Cisco Nexus 3000 シリーズ NX-OS レイヤ 2 スイッチング コンフィギュレーション ガイド リリース 5.0(3)U4(1)

初版：2012 年 08 月 26 日

最終更新：2012 年 08 月 26 日

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

Text Part Number: OL-26590-02-J

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

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

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

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

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。 シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2012 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xi

対象読者 xi

表記法 xi

Nexus 3000 シリーズ NX-OS ソフトウェアの関連資料 xiii

マニュアルに関するフィードバック xiv

マニュアルの入手方法およびテクニカル サポート xiv

このリリースの新規および変更情報 1

このリリースの新規および変更情報 1

概要 3

レイヤ 2 イーサネット スイッチングの概要 3

VLAN 3

プライベート VLAN 4

スパニングツリー 4

STP の概要 5

Rapid PVST+ 5

MST 5

STP 拡張機能 6

VLAN の設定 7

VLAN について 7

VLAN の概要 7

VLAN の範囲 8

VLAN の作成、削除、変更 9

VLAN トランキング プロトコルについて 10

VTP に関する注意事項および制約事項 11

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 14
管理 SVI としての VLAN の設定 15
VTP の設定 16
VLAN 設定の確認 18
VLAN の機能履歴 19
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 22
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 23
プライマリ VLAN とセカンダリ VLAN のアソシエーション 25
プライベート VLAN 内のブロードキャスト トラフィック 25
プライベート VLAN ポートの分離 26
プライベート VLAN に関する注意事項および制約事項 26
プライベート VLAN の設定 26
プライベート VLAN をイネーブルにするには 26
プライベート VLAN としての VLAN の設定 27
セカンダリ VLAN のプライマリ プライベート VLAN とのアソシエーション 28
インターフェイスをプライベート VLAN ホスト ポートとして設定するには 29
インターフェイスをプライベート VLAN 無差別ポートとして設定するには 31
プライベート VLAN 設定の確認 32
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 33
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 33
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 33
IEEE 802.1Q カプセル化の概要 35
アクセス VLAN の概要 35
トランク ポートのネイティブ VLAN ID の概要 36
許可 VLAN の概要 36
ネイティブ 802.1Q VLAN の概要 37
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 37

イーサネット アクセス ポートとしての LAN インターフェイスの設定 37
アクセス ホスト ポートの設定 38
トランク ポートの設定 39
802.1Q トランク ポートのネイティブ VLAN の設定 40
トランキング ポートの許可 VLAN の設定 40
ネイティブ 802.1Q VLAN の設定 41
インターフェイスの設定の確認 42
スイッチング モードの設定 45
スイッチング モードに関する情報 45
スイッチング モードに関する注意事項と制限事項 46
スイッチング モードのライセンス要件 47
スイッチング モードのデフォルト設定 47
スイッチング モードの設定 47
Store-and-Forward スイッチングのイネーブル化 47
カットスルー スイッチングの再イネーブル化 48
スイッチング モードの機能の履歴 48
Rapid PVST+ の設定 49
Rapid PVST+ について 49
STP の概要 50
STP の概要 50
トポロジ形成の概要 50
ブリッジ ID の概要 51
ブリッジ プライオリティ値 51
拡張システム ID 51
STP MAC アドレス割り当て 52
BPDU の概要 53
ルート ブリッジの選定 54
スパニングツリー トポロジの作成 54
Rapid PVST+ の概要 55
Rapid PVST+ の概要 55
Rapid PVST+ BPDU 57
提案と合意のハンドシェイク 58

プロトコル タイマー 59
ポート ロール 59
ポート ステート 61
Rapid PVST+ ポート ステートの概要 61
ブロッキング ステート 61
ラーニング ステート 62
フォワーディング ステート 62
ディセーブル ステート 62
ポート ステートの概要 63
ポート ロールの同期 63
優位 BPDU 情報の処理 64
下位 BPDU 情報の処理 65
スパニングツリー異議メカニズム 65
ポート コスト 65
ポート プライオリティ 66
Rapid PVST+ と IEEE 802.1Q トランク 66
Rapid PVST+ のレガシー 802.1D STP との相互運用 67
Rapid PVST+ の 802.1s MST との相互運用 68
Rapid PVST+ の設定 68
Rapid PVST+ のイネーブル化 68
Rapid PVST+ の VLAN ベースのイネーブル化 69
ルート ブリッジ ID の設定 70
セカンダリ ルート ブリッジの設定 71
Rapid PVST+ のポート プライオリティの設定 72
Rapid PVST+ のパス コスト方式とポート コストの設定 73
VLAN の Rapid PVST+ のブリッジ プライオリティの設定 74
VLAN の Rapid PVST+ の hello タイムの設定 74
VLAN の Rapid PVST+ の転送遅延時間の設定 75
VLAN の Rapid PVST+ の最大経過時間の設定 75
リンク タイプの設定 76
プロトコルの再開 77
Rapid PVST+ の設定の確認 77

Multiple Spanning Tree の設定 79

MST について 79

MST の概要 79

MST 領域 80

MST BPDU 80

MST 設定情報 81

IST、CIST、CST 82

IST、CIST、CST の概要 82

MST 領域内でのスパニングツリーの動作 82

MST 領域間のスパニングツリー動作 83

MST 用語 84

ホップ カウント 85

境界ポート 85

スパニングツリー異議メカニズム 86

ポート コストとポート プライオリティ 87

IEEE 802.1D との相互運用性 87

Rapid PVST+ の相互運用性と PVST シミュレーションについて 88

MST の設定 88

MST 設定時の注意事項 88

MST のイネーブル化 89

MST コンフィギュレーション モードの開始 90

MST の名前の指定 91

MST 設定のリビジョン番号の指定 91

MST 領域での設定の指定 92

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 94

プライベート VLAN でセカンダリ VLAN をプライマリ VLAN として同じ MSTI にマッピングするには 95

ルート ブリッジの設定 96

セカンダリ ルート ブリッジの設定 97

ポートのプライオリティの設定 98

ポート コストの設定 99

スイッチのプライオリティの設定 100

hello タイムの設定 101
転送遅延時間の設定 101
最大経過時間の設定 102
最大ホップ カウントの設定 102
PVST シミュレーションのグローバル設定 103
ポートごとの PVST シミュレーションの設定 104
リンク タイプの設定 105
プロトコルの再開 105
MST の設定の確認 106
STP 拡張機能の設定 107
STP 拡張機能について 107
STP 拡張機能について 107
STP ポート タイプの概要 107
スパニングツリー エッジ ポート 108
スパニングツリー ネットワーク ポート 108
スパニングツリー標準ポート 108
Bridge Assurance の概要 108
BPDU ガードの概要 109
BPDU フィルタリングの概要 109
ループ ガードの概要 111
ルート ガードの概要 112
STP 拡張機能の設定 112
STP 拡張機能の設定における注意事項 112
スパニングツリー ポート タイプのグローバルな設定 113
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 114
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 115
BPDU ガードのグローバルなイネーブル化 116
指定インターフェイスでの BPDU ガードのイネーブル化 117
BPDU フィルタリングのグローバルなイネーブル化 118
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 119
ループ ガードのグローバルなイネーブル化 120

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 121
STP 拡張機能の設定の確認 122
LLDP の設定 123
グローバル LLDP コマンドの設定 123
インターフェイス LLDP コマンドの設定 125
LLDP の MIB 127
MAC アドレス テーブルの設定 129
MAC アドレスの概要 129
MAC アドレスの設定 130
スタティック MAC アドレスの設定 130
MAC テーブルのエージング タイムの設定 130
MAC テーブルからのダイナミック アドレスのクリア 131
MAC アドレスの設定の確認 132
IGMP スヌーピングの設定 133
IGMP スヌーピングの情報 133
IGMPv1 および IGMPv2 134
IGMPv3 135
IGMP スヌーピング クエリア 135
IGMP 転送 135
IGMP スヌーピング パラメータの設定 136
IGMP スヌーピングの設定確認 140
トラフィック ストーム制御の設定 143
トラフィック ストーム制御の概要 143
トラフィック ストームに関する注意事項および制約事項 145
トラフィック ストーム制御の設定 145
トラフィック ストーム制御の設定の確認 146
トラフィック ストーム制御の設定例 147
デフォルトのトラフィック ストームの設定 147

はじめに

ここでは、次の項目について説明します。

- 対象読者，xi ページ
- 表記法，xi ページ
- Nexus 3000 シリーズ NX-OS ソフトウェアの関連資料，xiii ページ
- マニュアルに関するフィードバック ，xiv ページ
- マニュアルの入手方法およびテクニカル サポート，xiv ページ

対象読者

この出版物は Cisco Nexus シリーズ デバイスの設定と保守を行う経験豊富なネットワーク管理者を対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	角カッコで囲まれているものは、省略可能な要素（キーワードまたは引数）です。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。

表記法	説明
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。 角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。 string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。

（注） 「注釈」です。 役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

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

Nexus 3000 シリーズ NX-OS ソフトウェアの関連資料

完全な Cisco NX-OS 3000 シリーズ マニュアル セットは、次の URL で入手できます。

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 で入手できます。

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

インストレーション ガイドおよびアップグレード ガイド

インストールおよびアップグレード ガイドは次の URL で入手できます。

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は次のとおりです。

- *Cisco Nexus 5000* シリーズ、*Cisco Nexus 3000* シリーズ、および *Cisco Nexus 2000* シリーズの安全に関する情報およびドキュメント
- 『*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 の機能のライセンスに関する詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。次の URL で入手可能です。http://www.cisco.com/en/US/docs/switches/datacenter/sw/nx-os/licensing/guide/b_Cisco_NX-OS_Licensing_Guide.html

NX-OS のエンド ユーザ契約書および著作権情報については、『*License and Copyright Information for Cisco NX-OS Software*』を参照してください。次の URL で入手可能です。http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-ossw_lisns.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 で入手できます。

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は次のとおりです。

- 『*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*』

テクニカル リファレンス

テクニカル リファレンスは、次の URL で入手できます。

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

エラー メッセージおよびシステム メッセージ

エラー メッセージとシステム メッセージのリファレンス 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、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

マニュアルの入手方法およびテクニカル サポート

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

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

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

第 1 章

このリリースの新規および変更情報

次の表に、最新リリースに関するこのガイドでの重要な変更点の概要を示します。 この表は、実行コンフィギュレーション ガイドへのすべての変更や、またはこのリリースの新機能の詳細なリストを提供しません。

- このリリースの新規および変更情報, 1 ページ

このリリースの新規および変更情報

この章は、次の内容で構成されています。

表 *1*：新機能および変更された機能

機能	説明	リリースで追加または変更された機能	参照先
CISCO-VTP-MIB	VTP プロトコルおよび VLAN 管理を実装するエンティティの MIB モジュール。	5.0(3)U4(1)	VTP に関する注意事項および制約事項, （11 ページ）
『Layer 2 Switching Configuration Guide』から「Configuring Ethernet Interfaces」の章を削除	この章は、「Configuring Layer 2 Interfaces」という名前に変更され、『Interfaces Configuration Guide』に追加されました。	5.0(3)U4(1)	『*Cisco Nexus 3000 NX-OS Interfaces Configuration Guide, Release 5.0(3)U4(1)*』
LLDP MIB のサポート	LLDP MIB のサポートが追加されました。	5.0(3)U4(1)	LLDP の設定, （123 ページ）

このリリースの新規および変更情報

第 2 章

概要

この章は、次の内容で構成されています。

- レイヤ 2 イーサネット スイッチングの概要，3 ページ
- VLAN，3 ページ
- プライベート VLAN，4 ページ
- スパニングツリー，4 ページ

レイヤ 2 イーサネット スイッチングの概要

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

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

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

VLAN

VLAN は、ユーザの物理的な位置に関係なく、機能、プロジェクト チーム、またはアプリケーションなどで論理的に分割されたスイッチド ネットワークです。 VLAN は、物理 LAN と同じ属

性をすべて備えていますが、同じLANセグメントに物理的に配置されていないエンドステーションもグループ化できます。

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

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

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

（注） スイッチ間リンク（ISL）トランキングは、Cisco Nexus 3000 シリーズの NX-OS ソフトウェアではサポートされていません。

プライベート VLAN

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

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

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

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（Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット））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 Multiple Spanning Tree（MST）では、複数の VLAN を単一のスパニングツリー インスタンスにマッピングできます。 各インスタンスは、独立したスパニングツリー トポロジで実行されます。

ソフトウェアは、従来の 802.1D システムで相互運用できますが、システムでは Rapid PVST+ および MST が実行されます。 特定の 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、Cisco Nexus 3000 シリーズ用 Cisco NX-OS のデフォルトの STP プロトコルです。

（注） Cisco Nexus 3000 シリーズ用 Cisco NX-OS では、拡張システム ID と MAC アドレス リダクションを使用します。これらの機能をディセーブルにできません。

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

Rapid PVST+

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

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

MST

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

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

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

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、非指定ポートが STP フォワーディング ステートに移行するのを阻止し、ネットワーク上でのループの発生を防止します。
- ルート ガード：ルート ガードは、ポートが STP トポロジのルートにならないように防御します。

第 3 章

VLAN の設定

この章は、次の内容で構成されています。

- VLAN について，7 ページ
- VLAN の設定，11 ページ

VLAN について

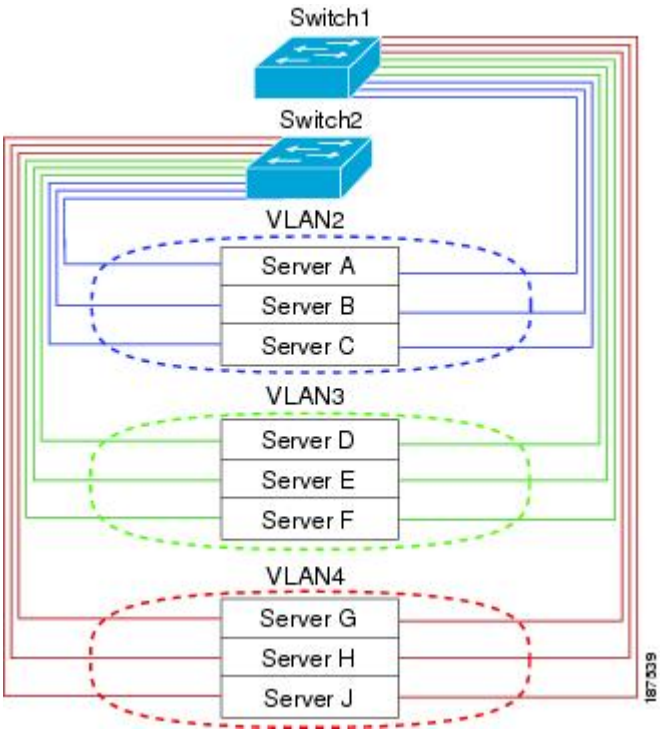
VLAN の概要

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を示します。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。

図 *1*：論理的に定義されたネットワークとしての *VLAN*



VLAN は、通常 IP サブネットワークと関連付けます。 たとえば、特定の IP サブネットに含まれるすべてのエンド ステーションを同じ VLAN に属させる場合などです。 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

（注） 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。

設定の制限については、スイッチの設定の制限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。

表 *2*：*VLAN* の範囲

VLAN 番号	範囲	用途
1	標準	シスコ システムズのデフォルトです。 この VLAN は使用できますが、変更や削除はできません。
2 ～ 1005	標準	これらの VLAN は、作成、使用、変更、削除できます。
1006 ～ 3967 および 4048 ～ 4093	拡張	これらの VLAN は、作成、命名、使用できます。 次のパラメータは変更できません。 • ステートは必ず、アクティブです。 • VLAN は常にイネーブルです。 これらの VLAN はシャットダウンできません。
3968 ～ 4047 および 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。 内部使用に予約されたブロック内の VLAN の作成、削除、変更はできません。

ソフトウェアは、内部 VLAN の使用を必要とするマルチキャストや診断などの機能のために、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）はデフォルト値だけを使用します。 デフォルト VLAN のアクティビティは作成、削除、または一時停止できません。

それに番号を割り当てることによって、VLAN を作成します。 VLAN の削除、およびそれらのアクティブ動作ステートから一時停止動作ステートへの移行ができます。 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。 しかしシステムはその VLAN の VLAN/ポート マッピングをすべて維持するため、この指定VLANの再イネーブル化や再作成を行うと、そのVLANの元のすべてのポートはシステムによって自動的に回復されます。

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

VLAN 3968 ～ 4047 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 トランキング プロトコルについて

VTP はドメイン全体で VTP VLAN データベースを同期する分散 VLAN データベース管理プロトコルです。 VTP ドメインは、同じ VTP ドメイン名を共有し、トランク インターフェイスを使用して接続される、1 つ以上のネットワーク スイッチで構成されます。 各スイッチは、1 つの VTP ドメイン、レイヤ 2 トランク インターフェイス、レイヤ 2 ポート チャネルに所属できます。

VTP モードには次の 4 つがあります。

- サーバモード：ユーザは設定を実行できます。これは、VLANデータベースのバージョン番号を管理し、VLAN データベースを保存します。
- クライアントモード：ユーザ設定を許可せず、ドメイン内の他のスイッチに依存して設定情報を提供します。
- オフモード：VLANデータベース（VTPがイネーブル）へのアクセスをユーザに許可しますが、VTP に参加しません。
- トランスペアレント モード：VTP に参加せず、ローカル設定を使用し、他の転送ポートに VTP パケットをリレーします。 VLAN を変更した場合は、ローカル スイッチだけに影響します。 VTP トランスペアレント ネットワーク スイッチは、その VLAN 設定をアドバタイズせず、受信したアドバタイズメントに基づいてその VLAN 設定を同期することもありません。

VTP に関する注意事項および制約事項

VTP 設定時の注意事項と制限事項は次のとおりです。

- スイッチが VTP クライアントとして設定されている場合、1 ～ 1005 の範囲のスイッチ上で VLAN を作成できません。
- 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で VLAN 1 をディセーブルにすると、VTP が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。
- show running-configuration コマンドでは、VLAN 1 ～ 1000 の VLAN または VTP の設定情報が表示されません。
- VTP プルーニングはサポートされません。
- PVLAN は、スイッチがトランスペアレント モードにある場合のみサポートされます。
- 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。
- スイッチが VTP クライアントまたはサーバ モードで設定されている場合、VLAN 1002 ～ 1005 は予約済み VLAN です。
- **copy running-config startup-config** を実行した後で、予約済み VLAN 範囲の変更後のリロードを行う必要があります。 次に例を示します。

```
switch(config)# system vlan 2000 reserve
This will delete all configs on vlans 2000-2127. Continue anyway? (y/n) [no] y
```

スイッチのリロード後、VLAN 2000 ～ 2127 は内部使用のために予約されています。 この場合、スイッチのリロード前に **copy running-config startup-config** コマンドを実行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。

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。

（注） 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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **vlan** {*vlan-id* | *vlan-range*}	VLAN または VLAN の範囲を作成します。 VLANにすでに割り当てられている番号を入力すると、そのVLANのVLANコンフィギュレーションサブモードがスイッチによって開始されます。 内部的に割り当てられているVLANに割り当てられている番号を入力すると、エラーメッセージが返されます。 VLAN の範囲を入力し、指定 VLAN の 1 つ以上が、内部的に割り当てられた VLAN の範囲外である場合、コマンドは範囲外の VLAN だけで有効になります。 指定できる範囲は 2 ～ 4094 です。VLAN1 はデフォルト VLAN であり、作成や削除はできません。 内部使用のために予約されている VLAN の作成や削除はできません。
ステップ 3	switch(config-vlan)# **no vlan** {*vlan-id* | *vlan-range*}	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。 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。

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
```

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

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
- シャットダウン

（注） デフォルト VLAN または内部的に割り当てられた VLAN の作成、削除、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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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。
ステップ 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。
ステップ 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。
ステップ 5	switch(config-vlan)# **no shutdown**	（任意） VLAN をイネーブルにします。 デフォルト値は **no shutdown**（イネーブル）です。 デフォルト VLAN の VLAN1、または VLAN 1006 ～ 4094 はシャットダウンできません。

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。 ポートを追加する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {**ethernet** *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。 インターフェイスには、物理イーサネット ポートまたは EtherChannel を指定できます。
ステップ 3	switch(config-if)# **switchport access vlan** *vlan-id*	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。

次の例は、VLAN 5 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。

はじめる前に

- レイヤ 3 ライセンスをインストールします。 詳細については、『*License and Copyright Information for Cisco NX-OS Software*』次の URL で入手可能です。http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-ossw_lisns.html
- 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。 詳細については、SVI に関する注意事項および制約事項を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**feature interface-vlan**	SVI の作成をイネーブルにします。
ステップ 3	**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。
ステップ 4	**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。

次に、ルーテッド SVI に VLAN を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)#
```

次の作業

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

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**feature interface-vlan**	SVI の作成をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**interface-vlan** *vlan-id* **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。
ステップ 4	**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。

次に、管理 VLAN として SVI を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 をイネーブルにした後で、VTP モードを設定できます。Cisco Nexus 3000 シリーズは VTP トランスペアレント モードだけをサポートします。 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。 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

	コマンドまたはアクション	目的

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

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

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

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

ステップ 9	**show vtp status** 例： `switch# show vtp status`	（任意） バージョン、モードおよびリビジョン番号などのデバイスの VTP 設定に関する情報を表示します。
ステップ 10	**show vtp counters** 例： `switch# show vtp counters`	（任意） デバイスの VTP アドバタイズメントの統計に関する情報を表示します。
ステップ 11	**show vtp interface** 例： `switch# show vtp interface`	（任意） VTP がイネーブルであるインターフェイスのリストを表示します。
ステップ 12	**show vtp password** 例： `switch# show vtp password`	（任意） 管理 VTP ドメインのパスワードを表示します。

	コマンドまたはアクション	目的
ステップ 13	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

次の例は、スイッチでバージョン2がサポートでき、スイッチがバージョン1を実行しているVTPステータスを表示する例を示します。

```
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 設定の確認

設定を確認するには、次のいずれかのコマンドを使用します。

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

この章は、次の内容で構成されています。

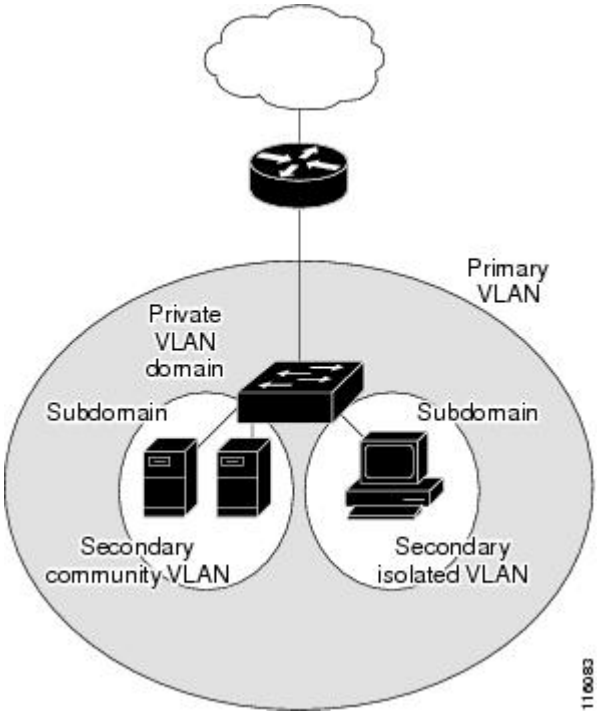
- プライベート VLAN について，21 ページ
- プライベート VLAN に関する注意事項および制約事項，26 ページ
- プライベート VLAN の設定，26 ページ
- プライベート VLAN 設定の確認，32 ページ

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ので、スイッチで相互にポートを分離できます。 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 で構成されます（次の図を参照）。 PVLAN にあるすべての VLAN は、同じプライマリ VLAN を共有します。 セカンダリ VLAN ID は、各サブドメインの区別に使用されます。 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。

図 *2*：プライベート *VLAN* ドメイン



（注） まず VLAN を作成してから、プライマリまたはセカンダリの PVLAN に変換する必要があります。

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 ポートと独立ホスト ポートも含まれます。 プライマリ VLAN には、複数の無差別ポートを含めることができます。 各無差別ポートは、そのポートに関連付けられた複数のセカンダリ VLAN を持つことができます。または、セカンダリ VLAN を持たないこともできます。 無差別ポートとセカンダリ VLAN が同じプライマリ VLAN にある限り、セカンダリ VLAN は、複数の無差別ポートとアソシエートすることができます。 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 ポートとして設定できます。

- 独立ポート：独立セカンダリ VLAN に属するホスト ポート。 このポートは、関連付けられた無差別ポートと通信できることを除き、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。 VLANは、無差別ポートからのトラフィックを除き、独立ポート宛て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、無差別ポートだけに転送されます。 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 ポートとして設定できます。

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

  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

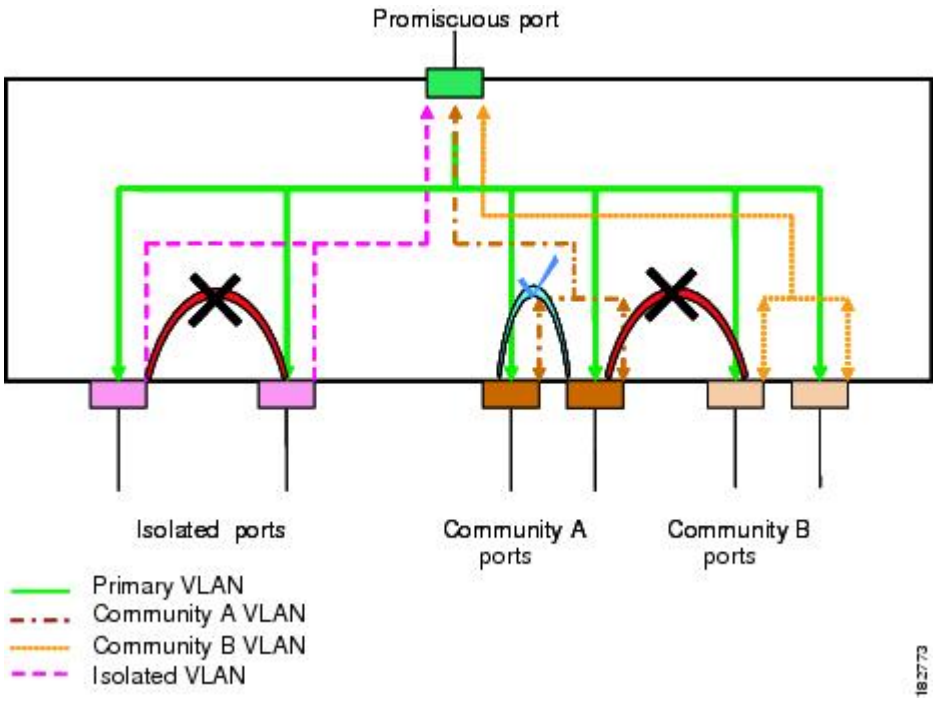
プライマリ VLAN および 2 つのタイプのセカンダリ VLAN（独立 VLAN とコミュニティ VLAN）には、次の特徴があります。

- 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。 PVLAN ドメインには、1 つの独立 VLAN だけ設定できます。 独立 VLANには、複数の独立ポートを設定できます。 各独立ポートからのトラフィックも完全に隔離されたままです。

- 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。 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。

次の図に、PVLAN 内のトラフィック フローと、VLAN のタイプ、ポートのタイプを示します。

図 *3*：プライベート *VLAN* のトラフィック フロー



（注） 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 で受信するトラフィックによって隔離は行われず、転送は通常 VLAN として実行されます。

無差別アクセスポートでは、1 つだけのプライマリ 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や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。 プライベート VLAN の外

部と通信するには、エンドステーションでは、デフォルト ゲートウェイのみと通信する必要があります。

プライマリ VLAN とセカンダリ VLAN のアソシエーション

セカンダリ PVLAN 内のホスト ポートで VLAN の外部と通信するには、セカンダリ VLAN をプライマリ VLAN に関連付けます。 アソシエーションの操作が可能ではない場合、セカンダリ VLAN のホスト ポート（コミュニティ ポートと独立ポート）は、ダウンされます。

（注） セカンダリ VLAN は、1 つのプライマリ VLAN のみにアソシエートすることができます。

アソシエーションの操作を可能にするには、次の条件を満たす必要があります。

- プライマリ VLAN を終了し、プライマリ VLAN として設定する必要があります。
- セカンダリ VLAN を終了し、独立 VLAN またはコミュニティ VLAN として設定する必要があります。

（注） 関連付けが動作していることを確認するには、**show vlan private-vlan** コマンドを使用します。関連付けが動作していないとき、スイッチはエラー メッセージを表示しません。

プライマリ VLAN またはセカンダリ VLAN を削除すると、その VLAN に関連付けされたポートは非アクティブになります。 VLAN を通常モードに戻すには、**no private-vlan** コマンドを使用します。 その VLAN におけるすべてのプライマリとセカンダリの関連付けは一時停止しますが、インターフェイスは PVLAN モードのままです。 VLAN を PVLAN モードに戻すときには、元の関連付けが戻されます。

プライマリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN に関連付けされたすべての PVLAN が削除されます。 ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力した場合、その VLAN と PVLAN の関連付けは一時停止します。この指定 VLAN を再作成して以前のセカンダリ VLAN として設定すると復元されます。

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

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。
- 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するには、デフォルトゲートウェイおよびエンドステーションに接続されているインターフェイスを、無差別ポートとして設定します。

プライベート VLAN に関する注意事項および制約事項

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。
- スイッチが PVLAN 機能を適用するには、PVLAN をイネーブルにする必要があります。
- PVLAN モードで動作しているポートがスイッチに含まれる場合、PVLAN をディセーブルにできません。
- プライマリ VLAN と同じ MST インスタンスにセカンダリ VLAN マッピングするには、Multiple Spanning Tree（MST）リージョン定義内から **private-vlan synchronize** コマンドを入力します。

プライベート VLAN の設定

プライベート VLAN をイネーブルにするには

PVLAN 機能を使用するには、スイッチの PVLAN をイネーブルにする必要があります。

（注） 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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **feature private-vlan**	スイッチの PVLAN 機能をイネーブルにします。
ステップ 3	switch(config)# **no feature private-vlan**	（任意） スイッチの PVLAN 機能をディセーブルにします。 （注） PVLAN モードにあるスイッチに動作しているポートがある場合、PVLAN をディセーブルにできません。

次に、スイッチの PVLAN 機能をイネーブルにする例を示します。

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

プライベート VLAN としての VLAN の設定

PVLAN を作成するには、まず VLAN を作成し、PVLAN になるようにその VLAN を設定します。

はじめる前に

PVLAN 機能がイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **vlan** {*vlan-id* | *vlan-range*}	VLAN 設定サブモードにします。
ステップ 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、1 つのプライマリ VLAN を設定する必要があります。 複数のコミュニティ VLAN と独立 VLAN を設定することができます。

	コマンドまたはアクション	目的
ステップ 4	switch(config-vlan)# **no private-vlan** {**community** | **isolated** | **primary**}	（任意） 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。

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

```
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ています。

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

次の例は、VLAN 200 を独立 VLAN として PVLAN に割り当てる方法を示しています。

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

セカンダリ VLAN のプライマリ プライベート VLAN とのアソシエーション

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、複数のコミュニティ VLAN ID と 1 つの独立 VLAN ID を指定できます。
- セカンダリ VLAN をプライマリ VLAN にアソシエートするには、*secondary-vlan-list* と入力するか、*secondary-vlan-list* に **add** キーワードを使用します。
- セカンダリ VLAN とプライマリ VLAN とのアソシエーションをクリアするには、*secondary-vlan-list* に **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。

プライマリまたはセカンダリ VLAN のいずれかを削除すると、VLAN はアソシエーションが設定されたポートで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 におけるすべてのプライマリとセカンダリの関連付けは一時停止しますが、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、元の関連付けが戻されます。

プライマリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN 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**コマンドを入力した場合、その VLAN との PVLAN の関連付けは一時停止します。この指定した VLAN を再作成して以前のセカンダリ VLAN として設定すると元に戻ります。

はじめる前に

PVLAN 機能がイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **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。
ステップ 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 とのアソシエーションをクリアするには、*secondary-vlan-list* に **remove** キーワードを使用します。
ステップ 4	switch(config-vlan)# **no private-vlan association**	（任意） プライマリ VLANからすべてのアソシエーションを削除し、通常のVLANモードに戻します。

次に、コミュニティ VLAN 100 ～ 110 および独立 VLAN 200 をプライマリ VLAN 5 に関連付ける例を示します。

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

インターフェイスをプライベート VLAN ホスト ポートとして設定するには

PVLAN では、ホスト ポートがセカンダリ VLAN の一部です。セカンダリ VLAN は、コミュニティ VLAN または独立 VLAN のいずれかです。 PVLAN ホスト ポートの設定には、2 つの手順が

必要です。 最初に、ポートを PVLAN ホスト ポートとして定義した後で、プライマリ VLAN とセカンダリ VLAN 間のホスト関連付けを設定します。

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

はじめる前に

PVLAN 機能がイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type* [*chassis*/]*slot*/*port*	PVLAN ホスト ポートとして設定するポートを選択します。 このポートは、FEX（chassis オプションで識別される）上に存在できます。
ステップ 3	switch(config-if)# **switchport mode private-vlan host**	PVLAN のホスト ポートとしてポートを設定します。
ステップ 4	switch(config-if)# **switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*}	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 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。
ステップ 5	switch(config-if)# **no switchport private-vlan host-association**	（任意） ポートから PVLAN の関連付けを削除します。

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ています。

```
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
```

インターフェイスをプライベート VLAN 無差別ポートとして設定するには

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。 無差別ポートの設定には、2 つの手順が必要です。 最初にポートを無差別ポートに定義した後で、セカンダリ VLAN とプライマリ VLAN 間のマッピングを設定します。

はじめる前に

PVLAN 機能がイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot*/*port*	PVLAN 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。 このポートは、FEX 上には設定できません。
ステップ 3	switch(config-if)# **switchport mode private-vlan promiscuous**	PVLAN の無差別ポートとしてポートを設定します。 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。
ステップ 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。
ステップ 5	switch(config-if)# **no switchport private-vlan mapping**	（任意） PVLAN のマッピングをクリアします。

次の例は、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 を設定し、プライマリ VLAN 5 およびセカンダリ独立 VLAN 200 にそのポートを関連付ける方法を示しています。

```
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 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になっている機能を表示します。
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。

次に、PVLAN コンフィギュレーションを表示する例を示します。

```
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
```

次に、イネーブルの機能を表示する例を示します（出力の一部を割愛してあります）。

```
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

この章は、次の内容で構成されています。

- アクセス インターフェイスとトランク インターフェイスについて，33 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，37 ページ
- インターフェイスの設定の確認，42 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

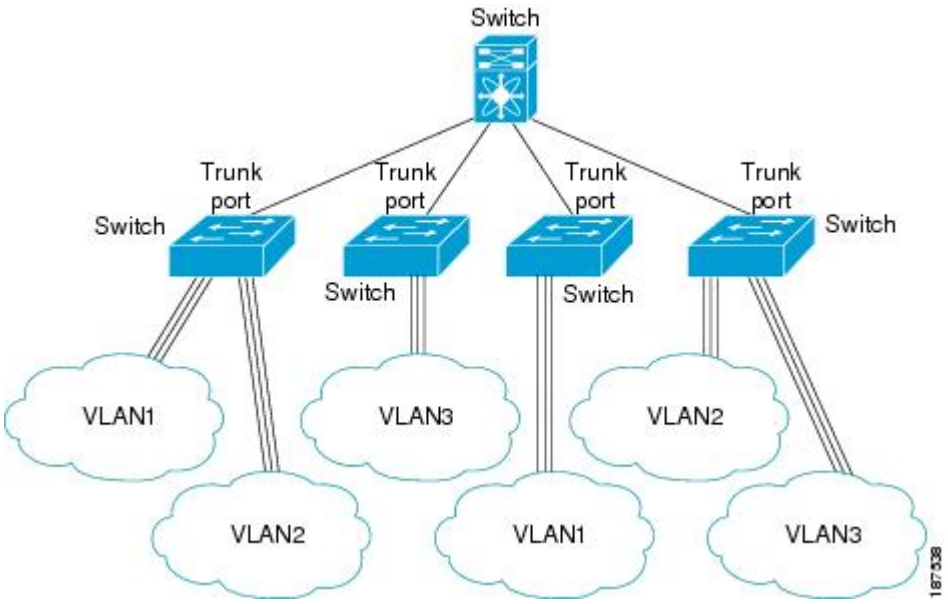
イーサネット インターフェイスは、次のように、アクセス ポートまたはトランク ポートとして設定できます。

- 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。

（注） 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、ネットワーク内でのトランク ポートの使用方法を示します。 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。

図 *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。

（注） 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。

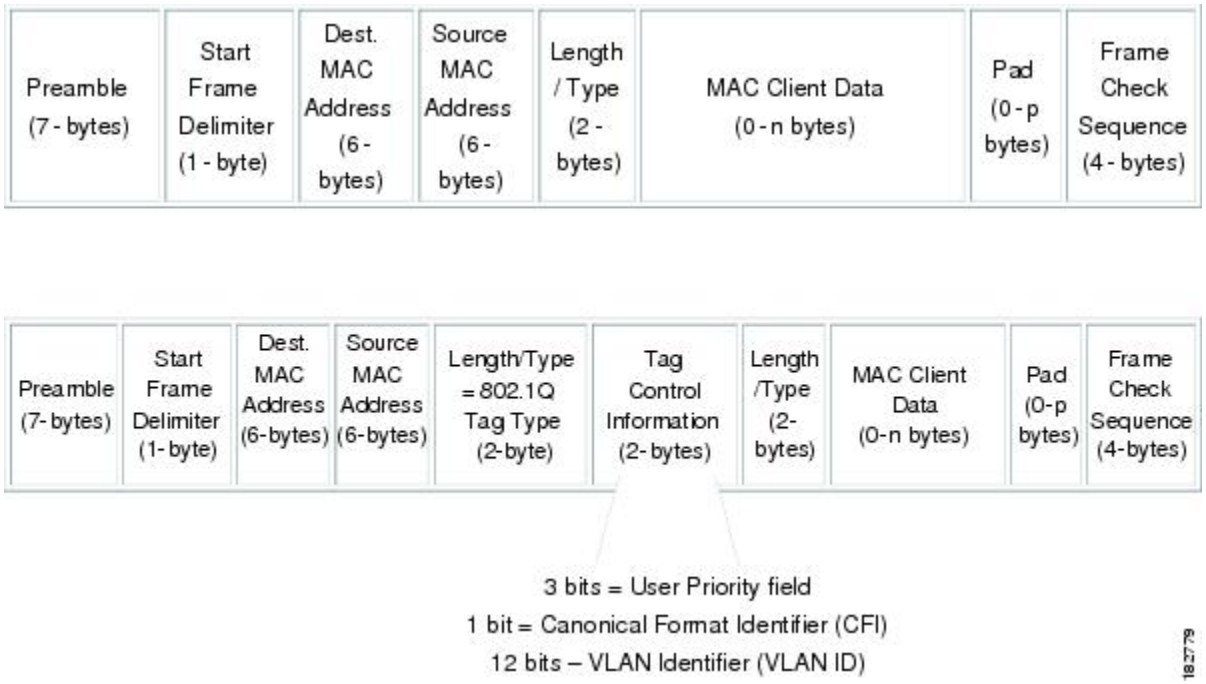
（注） イーサネット インターフェイスはアクセス ポートまたはトランク ポートとして動作できますが、両方のポート タイプとして同時に動作することはできません。

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。

図 *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**



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。

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。

（注） アクセス VLAN を割り当て、プライベート VLAN のプライマリ VLAN としても動作させると、そのアクセス VLAN に対応するすべてのアクセス ポートが、プライベート VLAN モードのプライマリ VLAN 向けのすべてのブロードキャスト トラフィックを受信するようになります。

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。

（注） 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 Spanning Tree Protocol（STP; スパニングツリー プロトコル）トポロジを分割するには、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 のコンバージェンス中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強化するために、**vlan dot1q tag native** コマンドが追加されました。 この機能は、802.1Q トランク ポートから出ていくすべてのパケットがタグ付けされていることを確認し、802.1Q トランク ポート上でタグなしパケットの受信を防止するための手段を提供します。

この機能がないと、802.1Q トランク ポートで受信されたすべてのタグ付き入力フレームは、許可 VLAN リスト内に入り、タグが維持されている限り受け入れられます。 タグなしフレームは、その後の処理の前にトランク ポートのネイティブ VLAN ID でタグ付けされます。 VLAN タグがその 802.1Q トランク ポートの許容範囲内である出力フレームだけが受信されます。 フレームの VLAN タグがトランク ポートのネイティブ VLAN のタグとたまたま一致すれば、そのタグが取り除かれ、フレームはタグなしで送信されます。

この動作は、ハッカーが別の VLAN へのフレーム ジャンプを試みて実行する「VLAN ホッピング」の取り込みに不正利用でき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 ポートに送信することによって、トラフィックがネイティブ VLAN の一部になる可能性もあります。

前述の問題を解決するために、**vlan dot1q tag native** コマンドは、次の機能を実行します。

- 入力側では、すべてのタグなしデータ トラフィックはドロップされます。
- 出力側では、すべてのトラフィックがタグ付けされます。トラフィックがネイティブ VLAN に属する場合、ネイティブ VLAN ID でタグ付けされます。

この機能は、Cisco Nexus 3000 シリーズ スイッチの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 EtherChannel インターフェイスでサポートされます。

（注） **vlan dot1q tag native** 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 モードでコマンドを発行します。

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

イーサネット アクセス ポートとしての LAN インターフェイスの設定

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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {{*type slot*/*port*} | {**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。
ステップ 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** コマンドを使用します。
ステップ 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。

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 ホストを使用して、アクセス ポートをスパニングツリー エッジ ポートにすること、および BPDU フィルタリングと BPDU ガードの両方を同時にイネーブルにすることができます。

はじめる前に

正しいインターフェイスを設定していることを確認します。これは、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である必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot*/*port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport host**	インターフェイスをスパニングツリー エッジ ポート タイプに設定し、BPDU フィルタリングおよび BPDU ガードをオンにします。 （注） ホストに接続しているスイッチポートにだけこのコマンドを適用します。

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

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

トランク ポートを設定する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {*type slot*/*port* | **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。
ステップ 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

	コマンドまたはアクション	目的
		VLAN はトラン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。

次に、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例を示します。

```
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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {*type slot*/*port* | **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。
ステップ 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。

次に、イーサネット トランク ポートのネイティブ VLAN を設定する例を示します。

```
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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {*type slot*/*port* | **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。
ステップ 3	switch(config-if)# **switchport trunk allowed vlan** {*vlan-list* **all** | **none** [**add** |except | none | **remove** {*vlan-list*}]}	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。 （注） 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と、メッセージが返されます。

次に、イーサネット トランク ポートで、許可 VLAN のリストに VLAN を追加する例を示します。

```
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に Cisco Nexus 3000 シリーズ スイッチの通過を許可します。 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、トランキング 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、グローバルでイネーブルになります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **vlan dot1q tag native**	Cisco Nexus 3000 シリーズ スイッチ上のすべてのトランキング 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、この機能はディセーブルになっています。
ステップ 3	switch(config)# **no vlan dot1q tag native**	（任意） スイッチ上のすべてのトランキング ポートのすべてのネイティブ VLAN の dot1q（IEEE 802.1Q）タギングをディセーブルにします。
ステップ 4	switch# **show vlan dot1q tag native**	（任意） ネイティブ VLAN のタギングのステータスを表示します。

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

アクセスインターフェイスとトランクインターフェイスの設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
switch# **show interface**	インターフェイス設定を表示します。

コマンド	目的
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

スイッチング モードの設定

この章は、次の内容で構成されています。

- スイッチング モードに関する情報，45 ページ
- スイッチング モードに関する注意事項と制限事項，46 ページ
- スイッチング モードのライセンス要件，47 ページ
- スイッチング モードのデフォルト設定，47 ページ
- スイッチング モードの設定，47 ページ
- スイッチング モードの機能の履歴，48 ページ

スイッチング モードに関する情報

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

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

スイッチは、次のスイッチング モードのいずれかで動作します。

カットスルー スイッチング モード

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

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

Store-and-Forward スイッチング モード

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

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

スイッチング モードに関する注意事項と制限事項

各スイッチング モードについて、次の注意事項および制約事項を考慮してください。

カットスルー スイッチング モードに関する注意事項および制約事項

- フレーム チェック シーケンス（FCS）エラーがあるパケットはドロップされます。 次に例を示します。
  - Cisco Nexus 3064PQ プラットフォームの場合、768 バイト以下のパケットはドロップされます。
  - Cisco Nexus 3016、3064E、3064X、および 3048 プラットフォームの場合、560 バイト以下のパケットはドロップされます。
  - Cisco Nexus 3064PQ プラットフォームの場合、769 バイト以上のパケットが転送されます。
  - 3016、3064E、3064X、および 3048 プラットフォームの場合、561 バイト以上のパケットが転送されます。
- FCS エラーがあるパケットは、SPAN が設定されている場合はミラーリングされません。

Store-and-Forward スイッチング モードに関する注意事項および制約事項

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

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

スイッチング モードのライセンス要件

カットスルー スイッチング モードおよび Store-and-Forward スイッチング モードにはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

スイッチング モードのデフォルト設定

カットスルー スイッチングは、デフォルトでイネーブルになっています。

スイッチング モードの設定

Store-and-Forward スイッチングのイネーブル化

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **switching-mode store-forward**	Store-and-Forward スイッチング モードをイネーブルにします。
ステップ 3	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

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

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

カットスルー スイッチングの再イネーブル化

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

手順

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

次に、カットスルー スイッチングを再度イネーブルにする例を示します。

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

スイッチング モードの機能の履歴

表 *3* : **スイッチング モードの機能の履歴**

機能名	リリース	情報
Store-and-Forward スイッチング	5.0(3)U3(1)	この機能が導入されました。

第 7 章

Rapid PVST+ の設定

この章は、次の内容で構成されています。

- Rapid PVST+ について，49 ページ
- Rapid PVST+ の設定，68 ページ
- Rapid PVST+ の設定の確認，77 ページ

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（Rapid Spanning Tree Protocol（RSTP; 高速スパニングツリー プロトコル））です。 Rapid PVST+ は、IEEE 802.1D 規格との相互運用が可能で、VLAN ごとではなく、すべての VLAN で、単一の STP インスタンスの役割を委任されます

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 が稼働するスイッチ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。

（注） 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 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、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）と呼ばれる STP フレーム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 スイッチが 1 台選択されます。
- LAN セグメントごとに指定スイッチが 1 台選定されます。
- 冗長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 スイッチ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 スイッチが論理的にスパニングツリー トポロジの中心になります。 STP では、BPDU を使用して、スイッチド ネットワークのルート スイッチやルート 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。

（注） Cisco NX-OS では、拡張システム ID が常にイネーブルであり、拡張システム ID をディセーブルにできません。

拡張システム ID

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

図 *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 と組み合わされ、VLAN の固有識別子として機能します。

表 *4*：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

（注） 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。

（注） 同じスパ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

VLANごとに、ブリッジID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定されます。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。

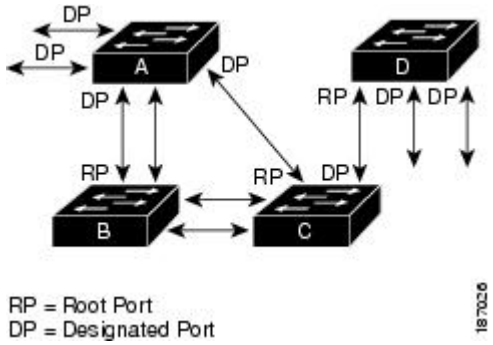
STPルートブリッジは論理的に、ネットワークで各スパニングツリートポロジの中心です。ネットワークの任意の箇所からルート ブリッジに到達するために必要ではないすべてのパスは、STP ブロッキング モードになります。

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

この図では、スイッチ A がルートブリッジに選定されます。これは、すべての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。 ただし、トラフィック パターン、転送ポートの数、またはリンク タイプによっては、スイッチ A が最適なルート ブリッジであるとは限りません。 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。

図 7：スパニングツリー トポロジ



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（Unshielded Twisted-Pair（UTP; シールドなしツイストペア）リンク）がルート ポートになっていると仮定します。 ネットワーク トラフィックを高速の光ファイバ リンクに流した方が効率的です。 光ファイバ ポートの STP ポート プライオリティをルート ポートよりも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 Rapid PVST+ インスタンスには、1 つのルート スイッチがあります。 Rapid PVST+ の実行中には、VLAN ベースで STP をイネーブルまたはディセーブルにできます。

（注） 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コンバージェンスが行われます。 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）。

（注） 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 BPDU 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 BPDU 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。 RSTP は、エッジ ポート、新しいルート ポート、およびポイントツーポイント リンクで接続されているポートに次のような高速コンバージェンスを提供します。

- 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。

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

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

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

- 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。

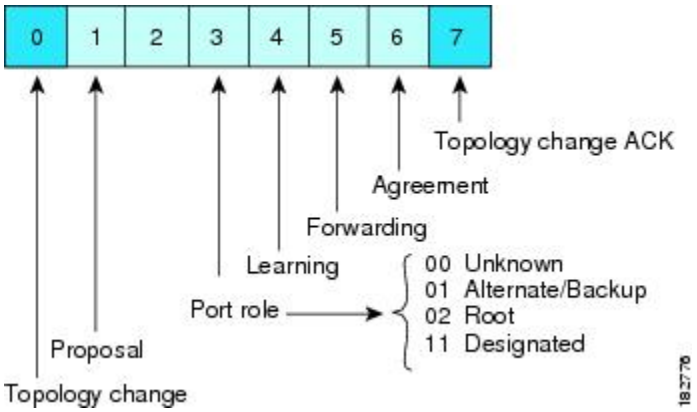
（注） スイッチが、レガシー 802.1D STP を実行しているスイッチと相互に動作しているときにのみ、TCA フラグが使用されます。

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+ BPDU

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、BPDU 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 BPDU フラグの使用について示します。

図 *8*： *BPDU* の *Rapid PVST+* フラグ バイト

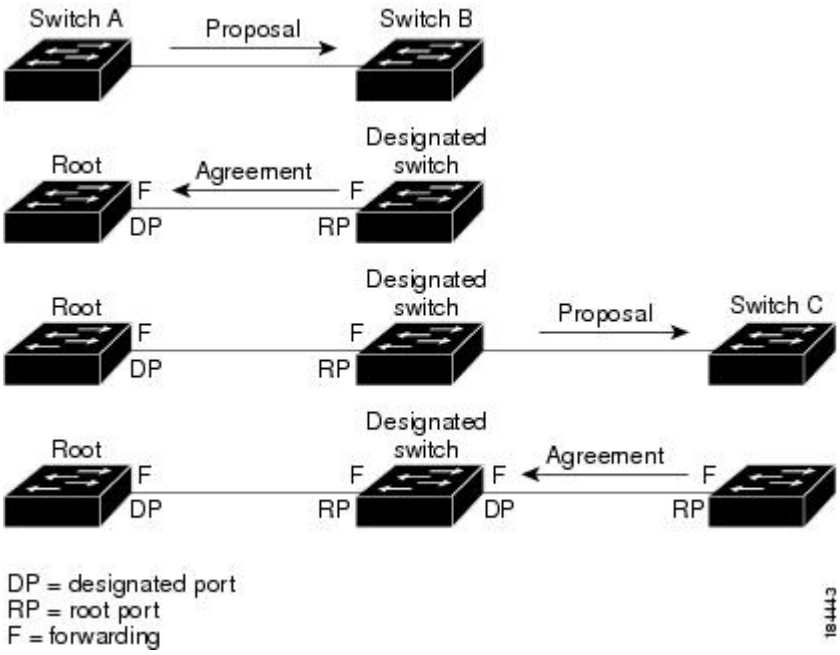


もう 1 つの重要な変更点は、Rapid PVST+ BPDU がタイプ 2、バージョン 2 であることで、これにより、スイッチでは、接続されているレガシー（802.1D）ブリッジを検出できるようになります。802.1D の BPDU は、バージョン 0 です。

提案と合意のハンドシェイク

次の図で示したように、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。 このとき、スイッチ A のプライオリティが、スイッチ B のプライオリティよりも小さい数値であるとします。

図 *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 は提案メッセージ（提案フラグ セットを設定したコンフィギュレーション BPDU）をスイッチ B に送信し、自分自身を指定スイッチとして提案します。

提案メッセージの受信後、スイッチ B は、その新しいルート ポートとして、提案メッセージが受信されたポートからポートを選択し、すべての非エッジポートをブロッキング ステートにし、新しいルート ポートを使ってアグリーメント メッセージ（合意フラグがオンに設定された 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は形成できません

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時には、この提案と合意のハンドシェーク処理がスパニングツリーのルートからリーフに進みます。

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。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は、**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ことで上書きできます。

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を及ぼすプロトコル タイマーを示します。

表 *5*：*Rapid PVST+* のプロトコル タイマー

変数	説明
hello 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 に構築され、最高のプライオリティ（最小数値のプライオリティの値）のスイッチがルート ブリッジとして選択されます。 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。

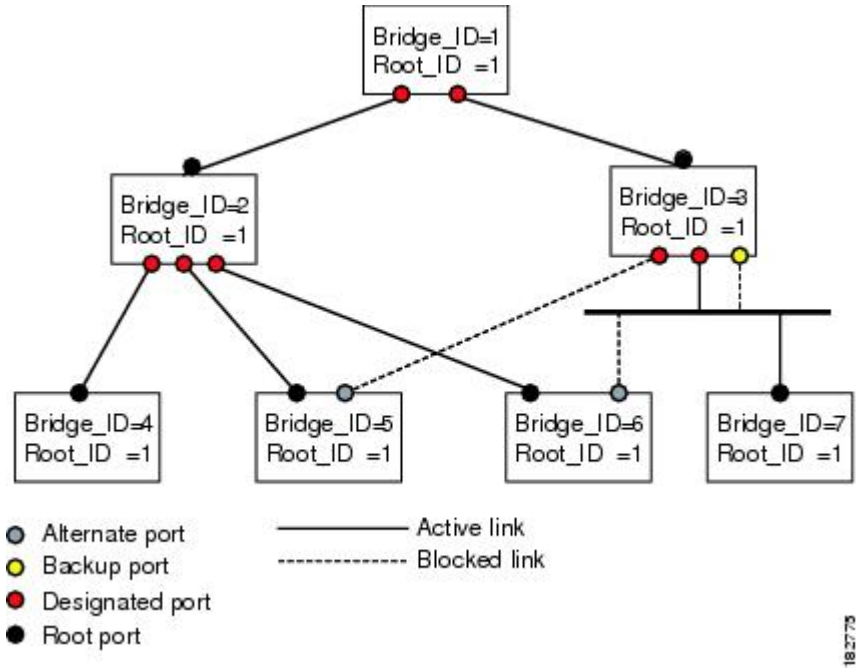
- ルート ポート：スイッチによりパケットがルート ブリッジに転送されるときに、最適のパス（最小コスト）を用意します。

- 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ロールが与えられていません。

ネットワーク全体でポートのロールに一貫性のある安定したトポロジでは、Rapid PVST+により、ルート ポートと指定ポートがすべてただちにフォワーディング ステートになり、代替ポートとバックアップ ポートはすべて、必ずブロッキング ステートになります。 指定ポートはブロッキング ステートで開始されます。 フォワーディング プロセスおよびラーニング プロセスの動作はポート ステートによって制御されます。

ルート ポートまたはDP の役割があるポートは、アクティブ トポロジーに組み込まれます。 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）。

図 *10*：ポート 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。

Rapid PVST+ 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 モジュールから受信した BPDU を、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 モジュールから受信した BPDU を、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 （学習は行われないため、アドレス データベースは更新されません）。
- ネイバーから BPDU を受信しません。
- システム モジュールから送信用の BPDU を受信しません。

ポート ステートの概要

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。

表 *6*：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	ポート ステート	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	No
イネーブル	ラーニング	Yes
イネーブル	フォワーディング	Yes
ディセーブル	ディセーブル	No

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。

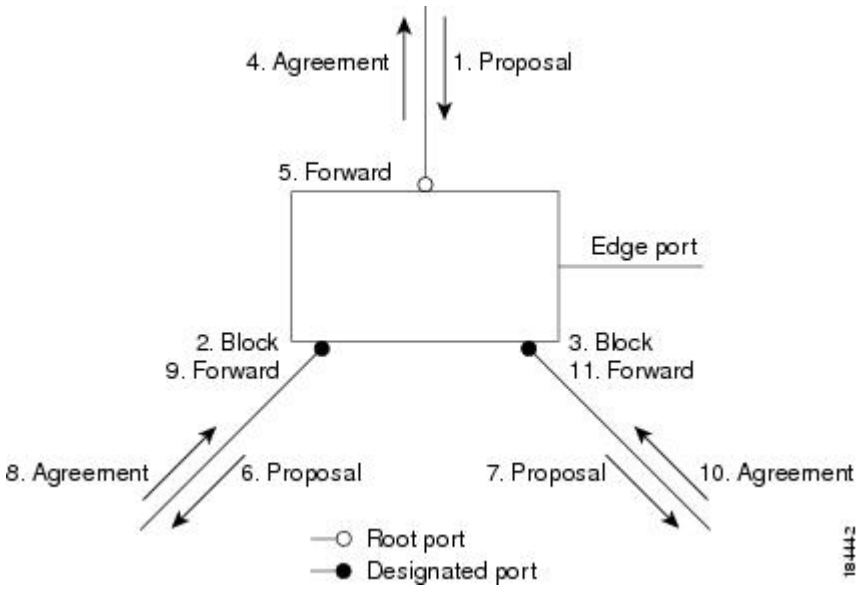
他のすべてのポートが同期化されると、スイッチはルート ポートで受信した優位のルート情報に同期化されます。 次のいずれかが当てはまる場合、スイッチ上の個々のポートで同期がとられます。

- ブロッキング ステートである場合
- エッジ ポートである場合（ネットワークのエッジとして設定されているポート）

指定ポートがフォワーディング ステートの場合で、エッジポートとして設定されていない場合、Rapid PVST+ により強制的に新しいルート情報との同期がとられるときに、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、アグリーメント 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。 イベントのシーケンスを次の図に示します。

図 *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 がプロポーザル 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、アグリーメント 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、アグリーメント 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、プロポーザル 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、独自の情報ですぐに応答します。

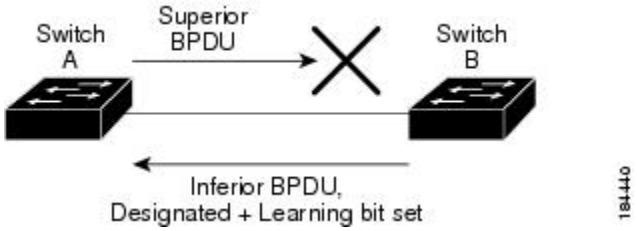
スパニングツリー異議メカニズム

ソフトウェアを使用することで、受信したBPDUからポートの役割とステートの一貫性を確認し、単一方向リンクが失敗してブリッジ処理のループを引き起こしていないかどうかを検証できます。

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 ループを解決できるからです。

次の図に、ブリッジング ループ発生の一般的な原因となる単一方向リンク障害を示します。 スイッチ A はルート ブリッジで、その BPDU は、スイッチ B へのリンク上では失われます。 802.1w 規格の BPDU には送信ポートのロールおよびステートが含まれます。 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。 結果として、スイッチ A は自身のポートをブロックし（またはブロックを維持して）、ブリッジ処理のループを回避します。 ブロックは、STP の矛盾として示されます。

図 *12*： 単一方向リンク障害の検出



ポート コスト

（注） Rapid PVST+ では、デフォルトで、ショート型（16 ビット）のパスコスト方式を使用して、コストが計算されます。 ショート型のパスコスト方式では、1 ～ 65535 の範囲で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。

表 7：デフォルトのポート コスト

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

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

アクセス ポートでは、ポートごとにポート 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 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、Rapid PVST+ 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。 Rapid PVST+ に最初に選択させる LAN ポートには小さいプライオリティ値を割り当て、Rapid PVST+ に最後に選択させる LAN ポートには大きいプライオリティ値を割り当てます。

すべての LAN ポートに同じプライオリティ値が割り当てられている場合、Rapid PVST+ は、LAN ポート番号が最小の LAN ポートをフォワーディング ステートにし、他の LAN ポートをブロックします。 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されます。 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、プロポーザル 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、アグリーメント 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、スイッチはプロポーザル フラグを設定せずに、ポートの転送遅延タイマーを開始します。 新しいルート ポートはフォワーディング ステートに移行するために 2 倍の転送遅延時間を必要とします。

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見なして、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。

（注） 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 Multiple Spanning Tree（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。

（注） スパニングツリー モードを変更すると、変更前のモードのスパニングツリー インスタンスがすべて停止されて新しいモードで起動されるため、トラフィックが中断する場合があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree mode rapid-pvst**	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。 （注） スパニングツリー モードを変更すると、変更前のモードのスパニングツリー インスタンスがすべて停止されて新しいモードで起動されるため、トラフィックが中断する場合があります。

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
```

（注） STP はデフォルトでイネーブルのため、設定結果を参照するために **show running-config** コマンドを入力しても、Rapid PVST+ 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。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree** *vlan-range*	VLAN ごとに Rapid PVST+（デフォルト STP）をイネーブルにします。 *vlan-range* の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。
ステップ 3	switch(config)# **no spanning-tree** *vlan-range*	（任意） 指定 VLAN で Rapid PVST+ をディセーブルにします。 **注意** 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限り、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なるため、この処理によって予想外の結果となることがあります。 VLAN 内に物理的なループが存在しないことを保証できる場合以外は、VLAN でスパニングツリーをディセーブルにしないでください。 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。

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。 各 VLAN では、最も小さいブリッジ ID を持つスイッチが VLAN のルート ブリッジになります。

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

spanning-tree vlan *vlan_ID* **root** コマンドを入力すると、各 VLAN の現在のルート ブリッジのブリッジ プライオリティ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。

（注） 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** コマンドはエラーになります。

注意 STP の各インスタンスのルート ブリッジは、バックボーン スイッチまたはディストリビューション 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、その直径のネットワークに最適な hello タイム、転送遅延時間、最大経過時間が自動的に選択されます。これにより、STP 収束の時間が大幅に削減されます。 キーワード **hello-time** を入力すると、自動的に計算された hello タイムを上書きできます。

（注） ルート ブリッジとして設定されているスイッチでは、hello タイム、転送遅延時間、最大エージング タイムは手動で設定（**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、**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）しないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree vlan** *vlan-range* **root primary** [**diameter** *dia* [**hello-time** *hello-time*]]	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。 *vlan-range* の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。*dia* のデフォルトは 7 です。 *hello-time* の範囲は 1 ～ 10 秒で、デフォルト値は 2 秒です。

次に、VLAN のルート ブリッジとしてスイッチを設定する例を示します。

```
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）から変更しておくと、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、その直径のネットワークに最適な hello タイム、転送遅延時間、最大経過時間が自動的に選択されます。これにより、STP コンバージェンスの時間が大幅に削減されます。 キーワード **hello-time** を入力すると、自動的に計算された hello タイムを上書きできます。

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。

（注） 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 タイムは手動で設定（**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、**spanning-tree mst max-age** の各グローバル コンフィギュレーション コマンドを使用）しないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree vlan** *vlan-range* **root secondary** [**diameter** *dia* [**hello-time** *hello-time*]]	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。 *vlan-range* の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。*dia* のデフォルトは 7 です。 *hello-time* の範囲は 1 ～ 10 秒で、デフォルト値は 2 秒です。

次に、VLAN のセカンダリ ルート ブリッジとしてスイッチを設定する例を示します。

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

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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot*/*port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	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。 *priority* の値は 0 ～ 224 を指定できます。 値が小さいほどプライオリティが高くなります。 プライオリティ値は、0、32、64、96、128、160、192、224 です。 その他すべての値は拒否されます。 デフォルト値は 128 です。

次に、イーサネット インターフェイスのアクセス ポート プライオリティを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-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+ のパス コスト方式とポート 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。

（注） 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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree pathcost method** {**long** | **short**}	Rapid PVST+ パス コストの計算に使用される方式を選択します。 デフォルト方式は short 型です。
ステップ 3	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。
ステップ 4	switch(config-if)# **spanning-tree** [**vlan** *vlan-id*] **cost** [*value* | **auto**]	LAN インターフェイスのポート コストを設定します。 コストの値は、パス コスト計算の方式により、次の値になります。 • ショート型：1 ～ 65535 • ロング型：1 ～ 200000000 （注） このパラメータは、アクセス ポートの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。 デフォルトは **auto** で、パス コスト計算方式とメディア速度の両方に基づいてポート コストが設定されます。

次に、イーサネット インターフェイスのアクセス ポート コストを設定する例を示します。

```
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。

（注） 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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree vlan** *vlan-range* **priority** *value*	VLAN のブリッジ プライオリティを設定します。有効な値は 0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。 その他すべての値は拒否されます。 デフォルト値は 32768 です。

次に、VLAN のブリッジ プライオリティを設定する例を示します。

```
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。

（注） 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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree vlan** *vlan-range* **hello-time** *hello-time*	VLAN の hello タイムを設定します。 hello タイム値には 1 ～ 10 秒を指定できます。 デフォルト値は 2 秒です。

次に、VLAN の hello タイムを設定する例を示します。

```
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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **spanning-tree vlan** *vlan-range* **forward-time** *forward-time*	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。

次に、VLAN の転送遅延時間を設定する例を示します。

```
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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree vlan** *vlan-range* **max-age** *max-age*	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。

次に、VLAN の最大エージング タイムを設定する例を示します。

```
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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot*/*port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	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 イ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。

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* [*interface-num* | *port-channel*]]	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+ を再起動する例を示します。

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

Rapid PVST+ の設定の確認

Rapid PVST+ の設定情報を表示するには、次のいずれかの処理を実行します。

コマンド	目的
switch# **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。
switch# **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。

次の例は、スパ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 8 章

Multiple Spanning Tree の設定

この章は、次の内容で構成されています。

- MST について，79 ページ
- MST の設定，88 ページ
- MST の設定の確認，106 ページ

MST について

MST の概要

（注） 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 をスパニングツリー インスタンスにマッピングします。各インスタンスには、他のスパニングツリー インスタンスとは別のスパニングツリー トポロジがあります。 このアーキテクチャでは、データ トラフィックに対して複数のフォワーディング パスがあり、ロードバランシングが可能です。これによって、非常に多数の VLAN をサポートする際に必要な STP インスタンスの数を削減できます。

MST では、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コンバージェンスが可能なため、802.1D転送遅延がなくなり、ルート ブリッジ ポートと指定ポートが迅速にフォワーディング ステートに変わります

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 802.1w では RSTP が定義されて、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。

（注） 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 MST インスタンス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 領域は、同じ MST 設定で MST ブリッジのグループとリンクされます。

MST 設定により、各スイッチが属す MST リージョンが制御されます。 設定には、リージョンの名前、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 領域には、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）をサポートできます。インスタンスは、1 ～ 4094 の範囲の任意の番号によって識別されます。 インスタンス 0 は、特別なインスタンスである IST 用に予約されています。 VLAN は、一度に 1 つの MST インスタンスに対してのみ割り当てることができます。

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

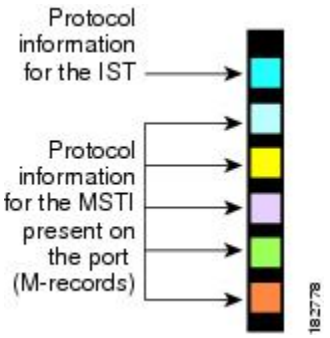
（注） ネットワークを、多数のリージョンに分け過ぎないことを推奨します。

MST BPDU

各リージョンに含まれる MST BPDU は 1 つだけで、その BPDU により、リージョン内の各 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 領域の 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。

図 *13*： *MSTI* の *M* レコードが含まれる *MST BPDU*



MST 設定情報

MST の設定は 1 つの MST リージョン内のすべてのスイッチで同一である必要があり、ユーザが設定します。

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 領域を指定します。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。

（注） 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。 リビジョン番号は、MST 設定がコミットされるごとに自動的には増やされません。

- 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。

注意 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 をその領域に受け入れます。 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 領域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 リージョンで実行されるスパニングツリーです。

MST では、各 MST リージョン内に追加のスパニングツリーが確立され、維持されます。これらのスパニングツリーを MSTI（複数スパニングツリー インスタンス）といいます。

インスタンス 0 は、IST という、リージョン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 に割り当てられています。 その他の MST インスタンスはすべて 1 ～ 4094 まで番号が付けられます。

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 リージョンにある IST の集まりです。 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 リージョン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、リージョンにあるすべての MST 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。 また、リージョンがネットワーク内に 1 つしかなければ、CIST リージョナル ルートは CIST ルートにもなります。 CIST ルートがリージョン外にある場合、リージョンの境界にある MST スイッチの 1 つが、CIST リージョナル ルートとしてプロトコルにより選択されます。

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。

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

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

MST 領域間のスパニングツリー動作

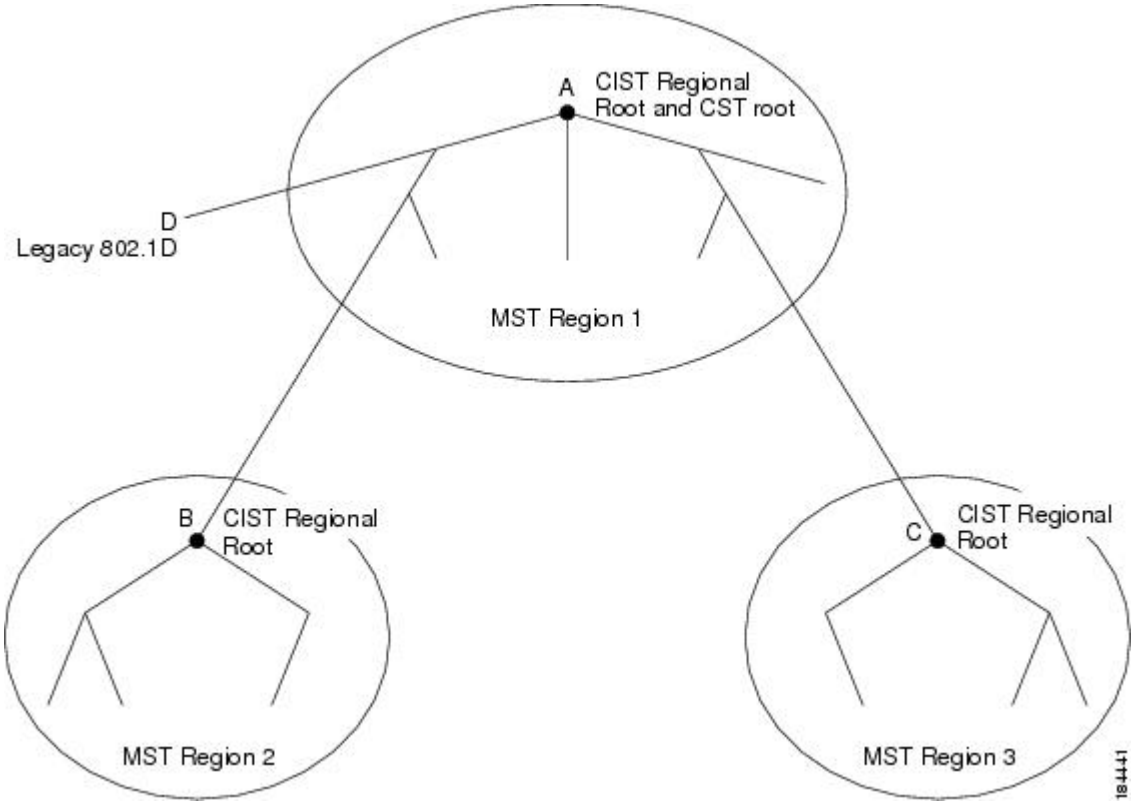
ネットワーク内に複数のリージョン、または 802.1 w や 802.1D STP インスタンスがある場合、MST はネットワーク内のすべての MST リージョン、すべての 802.1w と 802.1D STP スイッチを含む CST を確立して、維持します。 MSTI は、領域の境界で IST と結合して CST になります。

IST は、リージョン内のすべての MST スイッチを接続し、スイッチ ドメイン全体を含んだ CIST 内のサブツリーとして認識されます。 サブツリーのルートは CIST リージョナル ルートです。 MST 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 リージョンと 1 つの 802.1D スイッチ（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）、およびリージョン 3 の CIST リージョナル ルート（C）は、CIST 内のそれぞれのサブツリーのルートです。

図 *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用される外部パラメータと比較されます。 CIST だけがネットワーク全体に広がるスパニングツリー インスタンスなの

で、CISTパラメータだけに外部修飾子が必要になり、修飾子または領域修飾子は不要です。 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ルートがリージョン内にある場合、CISTリージョナル ルートがCISTルートになります。 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、リージョン内の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（インスタンス0）のみに関係します。

ホップ カウント

MST領域内のSTPトポロジを計算する場合、MSTはコンフィギュレーションBPDUのメッセージ有効期間と最大エージング 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ことにより、リージョン内の最大ホップを設定し、その値をリージョン内のISTインスタンスとすべてのMSTインスタンスに適用できます。

ホップ カウントを設定すると、メッセージ エージ情報を設定するのと同様の結果が得られます（再構成の開始時期を決定します）。 インスタンスのルートブリッジは、コストが0でホップ カウントが最大値に設定されたBPDU（Mレコード）を常に送信します。 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。

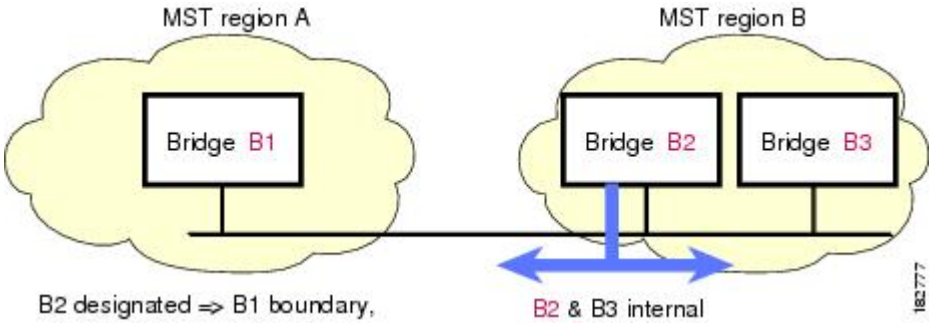
スイッチがスパニングツリー設定メッセージを受信せずに再設定を試行するまで待機する秒数として最大エージング タイムを設定します。

境界ポート

境界ポートは1つのリージョンを別のリージョン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、リージョンの内部にある2つのポー

トが、異なるリージョンに属する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をもたらします（次の図を参照）。

図 *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 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 ロール以外のすべてのポート ロールを引き継ぐことができます。

スパニングツリー異議メカニズム

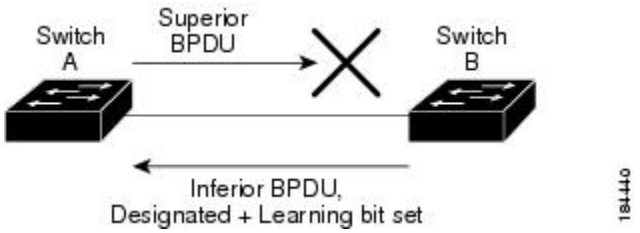
現在、この機能は、IEEE MST 規格にはありませんが、規格準拠の実装に含まれています。 ソフトウェアを使用することで、受信した BPDU からポートの役割とステートの一貫性を確認し、単一方向リンクが失敗してブリッジ処理のループを引き起こしていないかどうかを検証できます。

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 ループを解決できるからです。

次の図に、ブリッジング ループ発生の一般的な原因となる単一方向リンク障害を示します。 スイッチ A はルート ブリッジで、その BPDU は、スイッチ B へのリンク上では失われます。 Rapid PVST+（802.1w）および MST BPDU は、送信ポートのロールおよびステートが含まれます。 この情報により、スイッチ B は送信される上位 BPDU に対して反応せず、スイッチ B はルート ポートではなく指定ポートであることが、スイッチ A によって検出できます。 この結果、スイッチ A

は、そのポートをブロックし（またはブロックし続け）、ブリッジング ループが防止されます。ブロックは、STP の矛盾として示されます。

図 *16*： 単一方向リンク障害の検出



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。

（注） MST では、ロング パス コスト計算方式が常に使用されるため、有効値の範囲は、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プライオリティは 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。 さらに、MST スイッチでは、802.1D BPDU、異なるリージョンにアソシエートされている MST BPDU（バージョン 3）、または 802.1w BPDU（バージョン 2）を受信するときに、ポートがリージョン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、自動的には 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（強制的に隣接スイッチと再ネゴシエーションさせる）には、**clear spanning-tree detected-protocols** コマンドを入力します。

リンク上にあるすべての Rapid PVST+ スイッチ（およびすべての 8021.D STP スイッチ）では、MST BPDU を 802.1w BPDU の場合と同様に処理できます。 MST スイッチでは、境界ポート上にある、バージョン 0 コンフィギュレーションおよびトポロジ変更通知（TCN）BPDU、またはバージョン 3 MST BPDU のいずれかを送信できます。 境界ポートは 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。

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

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性がイネーブルにされます。

（注） PVST シミュレーションは、デフォルトでイネーブルになっています。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。

ポートごと、またはスイッチ全体にグローバルに、Rapid PVST+ シミュレーションをディセーブルにできますが、これを実行することにより、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 ステートになります。 このポートは、Rapid PVST+/SSTP BPDU の受信が停止されるまで不整合のステートのままになります。そしてポートは、通常の STP 送信プロセスに戻ります。

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。

- プライベート VLAN を操作するときには、**private-vlan synchronize** コマンドを使用して、プライマリ VLAN として、セカンダリ VLAN を同じ MST インスタンスにマッピングします。
- MST コンフィギュレーション 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。
  - 変更を一切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。
  - モードの終了前に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 のイネーブル化

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。

注意 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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree mode mst**	スイッチ上で MST をイネーブルにします。
ステップ 3	switch(config)# **no spanning-tree mode mst**	（任意） スイッチ上の MST がディセーブルにされ、Rapid PVST+ に戻ります。

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
```

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

（注） 各コマンド参照行により、MST コンフィギュレーション モードで保留中の領域設定が作成されます。 さたに、保留中の領域設定により、現在の領域設定が開始されます。

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** と **abort** コマンドの違いに注意してください。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree mst configuration**	システムで MST コンフィギュレーション モードを開始します。 次のように MST 設定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。 • 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 • プライベート VLAN でのプライマリ VLAN とセカンダリ VLAN との同期
ステップ 3	switch(config-mst)# **exit** または switch(config-mst)# **abort**	• 最初の形式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。 • 2 番めの形式は、変更を一切コミットせずに MST コンフィギュレーション モードを終了します。
ステップ 4	switch(config)# **no spanning-tree mst configuration**	（任意） MST 領域設定を次のデフォルト値に戻します。 • 領域名は空の文字列になります。

	コマンドまたはアクション	目的
		• 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

リージョン名は、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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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。
ステップ 3	switch(config-mst)# **name** *name*	MST リージョンの名前を指定します。 *name* ストリングには最大 32 文字まで使用でき、大文字と小文字が区別されます。 デフォルトは空の文字列です。

次の例は、MST 領域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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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。
ステップ 3	switch(config-mst)# **revision** *version*	MST 領域のリビジョン番号を指定します。範囲は 0 ～ 65535 で、デフォルト値は 0 です。

次の例は、MSTI リージョンのリビジョン番号を 5 に設定する方法を示しています。

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

MST 領域での設定の指定

2 台以上のスイッチを同一 MST リージョン内に存在させるには、同じ VLAN からインスタンスへのマッピング、同じ構成リビジョン番号、および同じ MST の名前が設定されている必要があります。

領域には、同じ MST 設定の 1 つのメンバーまたは複数のメンバーを存在させることができます。各メンバーでは、IEEE 802.1w RSTP BPDU を処理できる必要があります。 ネットワーク内の MST 領域には、数の制限はありませんが、各領域では、最大 65 までのインスタンスをサポートできます。 VLAN は、一度に 1 つの MST インスタンスに対してのみ割り当てることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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。
ステップ 3	switch(config-mst)# **instance** *instance-id* **vlan** *vlan-range*	VLAN を MST インスタンスにマッピングする手順は、次のとおりです。 • *instance-id* の範囲は 1 ～ 4094 です。 • **vlan** *vlan-range* の範囲は 1 ～ 4094 です。

	コマンドまたはアクション	目的
		MST インスタンスに VLAN をマッピングする場合、マッピングはインクリメンタルに行われ、コマンドで指定された VLAN がすでにマッピング済みの VLAN に対して追加または削除されます。 VLAN 範囲を指定する場合は、ハイフンを使用します。たとえば、**instance 1 vlan 1-63** とコマンドを入力すると、MST インスタンス 1 に VLAN 1 ～ 63 がマッピングされます。 一連の VLAN を指定する場合はカンマで区切ります。たとえば、**instance 1 vlan 10, 20, 30** コマンドを入力すると、MST インスタンス 1 に VLAN 10、20、および 30 がマッピングされます。
ステップ 4	switch(config-mst)# **name** *name*	インスタンス名を指定します。 *name* ストリングには最大 32 文字使用でき、大文字と小文字が区別されます。
ステップ 5	switch(config-mst)# **revision** *version*	設定リビジョン番号を指定します。 指定できる範囲は 0 ～ 65535 です。

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 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 コマンドを入力します。
- デフォルトの名前に戻すには、**no name** MST コンフィギュレーション コマンドを入力します。
- デフォルトのリビジョン番号に戻すには、**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、リージョンに region1 という名前を付けて、設定リビジョンを 1 に設定し、保留中の設定を表示し、変更を適用してグローバル コンフィギュレーション モードに戻る方法を示しています。

```
switch(config)# 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

注意 VLAN/MSTI マッピングを変更すると、MST は再起動されます。

（注） 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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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。
ステップ 3	switch(config-mst)# **instance** *instance-id* **vlan** *vlan-range*	VLAN を MST インスタンスにマッピングする手順は、次のとおりです。 • *instance-id* の範囲は 1 ～ 4094 です。 インスタンス 0 は、各 MST リージョンでの IST 用に予約されています。 • *vlan-range* の範囲は 1 ～ 4094 です。 VLAN を MSTI にマッピングすると、マッピングは差分で実行され、コマンドで指定された

	コマンドまたはアクション	目的
		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。
ステップ 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。

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
```

プライベート VLAN でセカンダリ VLAN をプライマリ VLAN として同じ MSTI にマッピングするには

システム上のプライベート VLAN を操作するときに、すべてのセカンダリ VLAN は、同じ MSTI とそれがアソシエートされているプライマリ VLAN に存在させておく必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **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。
ステップ 3	switch(config-mst)# **private-vlan synchronize**	すべてのセカンダリ VLANを、同じMSTIと、すべてのプライベート VLAN にアソシエートされているプライマリ VLANに、自動的にマッピングします。

次の例は、すべてのプライベート VLAN と同じ MSTI および関連プライマリ VLAN にすべてのセカンダリ VLAN を自動的にマッピングする方法を示しています。

```
switch# configure terminal
switch(config)# spanning-tree mst configuration
switch(config-mst)# private-vlan synchronize
```

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。

（注） 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。 hello キーワードを入力すると、自動的に計算された hello タイムを上書きできます。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]]	次のように、ルート ブリッジとしてスイッチを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 有効な範囲は 1 ～ 4094 です。 • diameter *net-diameter* には、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、MST インスタンス 0 にだけ使用できます。 • hello-time *seconds* には、ルート ブリッジによって生成された設定メッセージの間隔を秒単位で指定します。 有効な範囲は 1 ～ 10 秒で、デフォルトは 2 秒です。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **no spanning-tree mst** *instance-id* **root**	（任意） 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。

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も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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]]	次のように、セカンダリ ルート ブリッジとしてスイッチを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。有効な範囲は 1 ～ 4094 です。 • diameter *net-diameter* には、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、MST インスタンス 0 にだけ使用できます。 • hello-time *seconds* には、ルート ブリッジによって生成された設定メッセージの間隔を秒単位で指定します。 有効な範囲は 1 ～ 10 秒で、デフォルトは 2 秒です。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **no spanning-tree mst** *instance-id* **root**	（任意） 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。

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。最初に選択させるインターフェイスには低いプライオリティの値を割り当て、最後に選択させるインターフェイスには高いプライオリティの値を割り当てることができます。 すべてのインターフェイスのプライオリティ値が同一である場合、MST はインターフェイス番号が最も低いインターフェイスをフォワーディング ステートにして、その他のインターフェイスをブロックします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {{*type slot*/*port*} | {**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。
ステップ 3	switch(config-if)# **spanning-tree mst** *instance-id* **port-priority** *priority*	次のように、ポートのプライオリティを設定します。 • *instance-id* には、1 つの MSTI、それぞれをハイフンで区切った MSTI の範囲、またはカンマで区切った一連の MSTI を指定できます。 有効な範囲は 1 ～ 4094 です。 • *priority* の範囲は 0 ～ 224 で、32 ずつ増加します。 デフォルトは 128 です。 値が小さいほど、プライオリティが高いことを示します。 プライオリティ値は、0、32、64、96、128、160、192、224 です。 システムでは、他のすべての値が拒否されます。

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派生します。 ループが発生した場合、MST は、コストを使用して、フォワーディング ステートにするインターフェイスを選択します。 最初に選択させるインターフェイスには小さいコストの値を割り当て、最後に選択させるインターフェイスの値には大きいコストを割り当てることができます。 すべてのインターフェイスのコスト値が同一である場合、MST はインターフェイス番号が最も低いインターフェイスをフォワーディング ステートにして、その他のインターフェイスをブロックします。

（注） MST では、ロング パス コスト計算方式が使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {{*type slot*/*port*} | {**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。
ステップ 3	switch(config-if)# **spanning-tree mst** *instance-id* **cost** [*cost* | **auto**]	コストを設定します。 ループが発生する場合、MST は、フォワーディング ステートにするインターフェイスを選択するとき、パス コストを使用します。 パス コストが小さいほど、送信速度が速いことを示します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 有効な範囲は 1 ～ 4094 です。 • *cost* の範囲は 1 ～ 200000000 です。 デフォルト値は auto で、インターフェイスのメディア速度から取得されるものです。

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
```

スイッチの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。

（注） 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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree mst** *instance-id* **priority** *priority-value*	次のように、スイッチのプライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 有効な範囲は 1 ～ 4094 です。 • priority の範囲は 0 ～ 61440 で、4096 ずつ増加します。 デフォルト値は 32768 です。 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。 プライオリティ値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。 システムでは、他のすべての値が拒否されます。

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。

（注） 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、hello タイムを変更するには、**spanning-tree mst** *instance-id* **root primary** および **spanning-tree mst** *instance-id* **root secondary** コンフィギュレーション コマンドの使用を推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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間隔です。 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。 *seconds* の範囲は 1 ～ 10 で、デフォルトは 2 秒です。

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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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

	コマンドまたはアクション	目的
		数です。 *seconds* の範囲は 4 ～ 30 で、デフォルトは 15 秒です。

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
```

最大経過時間の設定

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）。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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。 *seconds* の範囲は 6 ～ 40 で、デフォルトは 20 秒です。

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。 リージョン内の最大ホップを設定し、それを、そのリージョンにある IST とすべての MST インスタンスに適用できます。 ホップ カウントを設定すると、メッセージ エージ情報を設定するのと同様の結果が得られます（再構成の開始時期を決定します）。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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* の範囲は 1 ～ 255 で、デフォルト値は 20 ホップです。

次の例は、最大ホップ カウントを 40 に設定する方法を示しています。

```
switch# 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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no 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インターフェイスをディセーブルにできます。 これはデフォルトでイネーブルです。つまり、デフォルトでは、スイッチ上のすべてのインターフェイスは、Rapid PVST+ と MST との間でシームレスに動作します。

次の例は、Rapid PVST+ 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。 Rapid PVST+ シミュレーションをディセーブルにした場合、MST がイネーブルなポートが Rapid PVST+ がイネーブルなポートに接続されていることが検出されると、MST がイネーブルなポートは、ブロッキング ステートに移行します。 このポートは、BPDU の受信が停止されるまで、一貫性のないステートのままになり、それから、ポートは、通常の STP 送信プロセスに戻ります。

この自動機能は、グローバルまたはポートごとにブロックできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {{*type slot*/*port*} | {**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。
ステップ 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。
ステップ 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。
ステップ 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設定します。

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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	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。

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 ブリッジでは、レガシー BPDU または異なるリージョンにアソシエートされている MST BPDU を受信するときに、ポートがリージョンの境界にあることを検出できます。 ただし、STP プロトコルの移行では、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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **clear spanning-tree detected-protocol** [**interface** *interface* [*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。

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、次のいずれかの作業を行います。

コマンド	目的
switch# **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。
switch# **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 9 章

STP 拡張機能の設定

この章は、次の内容で構成されています。

- STP 拡張機能について，107 ページ

STP 拡張機能について

シスコではコンバージェンスがより効率的になる拡張機能を STP に追加しました。 場合によっては、同様の機能が IEEE 802.1w Rapid Spanning Tree Protocol（RSTP; 高速スパニングツリー プロトコル）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、Rapid per VLAN Spanning Tree（RPVST+）および Multiple Spanning Tree（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、Bridge Protocol Data Units（BPDU; ブリッジ プロトコル データ ユニット）ガード、BPDU フィルタリング、ループ ガード、ルート ガードがあります。 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。

（注） 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 ステートを経由することなく、フォワーディング ステートに直接移行します （この直接移行動作は、以前は、シスコ独自の機能 PortFast として設定していました）。

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。

（注） 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 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だけに接続されます。 Bridge Assurance がグローバルにイネーブルになっているときに、「ネットワーク」としてポートを設定すると、そのポート上で Bridge Assurance がイネーブルになります。

（注） 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 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。

（注） 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。

（注） BPDU ガードをグローバル単位でイネーブルにすると、動作中のすべてのスパニングツリー エッジ インターフェイスに適用されます。

BPDU フィルタリングの概要

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キングであるか否かに関係なく、インターフェイス全体に適用されます。

注意 BPDU フィルタリングをインターフェイスごとに設定するときは注意が必要です。 ホストに接続されていないポートに BPDU フィルタリングを明示的に設定すると、ブリッジング ループに陥る可能性があります。 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ければ、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。

表 *8*： *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	イネーブル	イネーブル	イネーブル。ポートは最低 10 個の BPDU を送信します。 このポートは、BPDU を受信すると、スパニングツリー標準ポート状態に戻り、BPDU フィルタリングはディセーブルになります。
デフォルト	イネーブル	ディセーブル	ディセーブル
デフォルト	ディセーブル	イネーブルまたはディセーブル	ディセーブル
ディセーブル	イネーブルまたはディセーブル	イネーブルまたはディセーブル	ディセーブル

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
イネーブル	イネーブルまたはディセーブル	イネーブルまたはディセーブル	イネーブル 注意 BPDU は一切送信されず、受信された場合、これは通常の STP の動作をトリガーしないため、慎重に使用します。

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 ネットワークだけで役立ちます。 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。

（注） 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 Virtual LAN（VLAN; 仮想 LAN）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。 このポートは、上位 BPDU の送信を停止すると、再度ブロッキングを解除されます。 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。 このようにポートの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。 このようにして、ルート ガードはルート ブリッジを強制的に配置します。

ルート ガードをグローバルには設定できません。

（注） 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。

はじめる前に

STP が設定されていることを確認します。

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を確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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。 このコマンドでは、すべてのポートがホストまたはサーバに接続されているものとします。 エッジ ポートは、リンク アップすると、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。 デフォルトのスパニングツリー ポート タイプは「標準」です。
ステップ 3	switch(config)# **spanning-tree port type network default**	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。 このコマンドでは、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ものとします。 Bridge Assurance をイネーブルにすると、各ネットワーク ポート上で Bridge Assurance が自動的に実行されます。 デフォルトのスパニングツリーポートタイプは「標準」です。 （注） 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。

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**：このコマンドはアクセス ポートのエッジ動作を明示的にイネーブルにします。
- **spanning-tree port type edge trunk**：このコマンドはトランク ポートのエッジ動作を明示的にイネーブルにします。

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

- **spanning-tree port type normal**：このコマンドは、ポートを標準スパニングツリー ポートとして明示的に設定しますが、フォワーディング ステートへの直接移行はイネーブルにしません。
- **no spanning-tree port type**：このコマンドは、**spanning-tree port type edge default** コマンドをグローバル コンフィギュレーション モードで定義した場合に、エッジ動作を暗黙的にイネーブルにします。 エッジ ポートをグローバルに設定していない場合、**no spanning-tree port type** コマンドは、**spanning-tree port type disable** コマンドと同じです。

はじめる前に

STP が設定されていることを確認します。

インターフェイスがホストに接続されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot*/*port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **spanning-tree port type edge**	指定したアクセスインターフェイスをスパニングエッジ ポートに設定します。 エッジ ポートは、リンクアップすると、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。 デフォルトのスパニングツリー ポート タイプは「標準」です。

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**：このコマンドは指定したポートを明示的にネットワーク ポートとして設定します。 Bridge Assurance をグローバルにイネーブルにすると、スパニングツリー ネットワーク ポート上で Bridge Assurance が自動的に実行されます。
- **spanning-tree port type normal**：このコマンドは、ポートを明示的に標準スパニングツリー ポートとして設定します。このインターフェイス上では Bridge Assurance は動作しません。
- **no spanning-tree port type**：このコマンドは、**spanning-tree port type network default** コマンドをグローバル コンフィギュレーション モードで定義した場合に、ポートを暗黙的にスパニングツリー ネットワーク ポートとしてイネーブルにします。 Bridge Assurance をイネーブルにすると、このポート上で Bridge Assurance が自動的に実行されます。

（注） 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。

はじめる前に

STP が設定されていることを確認します。

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を確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** type slot/port	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。
ステップ 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。

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。

（注） すべてのエッジ ポートで BPDU ガードをイネーブルにすることを推奨します。

はじめる前に

STP が設定されていることを確認します。

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を確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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。

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**：インターフェイス上で BPDU ガードが無条件にイネーブルになります。
- **spanning-tree bpduguard disable**：インターフェイス上で BPDU ガードが無条件にディセーブルになります。
- **no spanning-tree bpduguard**：動作中のエッジ ポート インターフェイスに **spanning-tree port type edge bpduguard default** コマンドが設定されている場合、そのインターフェイスで BPDU ガードをイネーブルにします。

はじめる前に

STP が設定されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	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。

	コマンドまたはアクション	目的
ステップ 3	switch(config-if)# **spanning-tree bpduguard** {**enable** | **disable**}	指定したスパニングツリー エッジ インターフェイスの BPDU ガードをイネーブルまたはディセーブルにします。デフォルトでは、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。
ステップ 4	switch(config-if)# **no spanning-tree bpduguard**	（任意） インターフェイスの BPDU ガードをディセーブルにします。 （注） 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。

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。

注意 このコマンドの使用には注意してください。これを誤って使用すると、ブリッジング ループが発生することがあります。

（注） グローバルにイネーブルにされた BPDU フィルタリングは、動作中のエッジ ポートだけに適用されます。 ポートは数個の BPDU をリンクアップ時に送出してから、実際に、発信 BPDU のフィルタリングを開始します。 エッジポートは、BPDUを受信すると、動作中のエッジポート ステータスを失い、BPDU フィルタリングはディセーブルになります。

はじめる前に

STP が設定されていることを確認します。

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を確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree port type edge bpdufilter default**	すべてのスパニングツリー エッジ ポートで、BPDUフィルタリングを、デフォルトでイネーブルにします。 デフォルトでは、グローバルな BPDU フィルタリングはディセーブルです。

次に、すべての動作中のスパニングツリーエッジポートでBPDUフィルタリングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# spanning-tree port type edge bpdufilter 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、トランキング インターフェイスであるかどうかに関係なく、すべてのインターフェイスに適用されます。

注意 指定インターフェイスで **spanning-tree bpdufilter enable** コマンドを入力するときは注意してください。 ホストに接続されていないポートに BPDU フィルタリングを明示的に設定すると、ブリッジング ループに陥る可能性があります。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 bpdufilter enable**：インターフェイス上で BPDU フィルタリングが無条件にイネーブルになります。
- **spanning-tree bpdufilter disable**：インターフェイス上でBPDUフィルタリングが無条件にディセーブルになります。
- **no spanning-tree bpdufilter**：動作中のエッジ ポート インターフェイスに **spanning-tree port type edge bpdufilter default** コマンドが設定されている場合、そのインターフェイスで BPDU フィルタリングをイネーブルにします。

（注） 特定のポートだけで BPDU フィルタリングをイネーブルにすると、そのポートでの BPDU の送受信が禁止されます。

はじめる前に

STP が設定されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **spanning-tree bpdufilter** {**enable** | **disable**}	指定したスパニングツリー エッジ インターフェイスの BPDU フィルタリングをイネーブルまたはディセーブルにします。 デフォルトでは、BPDU フィルタリングはディセーブルです。
ステップ 4	switch(config-if)# **no spanning-tree bpdufilter**	（任意） インターフェイスの BPDU フィルタリングをディセーブルにします。 （注） 動作中のスパニングツリー エッジ ポート インターフェイスに spanning-tree port type edge bpdufilter default コマンドが設定されている場合、そのインターフェイスで BPDU フィルタリングをイネーブルにします。

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 bpdufilter 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。

（注） 指定インターフェイスでループ ガード コマンドを入力すると、グローバルなループ ガード コマンドが上書きされます。

はじめる前に

STP が設定されていることを確認します。

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を確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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。

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。

（注） 指定インターフェイスでループ ガード コマンドを入力すると、グローバルなループ ガード コマンドが上書きされます。

はじめる前に

STP が設定されていることを確認します。

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を確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot*/*port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	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。 （注） ループ ガードは、スパニングツリーの標準およびネットワーク インターフェイスだけで動作します。

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、次のいずれかの作業を行います。

コマンド	目的
switch# **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。
switch# **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 10 章

LLDP の設定

この章は、次の内容で構成されています。

- グローバル LLDP コマンドの設定，123 ページ
- インターフェイス LLDP コマンドの設定，125 ページ
- LLDP の MIB，127 ページ

グローバル LLDP コマンドの設定

グローバルな LLDP 設定値を設定できます。 これらの設定値には、ピアから受信した LLDP 情報を廃棄するまでの時間、任意のインターフェイスで LLDP 初期化を実行するまで待機する時間、LLDP パケットを送信するレート、ポートの説明、システム機能、システムの説明、およびシステム名が含まれます。

LLDP は一連の属性をサポートし、これらを使用してネイバー デバイスを検出します。 属性には、Type、Length、および Value の説明が含まれていて、これらを TLV と呼びます。 LLDP をサポートするデバイスは、ネイバーとの情報の送受信に TLV を使用できます。 設定情報、デバイスの機能、デバイス ID などの詳細情報は、このプロトコルを使用してアドバタイズできます。

スイッチは、次の必須の管理 LLDP TLV をサポートします。

- データセンター イーサネット パラメータ交換（DCBXP）TLV
- 管理アドレス TLV
- ポート記述 TLV
- ポート VLAN ID TLV（IEEE 802.1 に固有の TLV）
- システム機能 TLV
- システム記述 TLV
- システム名 TLV

Data Center Bridging Exchange Protocol（DCBXP）は LLDP を拡張したものです。 ピア間でのノード パラメータのアナウンス、交換、およびネゴシエートに使用されます。 DCBXP パラメータは特定の DCBXP TLV にパッケージ化されます。 この TLV は、受信した LLDP パケットに確認応答を提供するように設計されています。

DCBXP は LLDP がイネーブルの場合、デフォルトでイネーブルになっています。 LLDP がイネーブルの場合、DCBXP は [**no**] **ldp tlv-select dcbxp** コマンドを使用してイネーブルまたはディセーブルにできます。 LLDP による送信または受信がディセーブルであるポートでは、DCBXP はディセーブルになります。

LLDP 設定値を設定する手順は、次のとおりです。

はじめる前に

LLDP 機能がスイッチでイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **lldp** {**holdtime** *seconds* | **reinit** *seconds* | **timer** *seconds* | **tlv-select** {**dcbxp** | **management-address** | **port-description** | **port-vlan** | **system-capabilities** | **system-description** | **system-name**}}	LLDP オプションを設定します。 **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（10 ～ 255 秒）を設定します。 デフォルト値は 120 秒です。 **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（1 ～ 10 秒）を設定します。 デフォルト値は 2 秒です。 **timer** オプションを使用して、LLDP パケットを送信するレート（5 ～ 254 秒）を設定します。 デフォルト値は 30 秒です。 **tlv-select** オプションを使用して、タイプ、長さ、値（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になります。 **dcbxp** オプションを使用して、データセンターイーサネット パラメータ交換（DCBXP）TLV メッセージを指定します。 **managment-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。 **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。

	コマンドまたはアクション	目的
		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。 **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。 **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。 **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。
ステップ 3	switch(config)# **no lldp** {**holdtime** | **reinit** | **timer**}	LLDP 値をデフォルトにリセットします。
ステップ 4	（任意）switch#**show lldp**	LLDP 設定を表示します。

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 による管理アドレス TLV の送受信をイネーブルにする例を示します。

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

インターフェイス LLDP コマンドの設定

物理イーサネット インターフェイスの LLDP 機能を設定する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot*/*port*	変更するインターフェイスを選択します。
ステップ 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。

	コマンドまたはアクション	目的
ステップ 4	（任意）switch#**show lldp**	LLDP 設定を表示します。

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
LLDP Neighbors

Remote Peers Information on interface Eth1/40
Remote peer's MSAP: length 12 Bytes:
00    c0    dd    0e    5f    3a    00    c0    dd    0e    5f    3a

LLDP TLV's
LLDP TLV type:Chassis ID  LLDP TLV Length: 7
LLDP TLV type:Port ID  LLDP TLV Length: 7
LLDP TLV type:Time to Live  LLDP TLV Length: 2
LLDP TLV type:LLDP Organizationally Specific  LLDP TLV Length: 55
LLDP TLV type:LLDP Organizationally Specific  LLDP TLV Length: 5
LLDP TLV type:END of LLDPDU  LLDP TLV Length: 0

Remote Peers Information on interface Eth1/34
Remote peer's MSAP: length 12 Bytes:
00    0d    ec    a3    27    40    00    0d    ec    a3    27    69

LLDP TLV's
LLDP TLV type:Chassis ID  LLDP TLV Length: 7
LLDP TLV type:Port ID  LLDP TLV Length: 7
LLDP TLV type:Time to Live  LLDP TLV Length: 2
LLDP TLV type:LLDP Organizationally Specific  LLDP TLV Length: 55
LLDP TLV type:LLDP Organizationally Specific  LLDP TLV Length: 5
LLDP TLV type:END of LLDPDU  LLDP TLV Length: 0

Remote Peers Information on interface Eth1/33
Remote peer's MSAP: length 12 Bytes:
00    0d    ec    a3    27    40    00    0d    ec    a3    27    68
```

```
LLDP TLV's
LLDP TLV type:Chassis ID  LLDP TLV Length: 7
LLDP TLV type:Port ID  LLDP TLV Length: 7
LLDP TLV type:Time to Live  LLDP TLV Length: 2
LLDP TLV type:LLDP Organizationally Specific  LLDP TLV Length: 55
LLDP TLV type:LLDP Organizationally Specific  LLDP TLV Length: 5
LLDP TLV type:END of LLDPDU  LLDP TLV Length: 0
```

次に、LLDP タイマーの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	MIB Link
LLDP-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

第 11 章

MAC アドレス テーブルの設定

この章は、次の内容で構成されています。

- MAC アドレスの概要，129 ページ
- MAC アドレスの設定，130 ページ
- MAC アドレスの設定の確認，132 ページ

MAC アドレスの概要

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 デバイスのメディア アクセス コントロール（MAC）アドレスを受信側の LAN ポートに関連付けます。

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 ポートへフラッディングします。 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 ポートにフラッディング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。

さらに、マルチキャスト アドレスを静的に設定された MAC アドレスとして入力することもできます。マルチキャストアドレスは、複数のインターフェイスを送信先として受け付けることができます。

アドレステーブルには、フレームを一切フラッディングさせることなく、多数のユニキャスト アドレス エントリおよびマルチキャスト 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ージング タイマーによって定義されたエージング 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 アドレスの設定

スタティック MAC アドレスの設定

スイッチのスタティック MAC アドレスを設定できます。 これらのアドレスは、インターフェイス コンフィギュレーション モード、または VLAN コンフィギュレーション モードで設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **mac-address-table static** *mac_address* **vlan** *vlan-id* {**drop** | **interface** {*type slot*/*port*} | **port-channel** *number*} [**auto-learn**]	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。 **auto-learn** オプションをイネーブルにすると、同じMACアドレスが別のポート上で見つかった場合には、スイッチがエントリを更新します。
ステップ 3	switch(config)# **no mac-address-table static** *mac_address* **vlan** *vlan-id*	（任意） 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、仮想インターフェイスにスタティックMACアドレスを割り当てます。

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 2/1
switch(config) #
```

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 コンフィギュレーション モード、または VLAN コンフィギュレーション モードで設定できます。

（注） Cisco Nexus 3000 スイッチがレイヤ 2 またはレイヤ 3 のターミネーション スイッチとして使用される場合は、すべての VLAN に対して **mac-address-table aging-time** を 1800（デフォルトの ARP エージング タイムの 1500 秒より長い値）に設定することを推奨します。

Cisco Nexus 3000 スイッチは、VLAN 単位の CAM エージング タイマーをサポートしていません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **mac-address-table aging-time** *seconds* [**vlan** *vlan_id*]	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。 *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。 VLAN を指定しなかった場合、エージングの指定がすべての VLAN に適用されます。

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
switch(config)# **clear mac-address-table dynamic** {**address** *mac-addr*} {**interface** [*type slot*/*port* | **port-channel** *number*} {**vlan** *vlan-id*}	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 アドレスの設定の確認

設定を確認するには、次のいずれかのコマンドを使用します。

表 *9*：*MAC* アドレスの設定の確認コマンド

コマンド	目的
switch# **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。
switch# **show mac-address-table**	MAC アドレス テーブルの内容を表示します。

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
```

第 12 章

IGMP スヌーピングの設定

この章は、次の内容で構成されています。

- IGMP スヌーピングの情報，133 ページ
- IGMP スヌーピング パラメータの設定，136 ページ
- IGMP スヌーピングの設定確認，140 ページ

IGMP スヌーピングの情報

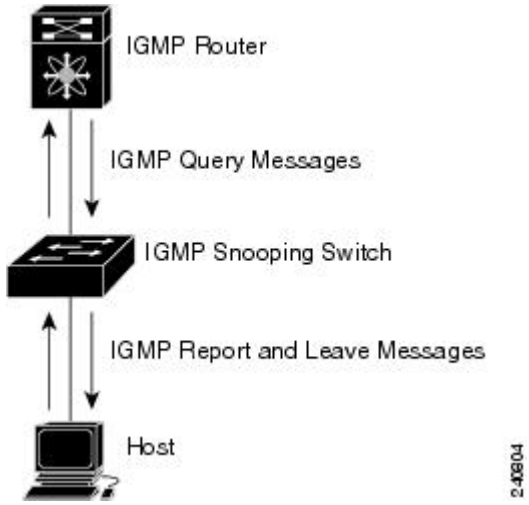
IGMP スヌーピング ソフトウェアは、VLAN 内の IGMP プロトコル メッセージを調べて、このトラフィックの受信に関連のあるホストまたはその他のデバイスに接続されているのはどのインターフェイスかを検出します。 IGMP スヌーピングは、インターフェイス情報を使用して、マルチアクセス LAN 環境での帯域幅消費を減らすことができ、これによって VLAN 全体のフラッディングを防ぎます。 IGMP スヌーピング機能は、どのポートがマルチキャスト対応ルータに接続されているかを追跡して、IGMP メンバーシップ レポートの転送管理を支援します。 トポロジの変更通知には、IGMP スヌーピング 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

（注） 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。 スヌーピング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 の転送決定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 クエリーとメンバーシップ 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。

図 *17*： *IGMP* スヌーピング スイッチ



（注） スイッチは、宛先マルチキャスト MAC アドレスのみに基づいて IGMPv3 スヌーピングをサポートしています。 送信元 MAC アドレスやプロキシ レポートに基づいてスヌーピングをサポートすることはありません。

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 フラッディング（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 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。

（注） 高速脱退機能をイネーブルにすると、残っているホストのチェックを行わないため、 Cisco NX-OS は、最後のメンバ クエリーの間隔の設定を無視します。

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。 この明示的な追跡機能は、高速脱退メカニズムをサポートしています。 すべての IGMPv3 ホストがメンバーシップ レポートを送信するため、レポート抑制機能によって、スイッチが他のマルチキャスト対応ルータに送信するトラフィックの量が制限されます。 レポート抑制をイネーブルにすると、過去にいずれの IGMPv1 ホストまたは IGMPv2 ホストからも対象のグループへの要求がなかった場合には、プロキシ レポートが作成されます。 プロキシ機能は、ダウンストリーム ホストからのメンバーシップ レポートからグループの状態を構築し、アップストリーム クエリアからのクエリーに応答してメンバーシップ レポートを生成します。

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。

IGMP 転送

Cisco Nexus 3000 シリーズ スイッチのコントロール プレーンは、IP アドレスを検出できますが、フォワーディングは MAC アドレスだけを使用して行われます。

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かにかかわらず、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。

ルータは定期的にマルチキャスト一般クエリーを送信し、スイッチはそれらのクエリーを VLAN 内のすべてのポート経由で転送します。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 MAC グループの情報を更新し、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、次の表で説明する、省略可能な IGMP スヌーピング パラメータを設定します。

表 *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。デフォルトはイネーブルです。 （注） 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、イネーブルかどうかに関係なくディセーブルと見なされます。
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 IGMPv3 メンバーシップ レポートを、VLAN別に追跡します。デフォルトはイネーブルです。

パラメータ	説明
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。 デフォルトはディセーブルです。
最終メンバのクエリー インターバル	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ー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。 デフォルトはディセーブルです。
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。 デフォルトはイネーブルです。
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な接続を設定します。 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。 仮想ポート チャネル（vPC）ピア リンクへのスタティック接続を設定します

パラメータ	説明
マルチキャスト ルータ vpc-peer-link	仮想ポートチャネル（vPC）ピア リンクへのスタティック接続を設定します。 デフォルトでは、vPC ピア リンクは、マルチキャストルータ ポートと見なされ、マルチキャスト パケットは、各レシーバ VLAN のピア リンクに送信されます。 孤立ポートを持つ各レシーバ VLAN に vPC ピア リンク上でマルチキャスト トラフィックを送信するには、**no ip igmp snooping mrouter vpc-peer-link** コマンドを使用します。 **no ip igmp snooping mrouter vpc-peer-link** コマンドを使用する場合、VLANに孤立ポートがない限り、マルチキャスト トラフィックは、送信元 VLAN とレシーバ VLAN のピア リンクに送信されません。 IGMP snooping mrouter vpc-peer-link もピア vPC スイッチでグローバルにディセーブルにする必要があります。 （注） Cisco NX-OS Release 5.0(3)N1(1) では、**no ip igmp snooping mrouter vpc-peer-link** コマンドは、Cisco Nexus 5000 シリーズ スイッチにデュアル ホーム接続する FEX があるトポロジではサポートされていません。
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にできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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。デフォルトはイネーブルです。

	コマンドまたはアクション	目的
		（注） 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、イネーブルかどうかに関係なくディセーブルと見なされます。
ステップ 3	switch(config)# **vlan configuration** *vlan-id*	VLAN コンフィギュレーション モードを開始します。
ステップ 4	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。 デフォルトはイネーブルです。 （注） 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。
ステップ 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 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。
ステップ 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。
ステップ 7	switch(config-vlan)# **ip igmp snooping last-member-query-interval** *seconds*	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、対応する 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。 デフォルトは 1 秒です。
ステップ 8	switch(config-vlan)# **ip igmp snooping querier** *IP-address*	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。 デフォルトはディセーブルです。
ステップ 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。 デフォルトはイネーブルです。

	コマンドまたはアクション	目的
ステップ 10	switch(config-vlan)# **ip igmp snooping mrouter interface** *interface*	マルチキャスト ルータへのスタティックな接続を設定します。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。
ステップ 11	switch(config-vlan)# **ip igmp snooping mrouter vpc-peer-link**	仮想ポート チャネル（vPC）ピア リンクへのスタティック接続を設定します。 デフォルトでは、vPC ピア リンクは、マルチキャスト ルータ ポートと見なされ、マルチキャスト パケットは、各レシーバ VLAN のピア リンクに送信されます。 孤立ポートを持つ各レシーバ VLAN に vPC ピア リンク上でマルチキャスト トラフィックを送信するには、**no ip igmp snooping mrouter vpc-peer-link** コマンドを使用します。 IGMP snooping mrouter vpc-peer-link もピア vPC スイッチでグローバルにディセーブルにする必要があります。
ステップ 12	switch(config-vlan)# **ip igmp snooping static-group** *group-ip-addr* [**source** *source-ip-addr*] **interface** *interface*	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。

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 スヌーピングの設定確認

IGMP スヌーピングの設定を確認するには、次のいずれかの作業を行います。

コマンド	説明
switch# **show ip igmp snooping** [[**vlan**] *vlan-id*]	IGMP スヌーピング設定を VLAN 別に表示します。

コマンド	説明
switch# **show ip igmp snooping groups** [[**vlan**] *vlan-id*] [**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。
switch# **show ip igmp snooping querier** [[**vlan**] *vlan-id*]	IGMP スヌーピング クエリアを VLAN 別に表示します。
switch# **show ip igmp snooping mrouter** [[**vlan**] *vlan-id*]	マルチキャスト ルータ ポートを VLAN 別に表示します。
switch# **show ip igmp snooping explicit-tracking vlan** *vlan-id*	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。

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: 172.16.24.1, version: 3
  Querier interval: 125 secs
  Querier last member query interval: 10 secs
  Querier robustness: 2
  Switch-querier enabled, address 172.16.24.1, 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
```

第 13 章

トラフィック ストーム制御の設定

この章は、次の内容で構成されています。

- トラフィック ストーム制御の概要，143 ページ
- トラフィック ストームに関する注意事項および制約事項，145 ページ
- トラフィック ストーム制御の設定，145 ページ
- トラフィック ストーム制御の設定例，147 ページ
- デフォルトのトラフィック ストームの設定，147 ページ

トラフィック ストーム制御の概要

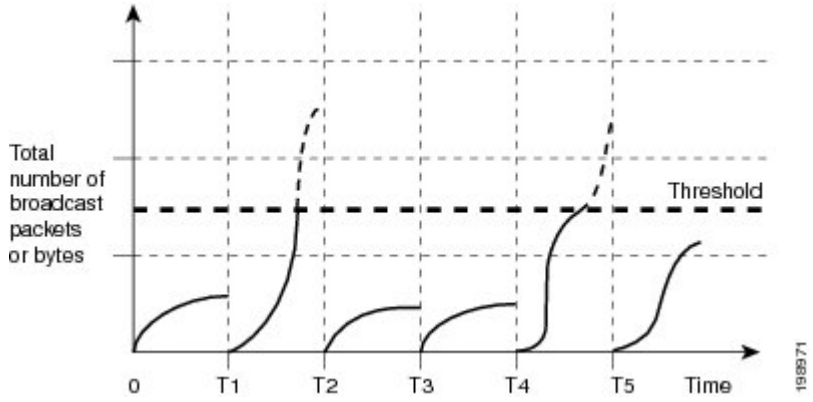
トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。 トラフィック ストーム制御機能を使用すると、ブロードキャスト ストーム、マルチキャスト ストーム、または未知のユニキャスト トラフィック ストームが原因の、イーサネット インターフェイス経由の通信の中断を防止できます。

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、マルチキャスト、ユニキャストの着信トラフィックのレベルを 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。

次の図は、指定された時間間隔中のイーサネット 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。

図 *18*：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パケット粒度で機能します。 たとえば、しきい値が高いほど、より多くのパケットを通過させることができます。

Cisco Nexus 3000 シリーズ スイッチのトラフィック ストーム制御は、ハードウェアで実装されています。 トラフィック ストーム制御回路は、イーサネット インターフェイスを通過してスイッチング バスに到着するパケットをモニタリングします。 また、パケットの宛先アドレスに設定されている Individual/Group ビットを使用して、パケットがユニキャストかブロードキャストかを判断し、10 マイクロ秒以内の間隔でパケット数を追跡します。パケット数がしきい値に到達したら、後続のパケットをすべて破棄します。

トラフィック ストーム制御では、トラフィック量の計測に帯域幅方式を使用します。制御対象のトラフィックが使用できる、利用可能な合計帯域幅に対するパーセンテージを設定します。 パケットは一定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。

デフォルトでは、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に関する注意事項および制約事項

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。

- 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ないようにするための、ローカル リンクと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。
- マルチキャスト ストーム制御設定は、リンクローカル宛先MACアドレス（01-00-5e-00-00-xx）のマルチキャスト データ パケットには適用されません。
- 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。

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。

（注） 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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {**ethernet** *slot*/*port* | **port-channel** *number*}	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **storm-control** {**broadcast** | **multicast** | **unicast**} **level** *percentage*[.*fraction*]	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。

次に、ユニキャスト トラフィック ストーム制御を Ethernet 1/4 に設定する例を示します。

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

トラフィック ストーム制御の設定の確認

トラフィック ストーム制御の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
switch# **show interface** [**ethernet** *slot*/*port* | **port-channel** *number*] **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。 （注） 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。
switch# **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 ストーム制御の設定例を示します。

```
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
switch(config-if)# storm-control unicast level 40
```

デフォルトのトラフィック ストームの設定

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を示します。

表 *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	ディセーブル
しきい値パーセンテージ	100

索 引

数字

802.1Q VLAN 41
　設定 41

B

BPDU ガード 109

C

CIST リージョナル ルート 82
CIST ルート 84

I

ICMPv2 134
IEEE 802.1w 79
IGMP 136
　スヌーピング パラメータ、設定 136
IGMPv1 134
IGMPv3 135
IGMP スヌーピング 135
　クエリー 135
IGMP 転送 135
　MAC アドレス 135

L

LAN インターフェイス 37
　イーサネット アクセス ポート 37
LLDP 127
　MIB 127

M

MAC アドレス 130
　スタティック、設定 130
設定、MAC アドレス 132
　確認 132
MAC アドレス リダクション 51
MAC テーブル 130
　エージング タイム、設定 130
MIB 127
　LLDP 127
MST 83, 92
　CIST リージョナル ルート 83
　デフォルト値への設定 92
MSTP 79, 80, 82, 83, 84, 85, 92
　CIST、説明 82
　CIST リージョナル ルート 82
　CIST ルート 84
　CST 82
　　定義 82
　　リージョン間の動作 82
　IEEE 802.1s 83
　　用語 83
　IST 82
　　リージョン内の動作 82
　MST リージョン 79, 80, 82, 84
　　CIST 82
　　サポートされるスパニングツリーインスタンス 80
　　説明 79
　　ホップ カウント メカニズム 84
　VLAN から MST インスタンスへのマッピング 92
　境界ポート 85
　　説明 85

P

PortFast BPDU フィルタリング 109

R

Rapid PVST+ 68
　設定 68
Rapid PVST+ の設定 77
　確認 77
Rapid PVST プライオリティ 74
RSTP 55, 59, 64, 79
　BPDU 64
　　処理 64
　アクティブ トポロジ 59
　高速コンバージェンス 55
　　ポイントツーポイント リンク 55
　　ルート ポート 55
　指定スイッチ、定義 59
　指定ポート、定義 59
　提案合意ハンドシェイク プロセス 55
　ルート ポート、定義 59

S

Store-and-Forward スイッチング 45, 46, 47
　イネーブル化 47
　注意事項および制約事項 46
　デフォルト設定 47
　に関する情報 45
Store-and-Forward モード 47, 48
　機能の履歴 48
　ライセンシング 47
STP 55, 61, 62, 107, 108
　PortFast 55, 108
　エッジ ポート 55, 108
　概要 61, 62
　　ディセーブル ステート 62
　　フォワーディング ステート 62
　　ブロッキング ステート 61
　　ラーニング ステート 62
　標準ポート 108
　ネットワーク ポート 108
　ポート タイプ 107
STP ブリッジ ID 51
STP ルート ガード 112
SVI 7, 14, 15
　VLAN インターフェイス 7
　管理 15
　ルーテッド 14

V

VLAN 7, 8, 12, 14, 15
　SVI 7
　拡張システム ID 8
　管理 SVI としての設定 15
　使用可能な VLAN 8
　設定 12
　説明 7
　ポートの追加 14
　予約範囲 8
　ルーテッド SVI としての設定 14
VLAN インターフェイス 7
　VLAN 間の通信 7
VLAN トラフィック 7
　配信 7
　ルーティング 7
VLAN の設定 18
　確認 18
VLAN の範囲 8
　説明 8
VLAN 番号 8
　許容数 8
　予約範囲 8
VTP 7, 16
　トランスペアレント モード 16
　モード 7

い

イネーブル化 47
　Store-and-Forward スイッチング 47

え

エージング タイム、設定 130
　MAC テーブル 130

か

拡張システム ID 8
　VLAN 8
確認 18, 77
　Rapid PVST+ の設定 77
　VLAN の設定 18

カットスルー スイッチング 45, 47, 48
イネーブル化 48
デフォルト設定 47
に関する情報 45
カットスルー モード 47, 48
機能の履歴 48
ライセンシング 47

き

機能の履歴 48
Store-and-Forward モード 48
カットスルー モード 48
スイッチング モード 48

こ

高速スパニングツリー プロトコル 79
コミュニティ VLAN 22, 23
コミュニティ ポート 23

さ

再イネーブル化 48
カットスルー スイッチング 48

し

新機能に関する情報 1
説明 1

す

スイッチング モード 47, 48
機能の履歴 48
ライセンシング 47
スタティック MAC アドレス、設定 130
スヌーピング パラメータ、設定 136
IGMP 136

せ

セカンダリ VLAN 22
設定 12
VLAN 12

ち

注意事項および制約事項 46
Store-and-Forward スイッチング 46

て

ディセーブル化 48
Store-and-Forward スイッチング 48
デフォルト設定 47
Store-and-Forward スイッチング 47
カットスルー スイッチング 47
スイッチング モード 47

と

独立 VLAN 22, 23
独立ポート 23
トラフィック ストーム 145
制御 145

ね

ネイティブ 802.1Q VLAN 41
設定 41

ふ

プライベート VLAN 22, 23, 26
エンド ステーションからのアクセス 26
コミュニティ VLAN 22, 23
セカンダリ VLAN 22
独立 VLAN 22, 23
プライマリ VLAN 22
ポート 23
コミュニティ 23
独立 23

プライベート VLAN *(続き)*
ポート *(続き)*
無差別 **23**
プライマリ VLAN **22**
ブリッジ ID **51**
ブロードキャスト ストーム **143**
ブロードキャスト トラフィック **7**
VLAN **7**
ブロッキング ステート、STP **61**

へ

変更された機能に関する情報 **1**
説明 **1**

ほ

ポート **14**
VLAN への追加 **14**
ホスト ポート **23**
種類 **23**

ま

マルチキャスト ストーム **143**
マルチキャスト トラフィック **7**
VLAN **7**

む

無差別ポート **23**

ゆ

ユニキャスト ストーム **143**

ら

ライセンシング **47**
Store-and-Forward モード **47**
カットスルー モード **47**
スイッチング モード **47**

り

リンク障害 **65, 85**
単方向の検出 **65, 85**

る

ルート ガード **112**

れ

レイヤ 2 スイッチング **3**
イーサネット スイッチング **3**