	(任意) switch# 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、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)		

Flex Link 設定の確認

次のコマンドを使用すると、Flex Link の設定情報を表示することができます。

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。

コマンド	目的
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。
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。

例

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構成を表示します。

```
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構成を表示します。

```
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
```



第 10 章

LLDP の設定

- [LLDP の設定, on page 151](#)
- [インターフェイス LLDP の設定, on page 153](#)
- [LLDP の MIB \(155 ページ\)](#)

LLDP の設定

Before you begin

スイッチでリンク層検出プロトコル（LLDP）機能がイネーブルになっていることを確認します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch# **feature lldp**
3. switch(config)# **lldp {holdtime seconds | reinit seconds | timer seconds | tlv-select {dcbxp | management-address | power management | port-description | port-vlan | system-capabilities | system-description | system-name}}**
4. switch(config)# **no lldp {holdtime | reinit | timer}**
5. （任意）switch# **show lldp**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch# feature lldp	LLDP をイネーブルにします。
Step 3	switch(config)# lldp {holdtime seconds reinit seconds timer seconds tlv-select {dcbxp management-address	LLDP オプションを設定します。

	Command or Action	Purpose
	power management port-description port-vlan system-capabilities system-description system-name }	<p>holdtime オプションを使用して、デバイスが受信した LLDP 情報を廃棄するまでの保存時間を設定します（10 ～ 255 秒）。デフォルト値は 120 秒です。</p> <p>reinit オプションを使用して、任意のインターフェイスで LLDP 初期化を実行するまでの待機時間を設定します（1 ～ 10 秒）。デフォルト値は 2 秒です。</p> <p>timer オプションを使用して、LLDP パケットを送信するレートを設定します（5 ～ 254 秒）。デフォルト値は 30 秒です。</p> <p>tlv-select オプションを使用して、Type Length Value (TLV) を指定します。デフォルトでは、すべての TLV の送受信がイネーブルです。</p> <p>dcbxp オプションを使用して、Data Center Ethernet Parameter Exchange (DCBXP) TLV メッセージを指定します。</p> <p>management-address オプションを使用して、管理アドレス TLV メッセージを指定します。</p> <p>power management オプションを使用して、LLDP の電源管理 TLV を指定します。</p> <p>port-description オプションを使用して、ポート記述 TLV メッセージを指定します。</p> <p>port-vlan オプションを使用して、ポート VLAN ID TLV メッセージを指定します。</p> <p>system-capabilities オプションを使用して、システム機能 TLV メッセージを指定します。</p> <p>system-description オプションを使用して、システム記述 TLV メッセージを指定します。</p> <p>system-name オプションを使用して、システム名 TLV メッセージを指定します。</p>
Step 4	switch(config)# no lldp { holdtime reinit timer }	LLDP 値をデフォルトにリセットします。
Step 5	(任意) switch# show lldp	LLDP の設定を表示します。

Example

次に、グローバルな LLDP ホールドタイムを 200 秒に設定する例を示します。

```
switch# configure terminal
switch(config)# lldp holdtime 200
```

```
switch(config)#
```

次に、LLDP をイネーブルにして管理アドレス TLV を送受信する例を示します。

```
switch# configure terminal
switch(config)# lldp tlv-select management-address
switch(config)#
```

インターフェイス LLDP の設定

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. switch(config-if)# [**no**] **lldp** {**receive** | **transmit**}
4. (Optional) switch# **show lldp** {**interface** | **neighbors** [**detail** | **interface** | **system-detail**] | **timers** | **traffic**}

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface <i>type slot/port</i>	変更するインターフェイスを選択します。
Step 3	switch(config-if)# [no] lldp { receive transmit }	選択したインターフェイスを受信または送信に設定します。 このコマンドの no 形式を使用すると、LLDP の送信または受信をディセーブルにします。
Step 4	(Optional) switch# show lldp { interface neighbors [detail interface system-detail] timers traffic }	LLDP の設定を表示します。

Example

次に、LLDP パケットを送信するようインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# lldp transmit
```

次に、LLDP をディセーブルにするようインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
```

```
switch(config-if)# no lldp transmit
switch(config-if)# no lldp receive
```

次に、LLDP インターフェイス情報を表示する例を示します。

```
switch# show lldp interface ethernet 1/2
tx_enabled: TRUE
rx_enabled: TRUE
dcbx_enabled: TRUE
Port MAC address:    00:0d:ec:a3:5f:48
Remote Peers Information
No remote peers exist
```

次に、LLDP ネイバーの情報を表示する例を示します。

```
switch# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf      Hold-time  Capability  Port ID
SW-INSBU-JWALA-PP52.cisco.com
                    mgmt0          120        B           Gi1/0/37
MTC-2               Eth1/41         120        BR          Ethernet1/43
MTC-CR2             Eth1/42         120        BR          Ethernet1/43
MTC-CR2             Eth1/43         120        BR          Ethernet1/42
MTC-2               Eth1/44         120        BR          Ethernet1/41
MTC-CR2             Eth1/45         120        BR          Ethernet1/41
MTC-2               Eth1/46         120        BR          Ethernet1/44
MTC-2               Eth1/47         120        BR          Ethernet1/42
MTC-CR2             Eth1/48         120        BR          Ethernet1/44
Total entries displayed: 9
```

次に、LLDP ネイバーに関するシステムの詳細を表示する例を示します。

```
switch# sh lldp neighbors system-detail
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID Local Intf Chassis ID PortID Hold-time Capability
switch-2  Eth1/7   0005.73b7.37ce Eth1/7   120 B
switch-3  Eth/9     0005.73b7.37d0 Eth1/9   120 B
switch-4  Eth1/10  0005.73b7.37d1 Eth1/10  120 B
Total entries displayed: 3
```

次に、LLDP タイマー情報を表示する例を示します。

```
switch# show lldp timers
LLDP Timers
holdtime 120 seconds
reinit 2 seconds
msg_tx_interval 30 seconds
```

次に、LLDP カウンタに関する情報を表示する例を示します。

```
switch# show lldp traffic
```


LLDP traffic statistics:

Total frames out: 8464

Total Entries aged: 6

Total frames in: 6342

Total frames received in error: 2

Total frames discarded: 2

Total TLVs unrecognized: 0

LLDP の MIB

MIB	リンク
LLDP-MIB	ftp://ftp.cisco.com/pub/mibs/supportlists/nexus3000/Nexus3000MIBSupportList.html



第 11 章

MAC アドレス テーブルの構成

- [MAC アドレスに関する情報, on page 157](#)
- [MAC アドレスの構成 \(158 ページ\)](#)
- [MAC 移動ループ検出の設定 \(161 ページ\)](#)
- [MAC アドレス設定の確認, on page 162](#)

MAC アドレスに関する情報

LAN ポート間でフレームをスイッチングするために、スイッチはアドレステーブルを保持しています。スイッチがフレームを受信すると、送信側のネットワーク デバイスの MAC アドレスを受信側の LAN ポートにアソシエートします。

スイッチは、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 テーブルを動的に構築します。そのアドレス テーブルにリストされていない受信側 MAC アドレスのフレームを受信すると、そのフレームを、同一 VLAN のフレームを受信したポート以外のすべての LAN ポートへフラッドします。送信先ステーションが応答したら、スイッチは、その関連の送信元 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。その後、スイッチは、以降のフレームを、すべての LAN ポートにフラッドするのではなく単一の LAN ポートへと転送します。

MAC アドレスを手作業で入力することもできます。これは、テーブル内で、スタティック MAC アドレスとなります。このようなスタティック MAC エントリは、スイッチを再起動しても維持されます。

マルチキャスト アドレスは、静的に設定された MAC アドレスとしては入力できません (IP マルチキャストおよび非 IP マルチキャスト MAC アドレスの両方)。これは N3548 プラットフォームではサポートされません。

アドレステーブルには、フレームを一切フラッドさせることなく、複数のユニキャストアドレスエントリを格納できます。スイッチは設定可能なエイジングタイマーによって定義されたエイジングメカニズムを使用するため、アドレスが非アクティブなまま指定した秒数が経過すると、そのアドレスはアドレス テーブルから削除されます。

MAC アドレスの構成

スタティック MAC アドレスの設定

スイッチの静的MACアドレスを構成できます。これらのアドレスは、インターフェイス構成モードまたは VLAN 構成モードで構成できます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config) # **mac address-table static** *mac_address* **vlan** *vlan-id* {**drop** | **interface** {*type slot/port*} | **port-channel** *number*}
3. (Optional) switch(config)# **no mac address-table static** *mac_address* **vlan** *vlan-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config) # mac address-table static <i>mac_address</i> vlan <i>vlan-id</i> { drop interface { <i>type slot/port</i> } port-channel <i>number</i> }	MAC アドレス テーブルに追加するスタティック アドレスを指定します。
Step 3	(Optional) switch(config)# no mac address-table static <i>mac_address</i> vlan <i>vlan-id</i>	MAC アドレス テーブルからスタティック エントリを削除します。 mac address-table static コマンドで静的 MAC アドレスを仮想インターフェイスに割り当てます。

Example

次に、MAC アドレス テーブルにスタティック エントリを登録する例を示します。

```
switch# configure terminal
switch(config) # mac address-table static 12ab.47dd.ff89 vlan 3 interface ethernet 1/4
switch(config) #
```

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
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface <i>type slot/port</i>	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。
Step 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。
Step 4	switch(config-if)# clear mac address-table dynamic interface <i>type slot/port</i>	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

エントリ（パケット送信元の MAC アドレスとそのパケットが入ってきたポート）が MAC テーブル内に留まる時間を設定できます。MAC エージング タイムは、インターフェイス構成モードまたは VLAN 構成モードで設定できます。



（注） Cisco Nexus デバイスは VLAN 単位の CAM エージング タイマーをサポートしません。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **mac-address-table aging-time seconds**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# mac-address-table aging-time seconds	エントリが無効になって、MAC アドレス テーブルから破棄されるまでの時間を指定します。 [秒（seconds）] の範囲は 0 ～ 1000000 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。

例

次に、MAC アドレス テーブル内エントリのエージング タイムを 1800 秒（30 分）に設定する例を示します：

```
switch# configure terminal
switch(config) # mac-address-table aging-time 1800
switch(config) #
```

MAC テーブルからのダイナミック アドレスのクリア

MAC アドレス テーブルからすべてのダイナミック エントリを消去できます。

コマンド	目的
<code>switch(config)# clear mac-address-table dynamic {address mac-addr} {interface [type slot/port port-channel number]} {vlan vlan-id}</code>	MAC アドレス テーブルからダイナミック アドレス エントリを消去します。

次に、MAC アドレス テーブル内のダイナミック エントリを消去する例を示します。

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

MAC 移動ループ検出の設定

2つのポート間でのMACアドレス移動数がしきい値を超えると、それによってループが形成されます。**mac address-table loop-detect port-down** コマンドを使用して、このようなループが検出されたときに、インターフェイス インデックスが低いポートをダウンさせるアクションを設定できます。MAC ラーニングをディセーブルにするデフォルト アクションに戻すには、このコマンドの **no** 形式を使用します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **[no] mac address-table loop-detect port-down**
3. switch(config)# **mac address-table loop-detect port-down edge-port**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 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。
Step 2	switch(config)# [no] mac address-table loop-detect port-down	MAC 移動ループ検出用のポート ダウン アクションを指定します。このコマンドの no 形式は、MAC ラーニングを 180 秒間ディセーブルにするデフォルト アクションに戻します。
Step 3	switch(config)# mac address-table loop-detect port-down edge-port	MAC 移動ループ検出のエッジ ポートの err-disabled 検出をイネーブル化します。

例

次に、MAC 移動ループ検出用のアクションとしてポート ダウンを構成する例を示します。

```
switch# configure terminal
switch(config)# mac address-table loop-detect port-down
```

次の例は、MAC 移動ループ検出のエッジポートの err-disabled 検出を有効にする方法を示しています。

```
switch# configure terminal
switch(config)# mac address-table loop-detect port-down edge-port
```

MAC アドレス設定の確認



Note Cisco Nexus 3000 および Cisco Nexus 3548 シリーズ プラットフォームでは、セルフ ルータの MAC または HSRP VMAC は、次の条件下でスイッチによって動的学習されます。

- スイッチが自身のパケットを受信するためにネットワークに一時的なループがある場合。
- 送信元 MAC がルータ MAC または HSRP MAC と同じであるスプーフィングされたパケットがある場合。

この動作は、他の Cisco Nexus プラットフォームとは異なります。ただし、MAC テーブルに存在するこれらの自己 MAC エントリによる操作上の影響はありません。ルータ MAC または HSRP MAC 宛てのパケットはすべて回送されます。これらのパケットにはレイヤ 2 ルックアップはありません。

次のいずれかのコマンドを使用して、設定を確認します。

Table 9: MAC アドレス構成の確認コマンド

コマンド	目的
show mac address-table aging-time	スイッチ内で定義されているすべての VLAN の MAC アドレスの経過時間を表示します。
show mac address-table	MAC アドレス テーブルの内容を表示します。 Note IGMP スヌーピングによって学習された MAC アドレスは表示されません。
show mac address-table loop-detect	現在構成されているアクションを表示します。

次に、MAC アドレス テーブルを表示する例を示します。


```
switch# show mac address-table
VLAN      MAC Address      Type    Age      Port
-----+-----+-----+-----+-----
1         0018.b967.3cd0    dynamic 10       Eth1/3
1         001c.b05a.5380    dynamic 200      Eth1/3
Total MAC Addresses: 2
```

次に、現在のエージング タイムを表示する例を示します。

```
switch# show mac address-table aging-time
Vlan  Aging Time
-----
1      300
13     300
42     300
```

次に、現在構成されているアクションを表示する例を示します。

```
switch# configure terminal
switch(config)# show mac address-table loop-detect
Port Down Action Mac Loop Detect : enabled

switch# configure terminal
switch(config)# no mac address-table loop-detect port-down
switch(config)# show mac address-table loop-detect
Port Down Action Mac Loop Detect : disabled
```




第 12 章

IGMP スヌーピングの設定

- [IGMP スヌーピングの情報, on page 165](#)
- [IGMP スヌーピング パラメータの設定, on page 168](#)
- [IGMP スヌーピング設定の確認, on page 172](#)

IGMP スヌーピングの情報

IGMP スヌーピング ソフトウェアは、VLAN 内の IGMP プロトコル メッセージを調べて、このトラフィックの受信に関連のあるホストまたはその他のデバイスに接続されているのはどのインターフェイスかを検出します。IGMP スヌーピングは、インターフェイス情報を使用して、マルチアクセス ローカル エリア ネットワーク（LAN）環境での帯域幅消費を減らすことができ、これによって VLAN 全体のフラグディングを防ぎます。IGMP スヌーピング機能は、どのポートがマルチキャスト対応ルータに接続されているかを追跡して、IGMP メンバーシップ レポートの転送管理を支援します。トポロジの変更通知には、IGMP スヌーピング ソフトウェアが応答します。

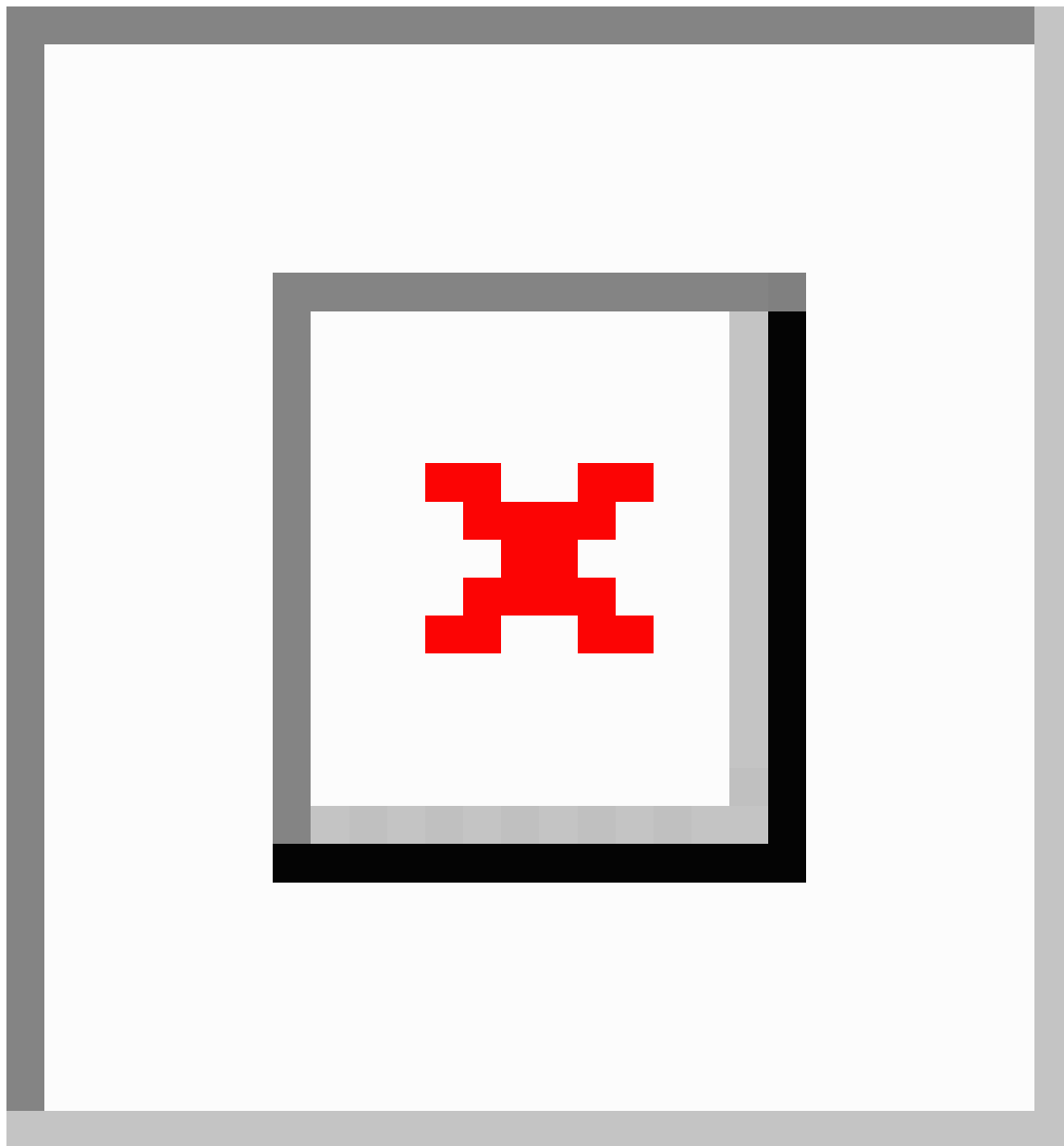


Note IGMP スヌーピングは、すべてのイーサネット インターフェイスでサポートされます。ただし、PVLANではサポートされていません。[スヌーピング (*snooping*)] という用語が使用されるのは、レイヤ 3 コントロールプレーン パケットが代行受信され、レイヤ 2 の転送判断に影響を与えるためです。

Cisco NX-OS は、IGMPv2 と IGMPv3 をサポートします。IGMPv2 は IGMPv1 をサポートし、IGMPv3 は IGMPv2 をサポートします。以前のバージョンの IGMP のすべての機能がサポートされるわけではありませんが、メンバーシップ クエリとメンバーシップ レポートに関連した機能はすべての IGMP バージョンについてサポートされます。

次の図に、ホストと IGMP ルータの間に置かれた IGMP スヌーピング スイッチを示します。IGMP スヌーピング スイッチは、IGMP メンバーシップ レポートと脱退メッセージをスヌーピングし、それらを必要な場合にだけ、接続されている IGMP ルータに転送します。

Figure 18: IGMP スヌーピング スイッチ



Cisco NX-OS IGMP スヌーピング ソフトウェアは、最適化されたマルチキャスト フラッドイング（OMF）をサポートします。これは、不明トラフィックをルータだけに転送し、データ駆動の状態生成は一切実行しません。IGMP スヌーピングの詳細については、<http://tools.ietf.org/wg/magma/draft-ietf-magma-snoop/rfc4541.txt> を参照してください。

IGMPv1 および IGMPv2

IGMPv1 と IGMPv2 は両方とも、メンバーシップ レポート抑制をサポートします。つまり、同一サブネット上の 2 つのホストが同一グループのマルチキャスト データを受信する場合、他方のホストからメンバー レポートを受信するホストは、そのレポートを送信しません。メンバーシップ レポート抑制は、同じポートを共有しているホスト間で発生します。

各 VLAN スイッチ ポートに接続されているホストが 1 つしかない場合は、IGMPv2 の高速脱退機能を設定できます。高速脱退機能を使用すると、最終メンバーのクエリー メッセージがホストに送信されません。ソフトウェアは IGMP Leave メッセージを受信すると、ただちに該当するポートへのマルチキャスト データ転送を停止します。

IGMPv1 では、明示的な IGMP Leave メッセージが存在しないため、特定のグループについてマルチキャスト データを要求するホストが存続しないことを示すために、メンバーシップ メッセージ タイムアウトが利用されます。



Note Cisco NX-OS 高速脱退機能がイネーブルになっている場合、他のホストの存在は確認されないため、最終メンバーのクエリー インターバル構成が無視されます。

IGMPv3

スイッチ上の IGMPv3 スヌーピングの実装は、アップストリーム マルチキャスト ルータが送信元に基づいたフィルタリングを行えるように、IGMPv3 レポートを転送します。

ソフトウェアのデフォルト設定では、各 VLAN ポートに接続されたホストが追跡されます。この明示的なトラッキング機能は、高速脱退メカニズムをサポートしています。

IGMPv3 メンバーシップ レポートには LAN セグメント上のグループ メンバの一覧が含まれていますが、最終ホストが脱退すると、メンバーシップ クエリーが送信されます。最終メンバーのクエリー インターバルについてパラメータを設定すると、タイムアウトまでにどのホストからも応答がなかった場合に、グループ ステートが解除されます。

IGMP スヌーピング クエリア

クエリーを発生させる VLAN 内にマルチキャスト ルータが存在しない場合、IGMP スヌーピング クエリアを設定して、メンバーシップ クエリーを送信させる必要があります。

IGMP スヌーピング クエリアがイネーブルな場合は、定期的に IGMP クエリーが送信されるため、IP マルチキャスト トラフィックを要求するホストから IGMP レポート メッセージが発信されます。IGMP スヌーピングはこれらの IGMP レポートを待ち受けて、適切な転送を確立します。

現在は、スイッチ クエリアと IGMP スヌーピング クエリアに対して同じ SVI IP アドレスを設定できます。そうすれば、両方のクエリアが同時にアクティブになって、一般的なクエリーを定期的に VLAN に送信するようになります。これを回避するには、IGMP スヌーピング クエリアとスイッチ クエリアで別々の IP アドレスを使用します。

IGMP フォワーディング

Cisco Nexus デバイスのコントロールプレーンは、IP アドレスを検出できますが、転送は [IP マルチキャスト グループ (IP multicast group)] だけを使用して発生します。

スイッチに接続されているホストは、IP マルチキャスト グループに参加する場合に、参加する IP マルチキャスト グループを指定して、要求されていない IGMP 参加メッセージを送信します。それとは別に、スイッチは、接続されているルータから一般クエリーを受信したら、そのクエリーを、物理インターフェイスか仮想インターフェイスにかかわらず、VLAN 内のすべてのインターフェイスに転送します。マルチキャスト グループに参加するホストは、スイッチに参加メッセージを送信することにより応答します。スイッチの CPU が、そのグループ用のマルチキャスト転送テーブルエントリを作成します（まだ存在しなかった場合）。また、CPU は、参加メッセージを受信したインターフェイスを、転送テーブルのエントリに追加します。そのインターフェイスと対応付けられたホストが、そのマルチキャストグループ用のマルチキャストトラフィックを受信します。

ルータはマルチキャスト一般クエリーを定期的に送信し、スイッチはそれらのクエリーを VLAN のすべてのポートを通じて転送します。関心のあるホストがクエリーに応答します。VLAN 内の少なくとも 1 つのホストがマルチキャストトラフィックを受信するようなら、ルータは、その VLAN へのマルチキャストトラフィックの転送を続行します。スイッチは、そのマルチキャストグループの転送テーブルにリストされているホストだけにマルチキャストグループトラフィックを転送します。

ホストがマルチキャストグループから脱退するときには、ホストは、通知なしで脱退することもできれば、脱退メッセージを送信することもできます。スイッチは、ホストから脱退メッセージを受信したら、グループ固有のクエリーを送信して、そのインターフェイスに接続されているその他のデバイスの中に、そのマルチキャストグループのトラフィックを受信するものがあるかどうかを調べます。スイッチはさらに、転送テーブルでその [IP マルチキャストグループ (IP multicast group)] の情報を更新し、そのグループのマルチキャストトラフィックの受信に関心のあるホストだけが、転送テーブルに指定されるようにします。ルータが VLAN からレポートを受信しなかった場合、その VLAN 用のグループは IGMP キャッシュから削除されます。

IGMP スヌーピング パラメータの設定

IGMP スヌーピング プロセスの動作を管理するには、次の表に示すオプションの IGMP スヌーピング パラメータを設定します。

Table 10: IGMP スヌーピング パラメータ

パラメータ	説明
IGMP スヌーピング	VLAN ごとに IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。 Note グローバルな設定がディセーブルになっている場合は、すべての VLAN がイネーブル化されてるかどうか関係なくディセーブル化されていると見なされます。
明示的な追跡	各ポートに接続されたそれぞれのホストから送信される IGMPv2 と IPMPv3 メンバーシップ レポートを、VLAN 別に追跡します。デフォルトではイネーブルになっています。
高速脱退	ソフトウェアが IGMP Leave レポートを受信した場合に、IGMP クエリーメッセージを送信することなく、グループ ステートを解除できるようにします。このパラメータは、IGMPv2 ホストに関して、各 VLAN ポート上のホストが1つしか存在しない場合に使用されます。デフォルトではディセーブルになっています。
最終メンバー クエリ 間隔	IGMP クエリーの送信後に待機する時間を設定します。この時間が経過すると、ソフトウェアは、特定のマルチキャスト グループについてネットワーク セグメント上に受信要求を行うホストが存在しないと見なします。いずれのホストからも応答がないまま、最終メンバのクエリ インターバルの期限が切れると、対応する VLAN ポートからグループが削除されます。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。
スヌーピング クエリア	クエリーを生成するマルチキャスト ルータが VLAN 内に存在しない場合に、インターフェイスのスヌーピング クエリアを設定します。デフォルトではディセーブルになっています。
レポート抑制	マルチキャスト対応ルータに送信されるメンバーシップレポートトラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトではイネーブルになっています。
マルチキャスト ルータ	マルチキャスト ルータへのスタティック接続を設定します。ルータと接続するインターフェイスが、選択した VLAN に含まれている必要があります。
スタティック グループ	VLAN に属するインターフェイスを、マルチキャスト グループのスタティック メンバとして設定します。

IGMP スヌーピングは、グローバルにも、特定の VLAN に対してだけでもディセーブル化できます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **ip igmp snooping**
3. switch(config)# **vlan configuration** *vlan-id*
4. switch(config-vlan)# **ip igmp snooping**
5. switch(config-vlan)# **ip igmp snooping explicit-tracking**
6. switch(config-vlan)# **ip igmp snooping fast-leave**
7. switch(config-vlan)# **ip igmp snooping last-member-query-interval** *seconds*
8. switch(config-vlan)# **ip igmp snooping querier** *IP-address*
9. switch(config-vlan)# **ip igmp snooping report-suppression**
10. switch(config-vlan)# **ip igmp snooping mrouter interface** *interface*
11. switch(config-vlan)# **ip igmp snooping static-group** *group-ip-addr* [*source source-ip-addr*] **interface** *interface*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# ip igmp snooping	IGMP スヌーピングをグローバルにイネーブルにします。デフォルトではイネーブルになっています。 Note グローバルな設定がディセーブルになっている場合は、すべての VLAN がイネーブル化されてるかどうかわ関係なくディセーブル化されていると見なされます。
Step 3	switch(config)# vlan configuration <i>vlan-id</i>	VLAN コンフィギュレーション モードを開始します。
Step 4	switch(config-vlan)# ip igmp snooping	現在の VLAN に対して IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。 Note IGMP スヌーピングがグローバルにイネーブルになっている場合は、このコマンドは必要ありません。
Step 5	switch(config-vlan)# ip igmp snooping explicit-tracking	各ポートに接続されたそれぞれのホストから送信される IGMPv2 と IGMPv3 メンバーシップ レポートを、VLAN 別に追跡します。デフォルトは、すべての VLAN でイネーブルです。

	Command or Action	Purpose
Step 6	switch(config-vlan)# ip igmp snooping fast-leave	IGMPv2 プロトコルのホスト レポート抑制メカニズムのために、明示的に追跡できない IGMPv2 ホストをサポートします。高速脱退がイネーブルの場合、IGMP ソフトウェアは、各 VLAN ポートに接続されたホストが 1 つだけであると見なします。デフォルトは、すべての VLAN でディセーブルです。
Step 7	switch(config-vlan)# ip igmp snooping last-member-query-interval <i>seconds</i>	いずれのホストからも IGMP クエリーメッセージへの応答がないまま、最終メンバのクエリーインターバルの期限が切れた場合に、関連する VLAN ポートからグループを削除します。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。
Step 8	switch(config-vlan)# ip igmp snooping querier <i>IP-address</i>	マルチキャストトラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、スヌーピング クエリアを設定します。IP アドレスは、メッセージの送信元として使用します。デフォルトではディセーブルになっています。
Step 9	switch(config-vlan)# ip igmp snooping report-suppression	マルチキャスト対応ルータに送信されるメンバシップ レポート トラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトではイネーブルになっています。
Step 10	switch(config-vlan)# ip igmp snooping mrouter interface <i>interface</i>	マルチキャストルータへのスタティック接続を設定します。ルータと接続するインターフェイスが、選択した VLAN に含まれている必要があります。インターフェイスは、タイプと番号で指定できます。
Step 11	switch(config-vlan)# ip igmp snooping static-group <i>group-ip-addr [source source-ip-addr] interface interface</i>	VLAN に属するインターフェイスを、マルチキャスト グループのスタティック メンバとして設定します。インターフェイスは、タイプと番号で指定できます。

Example

次に、VLAN の IGMP スヌーピング パラメータを設定する例を示します：

```
switch# configure terminal
switch(config)# vlan configuration 5
switch(config-vlan)# ip igmp snooping last-member-query-interval 3
switch(config-vlan)# ip igmp snooping querier 172.20.52.106
switch(config-vlan)# ip igmp snooping explicit-tracking
switch(config-vlan)# ip igmp snooping fast-leave
switch(config-vlan)# ip igmp snooping report-suppression
```

```
switch(config-vlan)# ip igmp snooping mrouter interface ethernet 1/10
switch(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface ethernet 1/10
switch(config-vlan)# end
```

IGMP スヌーピング設定の確認

IGMP スヌーピングの構成を確認するには、次のコマンドを使用します。

コマンド	説明
show ip igmp snooping [[vlan] <i>vlan-id</i>]	IGMP スヌーピング設定を VLAN 別に表示します。
show ip igmp snooping groups [[vlan] <i>vlan-id</i>] [detail]	グループに関する IGMP スヌーピング情報を VLAN 別に表示します。
show ip igmp snooping querier [[vlan] <i>vlan-id</i>]	IGMP スヌーピングクエリアを VLAN 別に表示します。
show ip igmp snooping mrouter [[vlan] <i>vlan-id</i>]	マルチキャスト ルータ ポートを VLAN 別に表示します。
show ip igmp snooping explicit-tracking vlan <i>vlan-id</i>	IGMP スヌーピングの明示的な追跡情報を VLAN 別に表示します。



Note [v2 EHT の VPC の動作（VPC behavior for v2 EHT）]: VPC シナリオでは、明示的なホストトラッキングは VPC ピアに同期されません。ただし、VPC ピアでは、EHT も cfs sync によって学習され、詳細オプションを使用して表示されます。

次に、IGMP スヌーピング パラメータを確認する例を示します。

```
switch# show ip igmp snooping
Global IGMP Snooping Information:
  IGMP Snooping enabled
IGMP Snooping information for vlan 1
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  Explicit tracking enabled
  Fast leave disabled
  Report suppression enabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
IGMP Snooping information for vlan 5
IGMP snooping enabled
  IGMP querier present, address: 192.0.2.1, version: 3
  Querier interval: 125 secs
  Querier last member query interval: 10 secs
  Querier robustness: 2
  Switch-querier enabled, address 192.0.2.1, currently running
```

```

Explicit tracking enabled
Fast leave enabled
Report suppression enabled
Router port detection using PIM Hellos, IGMP Queries
Number of router-ports: 1
Number of groups: 1

```

次の例は、IGMPv2 ホストでの明示的トラッキングの IGMP スヌーピング構成を表示する方法を示しています。

```

switch# show ip igmp snooping explicit tracking
IGMP Snooping Explicit-tracking information
Vlan Source/Group
  Intf      Reporter      Uptime      Last-Join Expires   Ver  Reports
100  */225.1.1.69
     Eth1/43  10.1.1.2      00:00:02    00:00:02    00:04:17  v2   1
100  */225.1.1.70
     Eth1/43  10.1.1.2      00:00:02    00:00:02    00:04:17  v2   1
100  */225.1.1.71
     Eth1/43  10.1.1.2      00:00:02    00:00:02    00:04:17  v2   1
100  */225.1.1.72
     Eth1/43  10.1.1.2      00:00:02    00:00:02    00:04:17  v2   1
100  */225.1.1.73
     Eth1/43  10.1.1.2      00:00:02    00:00:02    00:04:17  v2   1
100  */225.1.1.74
     Eth1/43  10.1.1.2      00:00:02    00:00:02    00:04:17  v2   1
100  */225.1.1.75
     Eth1/43  10.1.1.2      00:00:02    00:00:02    00:04:17  v2   1
100  */225.1.1.76
     Eth1/43  10.1.1.2      00:00:02    00:00:02    00:04:17  v2   1
100  */225.1.1.77
     Eth1/43  10.1.1.2      00:00:02    00:00:02    00:04:17  v2   1
100  */225.1.1.78
     Eth1/43  10.1.1.2      00:00:02    00:00:02    00:04:17  v2   1
switch#

```




第 13 章

トラフィック ストーム制御の設定

- [トラフィック ストーム制御の概要, on page 175](#)
- [トラフィック ストーム制御のガイドラインと制約事項 \(177 ページ\)](#)
- [トラフィック ストーム制御の設定, on page 178](#)
- [トラフィック ストーム制御の設定例, on page 179](#)
- [トラフィック ストーム制御のデフォルト設定, on page 180](#)

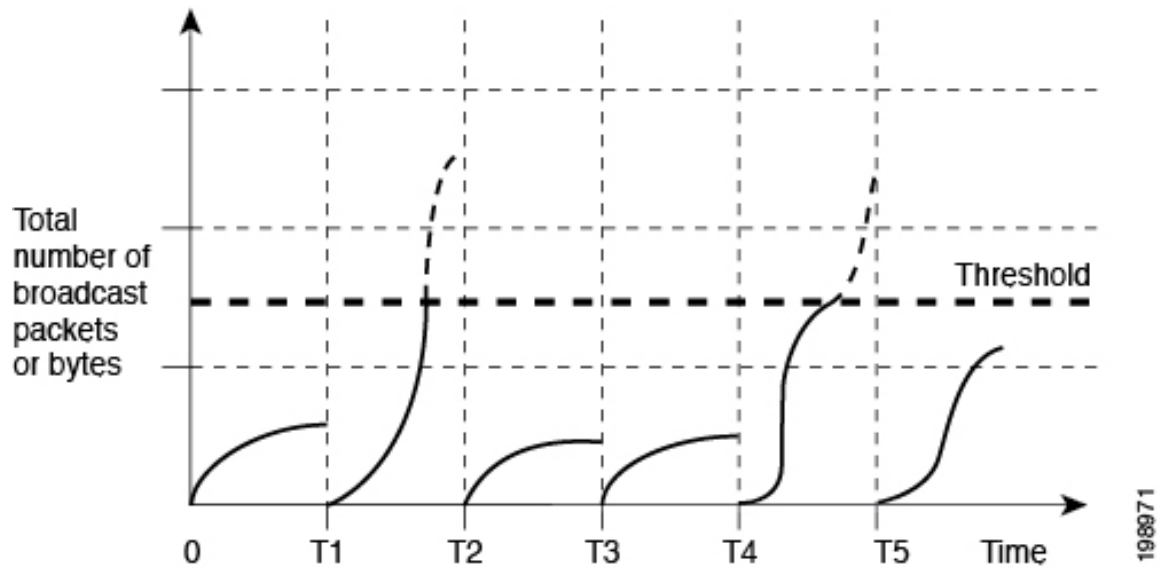
トラフィック ストーム制御の概要

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上における[ブロードキャストまたはマルチキャスト (broadcast or multicast)]トラフィック ストームによって、イーサネットインターフェイス経由の通信が妨害されるのを防ぐことができます。

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、[ブロードキャストまたはマルチキャスト (broadcast or multicast)]の着信トラフィックのレベルを 10 ミリ秒間隔で監視します。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。

次の図に、指定したタイム インターバル期間中におけるイーサネット 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 19: ブロードキャストの抑制



トラフィック ストーム制御のしきい値とタイム インターバルを使用することで、トラフィック ストーム制御アルゴリズムは、さまざまなレベルの packets 粒度で機能します。たとえば、しきい値が高いほど、より多くの packets を通過させることができます。

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 ストーム制御回路は、イーサネット インターフェイスから来て通過する packets を監視します。また、packets 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、packets がブロードキャストかを判断し、10 マイクロ秒以内の間隔で packets 数を追跡します。packets 数がしきい値に到達したら、後続の packets をすべて破棄します。

Cisco Nexus N3548 シリーズ スイッチは、トラフィック ストーム制御でアグリゲーション モードをサポートします。Cisco NX-OS では、トラフィック タイプはデフォルトでライン レートで設定されます。ブロードキャストおよびマルチキャスト ストーム制御が有効になっている場合、トラフィック は各レベルに設定されたレートに従ってフィルタ処理されます。ただし、集約モードでは、ユニキャスト、マルチキャスト、ブロードキャストを含むすべてのトラフィック タイプが、ポート レベルで設定されたレートに従ってフィルタ処理されます。

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。packets は一定の間隔で到着するわけではないので、10 マイクロ秒の間隔によって、トラフィック ストーム制御の動作が影響を受けることがあります。

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 10 マイクロ秒のインターバル以内にしきい値レベルを超えると、トラフィック ストーム制御により、そのインターバルが終了するまですべての超過ブロードキャスト トラフィック がドロップされます。

- マルチキャスト トラフィック ストーム制御をイネーブルにした場合、マルチキャスト トラフィックが 10 マイクロ秒のインターバル以内にしきい値レベルを超えると、トラフィック ストーム制御により、そのインターバルが終了するまですべての超過マルチキャスト トラフィックがドロップされます。
- ブロードキャストおよびマルチキャスト 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 10 マイクロ秒のインターバル以内にしきい値レベルを超えると、トラフィック ストーム制御により、そのインターバルが終了するまですべての超過ブロードキャスト トラフィックがドロップされます。
- ブロードキャストおよびマルチキャスト トラフィック ストーム制御をイネーブルにした場合、マルチキャスト トラフィックが 10 マイクロ秒のインターバル以内にしきい値レベルを超えると、トラフィック ストーム制御により、そのインターバルが終了するまですべての超過マルチキャスト トラフィックがドロップされます。

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 ストーム制御レベルを設定する場合は、次の注意事項と制限事項に留意してください。

- 出力マルチキャスト ストーム制御はサポートされていません。
- ポート チャネル インターフェイス上にトラフィック ストーム制御を設定できます。
- 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。
 - レベルの指定範囲は 0 ～ 100 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。
- ストーム制御ドロップが個別にカウントされることを防ぐ、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 `indiscards` 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、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。
- 現在、ユニキャストおよびブロードキャスト ストーム制御は、Cisco Nexus N3548 シリーズスイッチと Cisco Nexus N3548-X シリーズスイッチの両方で使用できます。

- ポート レベルのストーム制御を有効にすると、ユニキャスト、ブロードキャスト、およびマルチキャスト トラフィックをフィルタ処理する集約モードが強制されます。
- ポート レベルのストーム制御を有効にすると、マルチキャスト、ブロードキャスト、ユニキャストなどのすべてのタイプのトラフィックがフィルタ処理されます。既知と未知の両方のユニキャスト トラフィックは、UC トラフィックとともに MC/BC トラフィックがあり、MC/BC トラフィックのレートが設定されたポートストーム制御レベルを超えた場合にのみ、全体のトラフィック レートがストーム制御レベルを下回るまでフィルタリングされます。つまり、ポートレベルのストーム制御は、リンクにユニキャストトラフィックしかない場合、またはリンクの MC/BC トラフィックが設定されたストーム制御レベル内にある場合、ユニキャスト トラフィックをフィルタ処理しません。
- ポート レベルでストーム制御値を設定すると、マルチキャストおよびブロードキャストのレート制限値が上書きされ、すべてのトラフィックが単一のトラフィックしきい値に制限されます。
 - ポート レベルのストーム制御は、マルチキャスト レート制限値を使用します。
 - 10 未満のトラフィックしきい値の端数は 0 に丸められ、その情報は警告メッセージとして表示されます。丸め値は、10G ポートの場合は 0.9、1G ポートの場合は 89、40G ポートの場合は 3 のポート速度に基づいています。
- マルチキャストが有効で、ポートレベルのストーム制御を無効にしても、マルチキャスト値はポート レベルで構成された値で引き続き機能します。
- マルチキャストが無効になっていて、ポートレベルのストーム制御を無効にすると、マルチキャストの値とレジストリがリセットされます。

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 ストーム制御では 10 マイクロ秒のインターバルを使用しており、このインターバルがトラフィック ストーム制御の動作に影響を及ぼす可能性があります。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** {ethernet slot/port | port-channel number}
3. switch(config-if)# [no] **storm-control** [broadcast | multicast] level percentage[fraction]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	グローバル構成モードを開始します。
Step 2	switch(config)# interface { <i>ethernet slot/port</i> port-channel <i>number</i> }	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。
Step 3	switch(config-if)# [no] storm-control [broadcast multicast] level <i>percentage</i> [<i>fraction</i>]	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。デフォルトのステートはディセーブルです。

Example

次に、ポート チャネル 122 および 123 のトラフィック ストーム制御を設定する例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 122, port-channel 123
switch(config-if-range)# storm-control multicast level 66.75
switch(config-if-range)# storm-control broadcast level 66.75
switch(config-if-range)#
```

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、次のコマンドを使用します。。

コマンド	目的
show interface [<i>ethernet slot/port</i> port-channel <i>number</i>] counters storm-control	特定のインターフェイスについて、トラフィック ストーム制御の設定を表示します。
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。

トラフィック ストーム制御の設定例

次に、トラフィック ストーム制御を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# storm-control broadcast level 40
switch(config-if)# storm-control multicast level 40
```

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 11: 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

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。