Cisco Nexus 5000 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 5.1(3)N1(1)

初版：2011 年 12 月 05 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-25842-01-J

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

目 次

はじめに

ここでは、次の項について説明します。

対象読者

このマニュアルは、Cisco Nexus シリーズ デバイスおよび Cisco Nexus 2000 シリーズ ファブリック エクステンダの設定や管理を行う経験豊富なネットワーク管理者を対象としたものです。

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。

関連資料

Cisco NX-OS 5000 シリーズのマニュアル セット一式は、次の URL で入手できます。
http://www.cisco.com/en/US/products/ps9670/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/ps9670/prod_release_notes_list.html

コンフィギュレーション ガイド

これらのガイドは、次の URL で入手できます。
http://www.cisco.com/en/US/products/ps9670/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。

- 『*Adapter-FEX Configuration Guide*』
- 『*Cisco Fabric Manager Configuration Guide*』
- 『*Cisco Nexus 5000 Series NX-OS Software Configuration Guide*』
- 『*Configuration Limits for Cisco NX-OS*』
- 『*FabricPath Configuration Guide*』
- 『*Fibre Channel over Ethernet Configuration Guide*』
- 『*Layer 2 Switching Configuration Guide*』
- 『*Multicast Routing Configuration Guide*』
- 『*Operations Guide*』
- 『*SAN Switching Configuration Guide*』
- 『*Quality of Service Configuration Guide*』
- 『*Security Configuration Guide*』
- 『*System Management Configuration Guide*』
- 『*Unicast Routing Configuration Guide*』

メンテナンスおよび操作ガイド

さまざまな機能に対応する『Cisco Nexus 5000 Series NX-OS Operations Guide』は、http://www.cisco.com/en/US/products/ps9670/prod_maintenance_guides_list.html で入手できます。

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

これらのガイドは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9670/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。

- 『*FabricPath Command Reference*』
- 『*Software Upgrade and Downgrade Guides*』
- 『*Regulatory Compliance and Safety Information*』

ライセンス ガイド

『*License and Copyright Information for Cisco NX-OS Software*』は、http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-ossw_lisns.html で入手できます。

コマンド リファレンス

これらのガイドは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9670/prod_command_reference_list.html

このカテゴリのマニュアルは次のとおりです。

- 『*Command Reference Master Index*』
- 『*Fabric Extender Command Reference*』
- 『*FabricPath Command Reference*』
- 『*Fibre Channel Command Reference*』
- 『*Fundamentals Command Reference*』
- 『*Layer 2 Interfaces Command Reference*』
- 『*Multicast Routing Command Reference*』
- 『*QoS Command Reference*』
- 『*Security Command Reference*』
- 『*System Management Command Reference*』
- 『*TrustSec Command Reference*』
- 『*Unicast Routing Command Reference*』
- 『*vPC Command Reference*』

テクニカル リファレンス

『*Cisco Nexus 5000 and Cisco Nexus 2000 MIBs Reference*』は、http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/mib/reference/NX5000_MIBRef.html で入手できます。

エラー メッセージおよびシステム メッセージ

『*Nexus 5000 Series NX-OS System Message Reference*』は、http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/system_messages/reference/sl_nxos_book.html で入手できます。

トラブルシューティング ガイド

『*Cisco Nexus 5000 Series Troubleshooting Guide*』は、http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/troubleshooting/guide/N5K_Troubleshooting_Guide.html で入手できます。

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

新機能および変更された機能に関する情報

この章の内容は、次のとおりです。

このリリースの新規情報および変更情報

次の表は、この最新リリースに関するマニュアルでの主な変更点の概要を示したものです。ただし、このリリースに関するコンフィギュレーション ガイドの変更点や新機能の中には一部、この表に記載されていないものもあります。

表 *1*：新機能

機能	説明	参照先
FEX ポートでの PVLAN	FEX ポートで PVLAN を設定することができます。	プライベート VLAN の設定，（57 ページ）

第 2 章

概要

この章の内容は、次のとおりです。

レイヤ 2 イーサネット スイッチングの概要

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

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。

イーサネット ネットワークではコリジョンによって深刻な輻輳が発生するため、全二重通信を使用することが有効な対処法の 1 つとなります。 一般的に、10/100 Mbps イーサネットは半二重モードで動作するので、各ステーションは送信または受信のどちらかしか実行できません。 これらのインターフェイスを全二重モードに設定すると、2 つのステーション間で同時に送受信を実行できます。 パケットを双方向へ同時に送ることができるので、有効なイーサネット帯域幅は 2 倍になります。 1/10 ギガビット イーサネットは、全二重モードだけで動作します。

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 に属する端末だけに転送またはフラッディングされます。 各 VLAN は 1 つの論理ネットワークであると見なされます。VLAN に属していないステーション宛てのパケットは、ブリッジまたはルータを経由して転送する必要があります。

デバイスの初回の起動時は、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） Cisco Nexus 5000 シリーズ用 NX-OS ソフトェアでは、スイッチ間リンク（ISL）トランキング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 規格のマルチ スパニングツリー（MST）では、複数の VLAN を単一のスパニングツリー インスタンスにマッピングできます。 各インスタンスは、独立したスパニングツリー トポロジで実行されます。

ソフトウェアは、従来の 802.1D システムで相互運用できますが、システムでは Rapid PVST+ および MST が実行されます。 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 5000 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 5000 シリーズ用 Cisco NX-OS では、拡張システム ID と MAC アドレス リダクションが使用されます。これらの機能をディセーブルにすることはできません。

また、シスコ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

イーサネット インターフェイスの設定

この章の内容は、次のとおりです。

イーサネット インターフェイスの概要

イーサネット ポートは、サーバまたは LAN に接続される標準のイーサネット インターフェイスとして機能します。

イーサネット インターフェイスでは、Fibre Channel over Ethernet（FCoE）もサポートされます。FCoE により、イーサネット トラフィックとファイバ チャネル トラフィックの両方を物理イーサネット リンクで伝送できるようになります。

Cisco Nexus 5000 シリーズ スイッチでは、イーサネット インターフェイスがデフォルトでイネーブルになっています。

interface コマンドについて

interface コマンドを使用すれば、イーサネット インターフェイスのさまざまな機能をインターフェイスごとにイネーブルにできます。 **interface** コマンドを入力する際には、次の情報を指定します。

- インターフェイス タイプ：物理イーサネット インターフェイスには、常にキーワード **ethernet** を使用します。
- スロット番号
  - スロット 1 にはすべての固定ポートが含まれます。

- スロット 2 には上位拡張モジュールのポートが含まれます（実装されている場合）。
- スロット 3 には下位拡張モジュールのポートが含まれます（実装されている場合）。

- ポート番号
  - グループ内でのポート番号です。

Cisco Nexus 2000 シリーズ ファブリック エクステンダとの使用をサポートするために、インターフェイスのナンバリング規則は、次のように拡張されています。

switch(config)# **interface ethernet** [*chassis*/]*slot*/*port*

- シャーシ ID は、接続されているファブリック エクステンダのポートのアドレスを指定するための任意のエントリです。 インターフェイス経由で検出されたファブリック エクステンダを識別するために、シャーシ ID はスイッチ上の物理イーサネットまたは EtherChannel インターフェイスに設定されます。 シャーシ ID の範囲は、100 ～ 199 です。

ユニファイド ポートについて

シスコは、Cisco NX-OS Release 5.0(3)N1(1b) で初めて、ユニファイド ポート テクノロジーを導入しました。 Cisco Nexus のユニファイド ポートを使用すると、Cisco Nexus 5500 プラットフォーム スイッチの物理ポートを 1/10 ギガビット イーサネット ポート、Fibre Channel over Ethernet（FCoE）ポート、ネイティブ 1 ギガビット ファイバ チャネル ポート、ネイティブ 2 ギガビット ファイバ チャネル ポート、ネイティブ 4 ギガビット ファイバ チャネル ポート、またはネイティブ 8 ギガビット ファイバ チャネル ポートとして設定することができます。

最近では、さまざまなタイプのネットワークに対応できるように 2 つのタイプのスイッチを備えたネットワークがほとんどです。 たとえば、イーサネット トラフィックを Catalyst スイッチまで伝送するための LAN スイッチと、FC トラフィックをサーバから MDS スイッチへ伝送するための SAN スイッチを備えたネットワークなどはその一例です。 ユニファイド ポート テクノロジーを使用すると、ユニファイド プラットフォーム、ユニファイド デバイス、およびユニファイド ワイヤの方式を導入することができます。 ユニファイド ポートでは、LAN ポート オプションや SAN ポート オプションを選択する既存の分離プラットフォーム方式から、単一のユニファイド ファブリックへ移行することができます。ユニファイド ファブリックは透過的であり、従来の運用方法や管理ソフトウェアにも対応しています。ユニファイドファブリックの構成要素は次のとおりです。

- ユニファイド プラットフォーム：同一のハードウェア プラットフォームおよび同一のソフトウェア コード レベルをまとめて、LAN 環境および SAN 環境に対応できるようにしたものです。
- ユニファイド デバイス：同一のプラットフォーム スイッチ上で LAN サービスおよび SAN サービスが実行されます。 ユニファイド デバイスでは、イーサネット ケーブルやファイバ チャネル ケーブルを同一のデバイスに接続することができます。
- ユニファイド ワイヤ：LAN ネットワークおよび SAN ネットワークをただ 1 つの統合ネットワーク アダプタ（CNA）で集約し、それらをサーバに接続します。

ユニファイド ファブリックでは、イーサネット機能や FCoE 機能を、既存の Cisco ツールとは独立に管理することができます。

新型の Cisco Nexus 5548UP スイッチおよび Cisco Nexus 5596UP スイッチには、ユニファイド ポート テクノロジーが搭載されています。 さらに新型のユニファイド ポート拡張モジュールおよび 2 つのレイヤ 3 モジュールを使用すれば、導入されたユニファイド ファブリックの優れた機能をさらに強化することができます。シスコの新しいユニファイドポートのスイッチおよびモジュールに関する詳細については、『Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes for Cisco NX-OS Release 5.0(3)N1(1b) and NX-OS Release 5.0(3)N1(1c)』および『Cisco Nexus 5000 Series Hardware Installation Guide』を参照してください。

単一方向リンク検出パラメータについて

シスコ独自の Unidirectional Link Detection（UDLD; 単一方向リンク検出）プロトコルでは、光ファイバまたは銅線（たとえば、カテゴリ 5 のケーブル）のイーサネット ケーブルで接続されているポートでケーブルの物理的な構成をモニタリングし、単一方向リンクの存在を検出できます。 スイッチが単方向リンクを検出すると、UDLD は関連する LAN ポートをシャットダウンし、ユーザに警告します。 単方向リンクは、スパニングツリー トポロジ ループをはじめ、さまざまな問題を引き起こす可能性があります。

UDLD は、レイヤ 1 プロトコルと協調してリンクの物理ステータスを検出するレイヤ 2 プロトコルです。 レイヤ 1 では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。 UDLD は、ネイバーの ID の検知、誤って接続された LAN ポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。 自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 とレイヤ 2 の検出が協調して動作して、物理的な単一方向接続と論理的な単一方向接続を防止し、その他のプロトコルの異常動作を防止できます。

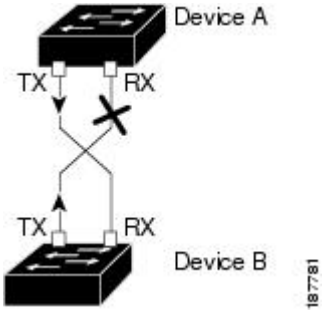
リンク上でローカル デバイスから送信されたトラフィックはネイバーで受信されるのに対し、ネイバーから送信されたトラフィックはローカル デバイスで受信されない場合には常に、単方向リンクが発生します。 対になったファイバケーブルのうち一方の接続が切断された場合、自動ネゴシエーションがアクティブである限り、そのリンクはアップ状態が維持されなくなります。 この場合、論理リンクは不定であり、UDLD は何の処理も行いません。 レイヤ 1 で両方の光ファイバが正常に動作している場合は、レイヤ 2 で UDLD が、これらの光ファイルが正しく接続されているかどうか、および正しいネイバー間でトラフィックが双方向に流れているかを調べます。 自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは、自動ネゴシエーションでは実行できません。

Cisco Nexus 5000 シリーズ スイッチは、UDLD をイネーブルにした LAN ポート上のネイバー デバイスに UDLD フレームを定期的に送信します。 一定の時間内にフレームがエコー バックされてきて、特定の確認応答（echo）が見つからなければ、そのリンクは単一方向のフラグが立てられ、その LAN ポートはシャットダウンされます。 UDLD プロトコルにより単方向リンクが正しく識別されその使用が禁止されるようにするためには、リンクの両端のデバイスで UDLD がサポートされている必要があります。

（注） UDLD は、銅線の LAN ポート上では、このタイプのメディアでの不要な制御トラフィックの送信を避けるために、ローカルでデフォルトでディセーブルになっています。

次の図は、単方向リンクが発生した状態の一例を示したものです。 デバイス B はこのポートでデバイス A からのトラフィックを正常に受信していますが、デバイス A は同じポート上でデバイス B からのトラフィックを受信していません。 UDLD によって問題が検出され、ポートがディセーブルになります。

図 *1*：単方向リンク



UDLD のデフォルト設定

次の表は、UDLD のデフォルト設定を示したものです。

表 *2*：*UDLD* のデフォルト設定

機能	デフォルト値
UDLD グローバル イネーブル ステート	グローバルにディセーブル
UDLD アグレッシブ モード	ディセーブル
ポート別の UDLD イネーブル ステート（光ファイバ メディア用）	すべてのイーサネット光ファイバ LAN ポートでイネーブル
ポート別の UDLD イネーブル ステート（ツイストペア（銅製）メディア用）	すべてのイーサネット 10/100 および 1000BASE-TX LAN ポートでディセーブル

UDLD アグレッシブ モードと非アグレッシブ モード

UDLD アグレッシブ モードはデフォルトではディセーブルに設定されています。 UDLD アグレッシブ モードは、UDLD アグレッシブ モードをサポートするネットワーク デバイスの間のポイントツーポイントのリンク上に限って設定できます。 UDLD アグレッシブ モードがイネーブルに

なっている場合、UDLD ネイバー関係が確立されている双方向リンク上のポートが UDLD フレームを受信しなくなったとき、UDLD はネイバーとの接続の再確立を試行します。 この試行に 8 回失敗すると、ポートはディセーブルになります。

スパニングツリー ループを防止するため、間隔がデフォルトの 15 秒である非アグレッシブな UDLD でも、（デフォルトのスパニングツリー パラメータを使用して）ブロッキング ポートがフォワーディング ステートに移行する前に、単方向リンクをシャットダウンすることができます。

UDLD アグレッシブ モードをイネーブルにすると、次のようなことが発生します。

- リンクの一方にポート スタックが生じる（送受信どちらも）
- リンクの一方がダウンしているにもかかわらず、リンクのもう一方がアップしたままになる

このような場合、UDLD アグレッシブ モードでは、リンクのポートの 1 つがディセーブルになり、トラフィックが廃棄されるのを防止します。

インターフェイスの速度について

Cisco Nexus 5000 シリーズ スイッチには、固定 10 ギガビット ポートが多数あり、それぞれが SFP+ インターフェイス アダプタを備えています。 Cisco Nexus 5010 スイッチには 20 個の固定ポートが装備されており、そのうち、最初の 8 個がスイッチ可能な 1 ギガビットおよび 10 ギガビットのポートです。 Cisco Nexus 5020 スイッチには 40 個の固定ポートが装備されており、そのうち、最初の 16 個がスイッチ可能な 1 ギガビットおよび 10 ギガビットのポートです。

Cisco Discovery Protocol について

Cisco Discovery Protocol（CDP）は、すべてのシスコ デバイス（ルータ、ブリッジ、アクセス サーバ、およびスイッチ）のレイヤ 2（データリンク層）で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションはCDP を使用することにより、既知のデバイスのネイバーであるシスコ デバイスを検出することができます。 また、下位レイヤのトランスペアレント プロトコルが稼働しているネイバーデバイスのデバイス タイプや、簡易ネットワーク管理プロトコル（SNMP）エージェント アドレスを学習することもできます。 この機能によって、アプリケーションからネイバー デバイスに SNMP クエリーを送信できます。

CDP は、Subnetwork Access Protocol（SNAP; サブネットワーク アクセス プロトコル）をサポートしているすべてのメディアで動作します。 CDP はデータリンク層でのみ動作するため、異なるネットワーク層プロトコルをサポートする 2 つのシステムで互いの情報を学習できます。

CDP が設定された各デバイスはマルチキャスト アドレスに定期的にメッセージを送信して、SNMP メッセージを受信可能なアドレスを 1 つまたは複数アドバタイズします。 このアドバタイズには、受信側デバイスでCDP 情報を廃棄せずに保持する時間を表す存続可能時間、つまりホールドタイム情報も含まれます。 各デバイスは他のデバイスから送信されたメッセージも待ち受けて、ネイバー デバイスについて学習します。

このスイッチは、CDP バージョン 1 とバージョン 2 の両方をサポートします。

CDP のデフォルト設定

次の表は、CDP のデフォルト設定を示したものです。

表 *3*：*CDP* のデフォルト設定

機能	デフォルト設定
CDP インターフェイス ステート	イネーブル
CDP タイマー（パケット更新頻度）	60 秒
CDP ホールドタイム（廃棄までの時間）	180 秒
CDP バージョン 2 アドバタイズ	イネーブル

errdisable ステートの設定

インターフェイスが管理上は（**no shutdown** コマンドを使用して）イネーブルになっていながら、実行時にプロセスによってディセーブルになっている場合、そのインターフェイスは errdisable ステートであると言います。 たとえば、UDLD が単方向リンクを検出した場合、そのインターフェイスは実行時にシャットダウンされます。 ただし、そのインターフェイスは管理上イネーブルであるため、そのステータスは errdisable として表示されます。 いったん errdisable ステートになったインターフェイスは、手動でイネーブルにする必要があります。ただし、自動回復までのタイムアウト値を設定することもできます。errdisable 検出はすべての原因に対してデフォルトでイネーブルです。自動回復はデフォルトでは設定されていません。

インターフェイスが errdisable ステートになった場合は、**errdisable detect cause** コマンドを使用して、そのエラーに関する情報を取得してください。

errdisable の特定の原因に対する errdisable 自動回復タイムアウトを設定する場合は、time 変数の値を変更します。

errdisable recovery cause コマンドを使用すると、300 秒後に自動回復します。 回復までの時間を変更する場合は、**errdisable recovery interval** コマンドを使用して、タイムアウト時間を指定します。 指定できる値は 30 ～ 65535 秒です。

原因に対する errdisable 回復をイネーブルにしない場合、そのインターフェイスは **shutdown** コマンドおよび **no shutdown** コマンドが入力されるまで errdisable ステートのままです。 原因に対して回復をイネーブルにすると、そのインターフェイスの errdisable ステートは解消され、すべての原因がタイムアウトになった段階で動作を再試行できるようになります。 エラーの原因を表示する場合は、**show interface status err-disabled** コマンドを使用します。

ポート プロファイルについて

さまざまなインターフェイス コマンドを含むポートプロファイルを作成し、そのポートプロファイルを Cisco Nexus 5000 シリーズ スイッチのインターフェイス（複数可）に適用することができます。 ポート プロファイルは、次のようなタイプのインターフェイスに適用できます。

- イーサネット
- VLAN ネットワーク インターフェイス
- ポート チャネル

ポートプロファイルに含まれるコマンドは、ポートプロファイル外部でも設定することができます。 ポート プロファイルの新しい設定と、ポート プロファイル外部の既存の設定が競合する場合は、ポート プロファイル内のコマンドよりも、インターフェイスに対して設定端末モードで設定されたコマンドの方が優先されます。 ポートプロファイルの適用後に変更したインターフェイス設定が、そのポート プロファイルの設定と競合した場合は、インターフェイス設定が優先されます。

単独のインターフェイスまたはある範囲に属する複数のインターフェイスに適用されているポートプロファイルは継承することができます。ポートプロファイルを単独のインターフェイスまたはある範囲に属する複数のインターフェイスに適用した場合も、ポート プロファイルを継承した場合も、スイッチではそのポート プロファイル内のすべてのコマンドがインターフェイスに適用されます。

ポートプロファイルには、別のポートプロファイルの設定を継承することができます。別のポートプロファイルを継承した場合、最初のポート プロファイルでは、それを継承した第 2 のポート プロファイルに含まれるすべてのコマンドは、最初のポート プロファイルとは競合していないものと見なされます。 4 つのレベルの継承がサポートされています。 任意の数のポート プロファイルで同じポート プロファイルを継承できます。

ポートプロファイル設定をインターフェイスに適用するには、そのポートプロファイルをイネーブルにする必要があります。 ポート プロファイルをイネーブルにする前に、インターフェイス（複数可）に対してそのポート プロファイルを設定および継承することができます。そのうえでポート プロファイルをイネーブルにすると、指定したインターフェイスにその設定内容が反映されます。

ポート プロファイルをインターフェイス（複数可）から削除する場合は、スイッチでは最初にインターフェイスの設定が無効にされ、その後でポート プロファイルのリンクそのものが削除されます。また、ポートプロファイルを削除すると、スイッチではインターフェイス設定の確認が行われた後、直接入力されたインターフェイス コマンドにより無効になったポート プロファイル コマンドがスキップされるか、またはそれらのコマンドがデフォルト値に戻されます。

他のポート プロファイルにより継承されたポート プロファイルを削除する場合は、そのポート プロファイルを削除する前に継承を無効にする必要があります。

また、ポート プロファイルを元々適用していたインターフェイスのグループの中から、そのプロファイルを削除するインターフェイスを選択することもできます。 たとえば、1 つのポート プロファイルを設定した後、10 個のインターフェイスに対してそのポートプロファイルを継承するよ

う設定した場合、その 10 個のうちいくつかのインターフェイスからのみポート プロファイルを削除することができます。 ポートプロファイルは、適用されている残りのインターフェイスで引き続き動作します。

インターフェイス コンフィギュレーション モードを使用して指定したインターフェイスの範囲の特定のコンフィギュレーションを削除する場合、そのコンフィギュレーションもそのインターフェイスの範囲のポート プロファイルからのみ削除されます。 たとえば、ポート プロファイル内にチャネル グループがあり、インターフェイス コンフィギュレーション モードでそのポート チャネルを削除する場合、指定したポートチャネルも同様にポートプロファイルから削除されます。

単独のインターフェイスまたはある範囲に属する複数のインターフェイスに対してポート プロファイルを継承した後、特定の設定値を削除すると、それらのインターフェイスではそのポートプロファイル設定が機能しなくなります。

ポート プロファイルを誤ったタイプのインターフェイスに適用しようとすると、エラーが返されます。

ポート プロファイルをイネーブル化、継承、または変更しようとすると、スイッチによりチェックポイントが作成されます。 ポートプロファイル設定が正常に実行されなかった場合は、その前の設定までロールバックされ、エラーが返されます。 ポートプロファイルは部分的にだけ適用されることはありません。

ポート プロファイルに関する注意事項と制約事項

ポート プロファイルの設定に関する注意事項および制約事項は次のとおりです。

- 各ポートプロファイルは、インターフェイスのタイプにかかわらず、ネットワーク上で一意の名前を持つ必要があります。
- 競合が発生した場合は、インターフェイス モードで入力したコマンドがポート プロファイルのコマンドに優先します。 しかし、ポートプロファイルはそのコマンドをポートプロファイルに保持します。
- ポートプロファイルのコマンドに対してインターフェイスのデフォルトのコマンドを明示的に優先させない限り、ポート プロファイルのコマンドがデフォルトのコマンドに優先します。
- ポート プロフィルをインターフェイスまたはインターフェイスの範囲に継承した後、インターフェイス コンフィギュレーション レベルで新しい値を入力して、個々の設定値を上書きできます。 インターフェイス コンフィギュレーション レベルで個々の設定値を削除すると、インターフェイスではポート プロファイル内の値が再度使用されます。
- ポート プロファイルに関連したデフォルト設定はありません。
- ポート プロファイル コンフィギュレーション モードでは、指定したインターフェイス タイプに応じて、特定のグループのコマンドを使用することができます。
- Session Manager にポート プロファイルは使用できません。

デバウンス タイマー パラメータについて

ポート デバウンス時間は、リンクがダウンしたことをスーパーバイザに通知するためにインターフェイスが待機する時間です。 この時間、インターフェイスはリンクがアップ状態に戻ったかどうかを確認するために待機します。 待機時間は、トラフィックが停止している時間です。

デバウンス タイマーは各インターフェイスに対してイネーブルにでき、ミリ秒単位で遅延時間を指定できます。

注意 ポート デバウンス タイマーをイネーブルにすると、リンク アップ検出とリンク ダウン検出に遅延が発生するため、デバウンス期間中にトラフィックが一部損失します。 トラフィックが損失することにより、一部のプロトコルの収束および再収束に影響を及ぼす場合があります。

MTU 設定について

Cisco Nexus 5000 シリーズスイッチでは、フレームのフラグメント化は行われません。 そのためスイッチでは、同じレイヤ 2 ドメイン内の 2 つのポートに別々の最大伝送単位（MTU）を設定することはできません。 物理イーサネット インターフェイス別 MTU はサポートされていません。 代わりに、MTU は QoS クラスに従って設定されます。 MTU を変更する場合は、クラス マップおよびポリシー マップを設定します。

（注） インターフェイス設定を表示すると、物理イーサネット インターフェイスのデフォルト MTU は 1500 と表示され、ファイバ チャネル インターフェイスの受信データ フィールド サイズは 2112 と表示されます。

イーサネット インターフェイスの設定

ここでは、次の内容について説明します。

Cisco Nexus 5500 プラットフォーム スイッチにおけるレイヤ 3 インターフェイスの設定

NX-OS Release 5.0(3)N1(1) 以降、Cisco Nexus 5000 プラットフォーム スイッチではレイヤ 3 インターフェイスの設定を行えるようになりました。

レイヤ 3 インターフェイスをレイヤ 2 インターフェイスに変更するには、**switchport** コマンドを使用します。 レイヤ 2 インターフェイスをレイヤ 3 インターフェイスに変更する場合は、**no switchport** コマンドを使用します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet** *slot*/*port*
3. switch(config-if)# **no switchport**
4. switch(config-if)# **no shutdown**

手順の詳細

	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*	指定されたインターフェイスのコンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **no switchport**	レイヤ 3 インターフェイスを選択します。
ステップ 4	switch(config-if)# **no shutdown**	インターフェイスを再起動します。

次の例は、レイヤ 3 インターフェイスの設定方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# no shutdown
```

ユニファイド ポートの設定

Cisco N55-M16UP 拡張モジュールがインストールされた Cisco Nexus 5548UP スイッチ、Cisco Nexus 5596UP スイッチ、および Cisco Nexus 5548P スイッチでは、ユニファイド ポートを設定することができます。

ユニファイド ポートでは、ポートをイーサネット ポート、ネイティブ ファイバ チャネル ポート、または Fibre Channel over Ethernet（FCoE）ポートとして設定することが可能です。 デフォルトはイーサネット ポートですが、次のユニファイド ポートではポート モードをネイティブ ファイバ チャネルに変更することができます。

- Cisco Nexus 5548UP スイッチまたは Cisco Nexus 5596UP スイッチの任意のポート。
- Cisco Nexus 5548P スイッチにインストールされた Cisco N55-M16UP 拡張モジュールのポート。

（注） イーサネット ポートおよびファイバ チャネル ポートは、指定された順序で設定する必要があります。

- ファイバ チャネル ポートは、モジュールの最後のポートから設定する必要があります。
- イーサネット ポートは、モジュールの先頭のポートから設定する必要があります。

この順序に従って設定が行われていない場合は、次のようなエラーが表示されます。

```
ERROR: Ethernet range starts from first port of the module
ERROR: FC range should end on last port of the module
```

Cisco Nexus 5548UP スイッチでは、メイン スロット（slot1）の 32 ポートがユニファイド ポートとなります。 イーサネット ポートは、ポート 1/1 から始めてポート 1/32 まで順に設定されます。 ファイバ チャネル ポートは、ポート 1/32 から始めてポート 1/1 まで順に設定されます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **slot** *slot number*
3. switch(config-slot)# **port** *port number* **type** {**ethernet** | **fc**}
4. switch(config-slot)# **copy running-config startup-config**
5. switch(config-slot)# **reload**
6. switch(config)# **no port** *port number* **type fc**

手順の詳細

	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)# **slot** *slot number*	スイッチ上のスロットを指定します。
ステップ 3	switch(config-slot)# **port** *port number* **type** {**ethernet** | **fc**}	ユニファイド ポートをネイティブ ファイバ チャネル ポートおよびイーサネット ポートとして設定します。 • type：シャーシのスロット上で設定するポートのタイプを指定します。 • ethernet：イーサネット ポートを指定します。 • fc：ファイバ チャネル（FC）ポートを指定します。 （注） 変更内容を有効にするためには、スイッチをリブートする必要があります。

	コマンドまたはアクション	目的
ステップ 4	switch(config-slot)# **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。
ステップ 5	switch(config-slot)# **reload**	スイッチをリブートします。
ステップ 6	switch(config)# **no port** *port number* **type fc**	ユニファイド ポートを削除します。

次の例は、Cisco Nexus 5548UP スイッチまたは Cisco Nexus 5596UP スイッチでユニファイド ポートを設定する方法を示したものです。

```
switch# configure terminal
switch(config)# slot 1
switch(config-slot)# port 32 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

次の例は、Cisco N55-M16UP 拡張モジュールでユニファイド ポートを設定する方法を示したものです。

```
switch# configure terminal
switch(config)# slot 2
switch(config-slot)# port 32 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

次の例は、20 個のポートをイーサネット ポートとして設定し、12 個のポートを FC ポートとして設定する方法を示したものです。

```
switch# configure terminal
switch(config)# slot 1
switch(config-slot)# port 21-32 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

UDLD モードの設定

Unidirectional Link Detection（UDLD; 単一方向リンク検出）を実行するように設定されているデバイス上のイーサネット インターフェイスには、ノーマル モードまたはアグレッシブ モードの UDLD を設定できます。 インターフェイスの UDLD モードをイネーブルにするには、そのインターフェイスを含むデバイス上で UDLD を事前にイネーブルにしておく必要があります。 UDLD は他方のリンク先のインターフェイスおよびそのデバイスでもイネーブルになっている必要があります。

ノーマル UDLD モードを使用するには、ポートの 1 つをノーマル モードに設定し、他方のポートをノーマル モードまたはアグレッシブ モードに設定する必要があります。 アグレッシブ UDLD モードを使用するには、両方のポートをアグレッシブ モードに設定する必要があります。

（注） 設定前に、リンクされている他方のポートとそのデバイスの UDLD をイネーブルにしておかなければなりません。

UDLD モードを設定する手順は、次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature udld**
3. switch(config)# **no feature udld**
4. switch(config)# **show udld global**
5. switch(config)# **interface** *type slot*/*port*
6. switch(config-if)# **udld** {**enable** | **disable** | **aggressive**}
7. switch(config-if)# **show udld** *interface*

手順の詳細

	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 udld**	デバイスの UDLD をイネーブルにします。
ステップ 3	switch(config)# **no feature udld**	デバイスの UDLD をディセーブルにします。
ステップ 4	switch(config)# **show udld global**	デバイスの UDLD ステータスを表示します。
ステップ 5	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 6	switch(config-if)# **udld** {**enable** | **disable** | **aggressive**}	ノーマル UDLD モードをイネーブルにするか、UDLD をディセーブルにするか、またはアグレッシブ UDLD モードをイネーブルにします。
ステップ 7	switch(config-if)# **show udld** *interface*	インターフェイスの UDLD ステータスを表示します。

次の例は、スイッチの UDLD をイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# feature udld
```

次の例は、イーサネット ポートのノーマル UDLD モードをイネーブルにする方法を示しています。

```
switch# configure terminal
```

```
switch(config)# interface ethernet 1/4
switch(config-if)# udld enable
```

次の例は、イーサネット ポートのアグレッシブ UDLD モードをイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# udld aggressive
```

次の例は、イーサネット ポートの UDLD をディセーブルにする例を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# udld disable
```

次の例は、スイッチの UDLD をディセーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# no feature udld
```

インターフェイスの速度の設定

Cisco Nexus 5010 スイッチの最初の 8 個のポートと、Cisco Nexus 5020 スイッチの最初の 16 個のポートはスイッチ可能な 1 ギガビット ポートと 10 ギガビット ポートです。 デフォルトのインターフェイス速度は 10 ギガビットです。 これらのポートを 1 ギガビット イーサネットに設定するには、1 ギガビット イーサネット SFP トランシーバを該当するポートに挿入してから、その速度を **speed** コマンドで設定します。

手順の概要

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

手順の詳細

	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*	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。 このインターフェイスに、1 ギガビット イーサネット SFP トランシーバが挿入されている必要があります。
ステップ 3	switch(config-if)# **speed** *speed*	インターフェイスの速度を設定します。 このコマンドは、物理的なイーサネット インターフェイスにしか適用できません。 *speed* 引数には次のいずれかを設定できます。 • 10 Mbps

	コマンドまたはアクション	目的
		• 100 Mbps • 1 Gbps • 10 Gbps • automatic

次に、1 ギガビット イーサネット ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# speed 1000
```

（注） インターフェイスとトランシーバの速度が一致しない場合に **show interface ethernet** *slot*/*port* コマンドを入力すると、SFP 検証失敗メッセージが表示されます。 たとえば、speed 1000 コマンドを設定しないで 1 ギガビット SFP トランシーバをポートに挿入すると、このエラーが発生します。 デフォルトでは、すべてのポートが 10 ギガビットです。

リンク ネゴシエーションのディセーブル化

no negotiate auto コマンドを使用することにより、リンク ネゴシエーションをディセーブルにすることができます。 デフォルトの場合、自動ネゴシエーションは 1 ギガビット ポートではイネーブル、10 ギガビット ポートではディセーブルです。

このコマンドの機能は、IOS の **speed non-negotiate** コマンドと同等です。

（注） 10 ギガビット ポートで自動ネゴシエーションをイネーブルにすることは推奨されません。 10 ギガビット ポートで自動ネゴシエーションをイネーブルにすると、リンクがダウンします。 デフォルトの場合、リンク ネゴシエーションは 10 ギガビット ポートではディセーブルです。

手順の概要

1. switch# configure terminal
2. switch(config)# interface ethernet slot/port
3. switch(config-if)# no negotiate auto
4. （任意） switch(config-if)# negotiate auto

手順の詳細

	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	インターフェイスを選択し、インターフェイス モードを開始します。
ステップ 3	switch(config-if)# no negotiate auto	選択したイーサネット インターフェイス（1 ギガビット ポート）に対してリンク ネゴシエーションをディセーブルにします。
ステップ 4	switch(config-if)# negotiate auto	（任意） 選択したイーサネット インターフェイスに対してリンク ネゴシエーションをイネーブルにします。1 ギガビット ポートに対してはデフォルトでイネーブルです。

次の例は、指定したイーサネット インターフェイス（1 ギガビット ポート）に対して自動ネゴシエーションをディセーブルにする方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no negotiate auto
switch(config-if)#
```

次の例は、指定したイーサネット インターフェイス（1 ギガビット ポート）に対して自動ネゴシエーションをイネーブルにする方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# negotiate auto
switch(config-if)#
```

CDP の特性の設定

Cisco Discovery Protocol（CDP）更新の頻度、情報を廃棄するまでの保持期間、およびバージョン 2 アドバタイズを送信するかどうかを設定することができます。

インターフェイスの CDP 特性を設定する手順は、次のとおりです。

手順の概要

1. switch# **configure terminal**
2. （任意） switch(config)# [**no**] **cdp advertise** {**v1** | **v2** }
3. （任意） switch(config)# [**no**] **cdp format device-id** {**mac-address** | **serial-number** | **system-name**}
4. （任意） switch(config)# [**no**] **cdp holdtime** *seconds*
5. （任意） switch(config)# [**no**] **cdp timer** *seconds*

手順の詳細

	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**] **cdp advertise** {**v1** | **v2** }	（任意） 使用するバージョンを設定して、CDP アドバタイズメントを送信します。 バージョン 2 がデフォルト ステートです。 デフォルト設定に戻す場合は、このコマンドの **no** 形式を使用します。
ステップ 3	switch(config)# [**no**] **cdp format device-id** {**mac-address** | **serial-number** | **system-name**}	（任意） CDP デバイス ID の形式を設定します。 デフォルトはシステム名です。完全修飾ドメイン名で表すことができます。 デフォルト設定に戻す場合は、このコマンドの **no** 形式を使用します。
ステップ 4	switch(config)# [**no**] **cdp holdtime** *seconds*	（任意） デバイスから送信された情報が受信デバイスで破棄されるまでの保持時間を指定します。 指定できる範囲は 10 ～ 255 秒です。デフォルトは 180 秒です。 デフォルト設定に戻す場合は、このコマンドの **no** 形式を使用します。
ステップ 5	switch(config)# [**no**] **cdp timer** *seconds*	（任意） CDP アップデートの送信頻度を秒単位で設定します。 指定できる範囲は 5 ～ 254 です。デフォルトは 60 秒です。 デフォルト設定に戻す場合は、このコマンドの **no** 形式を使用します。

次の例は、CDP 特性を設定する方法を示しています。

```
switch# configure terminal
switch(config)# cdp timer 50
switch(config)# cdp holdtime 120
switch(config)# cdp advertise v2
```

CDP のイネーブル化/ディセーブル化

CDP をイーサネット インターフェイスに対してイネーブルにしたり、ディセーブルにしたりできます。 このプロトコルは、同一リンクの両方のインターフェイスでイネーブルになっている場合にだけ機能します。

インターフェイスに対してCDPをイネーブルにしたりディセーブルにしたりする手順は、次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port*
3. switch(config-if)# **cdp enable**
4. switch(config-if)# **no cdp enable**

手順の詳細

	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*	指定したインターフェイスに対してインターフェイス 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)# **cdp enable**	インターフェイスに対して CDP をイネーブルにします。 正常に機能するには、このパラメータが同一リンク上の両方のインターフェイスでイネーブルになっている必要があります。
ステップ 4	switch(config-if)# **no cdp enable**	インターフェイスに対して CDP をディセーブルにします。

次に、イーサネット ポートに対して CDP 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)# cdp enable
```

このコマンドは、物理的なイーサネット インターフェイスにしか適用できません。

errdisable ステート検出のイネーブル化

アプリケーションでのerrdisableステート検出をイネーブルにすることができます。 これにより、インターフェイスで原因が検出されると、そのインターフェイスはerrdisableステートになります。このerrdisableステートは、リンクダウン ステートに類似した動作ステートです。

手順の概要

1. **config t**
2. **errdisable detect cause** {*all* | *link-flap* | *loopback*}
3. **shutdown**
4. **no shutdown**
5. **show interface status err-disabled**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**errdisable detect cause** {*all* | *link-flap* | *loopback*}
	
	例：
	`switch(config)# errdisable detect cause all`
	`switch(config)#`
		インターフェイスを errdisable ステートにする条件を指定します。 デフォルトではイネーブルになっています。

ステップ 3	**shutdown**
	
	例：
	`switch(config)# shutdown`
	`switch(config)#`
		インターフェイスを管理的にダウンさせます。 インターフェイスを errdisable ステートから手動で回復させる場合は、このコマンドを最初に入力します。

ステップ 4	**no shutdown**
	
	例：
	`switch(config)# no shutdown`
	`switch(config)#`
		インターフェイスを管理的にアップし、errdisable ステートから手動で回復できるようにします。

ステップ 5	**show interface status err-disabled** 例： `switch(config)# show interface status err-disabled`	errdisable ステートにあるインターフェイスについての情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、いずれの場合にもerrdisableステート検出をイネーブルにする方法を示したものです。

```
switch(config)#errdisable detect cause all
switch(config)#
```

errdisable ステート回復のイネーブル化

インターフェイスがerrdisableステートから回復して再びアップ状態になるようにアプリケーションを設定することができます。 回復タイマーを設定しない限り、300 秒後にリトライします（**errdisable recovery interval** コマンドを参照）。

手順の概要

1. **config t**
2. **errdisable recovery cause** {*all* | *udld* | *bpduguard* | *link-flap* | *failed-port-state* | *pause-rate-limit*}
3. **show interface status err-disabled**
4. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**errdisable recovery cause** {*all* | *udld* | *bpduguard* | *link-flap* | *failed-port-state* | *pause-rate-limit*}
	
	例：
	`switch(config)#errdisable recovery cause all`
	`switch(config-if)#`
		インターフェイスが errdisable ステートから自動的に回復し、デバイスがそのインターフェイスを再びアップ状態にする条件を指定します。デバイスは300秒待機してからリトライします。デフォルトではディセーブルになっています。

ステップ 3	**show interface status err-disabled** 例： `switch(config)#show interface status err-disabled`	errdisableステートにあるインターフェイスについての情報を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)#copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、いずれの条件に対しても errdisable ステート回復をイネーブルにする方法を示したものです。

```
switch(config)#errdisable recovery cause all
switch(config)#
```

errdisable ステート回復間隔の設定

下記の手順により、errdisable ステート回復のタイマー値を設定することができます。 有効な範囲は 30 ～ 65535 秒です。 デフォルト値は 300 秒です。

手順の概要

1. **config t**
2. **errdisable recovery interval** *interval*
3. **show interface status err-disabled**
4. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**errdisable recovery interval** *interval*
	
	例：
	`switch(config)#errdisable recovery interval 32`
	`switch(config-if)#`
		インターフェイスが errdisable ステートから回復する間隔を指定します。 有効な範囲は 30 ～ 65535 秒です。 デフォルト値は 300 秒です。

ステップ 3	**show interface status err-disabled** 例： `switch(config)#show interface status err-disabled`	errdisable ステートにあるインターフェイスについての情報を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)#copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次の例は、いずれの条件の下でも errdisable ステート回復をイネーブルにする方法を示したものです。

```
switch(config)#errdisable recovery cause all
switch(config)#
```

ポート プロファイル

ポート プロファイルの作成

スイッチでポートプロファイルを作成することができます。各ポートプロファイルは、インターフェイスのタイプにかかわらず、ネットワーク上で一意の名前を持つ必要があります。

手順の概要

1. **configure terminal**
2. **port-profile** [**type** {**ethernet** | **interface-vlan** | **port channel**}] *name*
3. **exit**
4. （任意） **show port-profile**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`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	**port-profile** [**type** {**ethernet** | **interface-vlan** | **port channel**}] *name*
	
	例：
	`switch(config)# port-profile type ethernet test`
	`switch(config-port-prof)#`
		指定されたタイプのインターフェイスのポート プロファイルを作成して命名し、ポート プロファイル コンフィギュレーション モードを開始します。

ステップ 3	**exit**
	
	例：
	`switch(config-port-prof)# exit`
	`switch(config)#`
		ポート プロファイル コンフィギュレーション モードを終了します。

ステップ 4	**show port-profile** 例： `switch(config)# show port-profile name`	（任意） ポート プロファイルの設定を表示します。

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

次の例は、イーサネット インターフェイスに対して test という名前のポート プロファイルを作成する方法を示したものです。

```
switch# configure terminal
switch(config)# port-profile type ethernet test
switch(config-port-prof)#
```

次の例は、イーサネット インターフェイスに対して設定した ppEth という名前のポート プロファイルに、インターフェイス コマンドを追加する方法を示したものです。

```
switch# configure terminal
switch(config)# port-profile ppEth
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport trunk allowed vlan 300-400
switch(config-port-prof)# flowcontrol receive on
switch(config-port-prof)# speed 10000
switch(config-port-prof)#
```

ポート プロファイルの変更

ポート プロファイル コンフィギュレーション モードでポート プロファイルを変更することができます。

このコマンドの **no** 形式を使用すると、ポート プロファイルからコマンドを削除することができます。ポートプロファイルからコマンドを削除すると、それに対応するコマンドも、そのポートプロファイルが適用されているインターフェイスから削除されます。

手順の概要

1. **configure terminal**
2. **port-profile** [**type** {**ethernet** | **interface-vlan** | **port channel**}] *name*
3. **exit**
4. （任意） **show port-profile**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`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	**port-profile** [**type** {**ethernet** | **interface-vlan** | **port channel**}] *name*
	
	例：
	`switch(config)# port-profile type ethernet test`
	`switch(config-port-prof)#`
		指定されたポート プロファイルのポート プロファイル コンフィギュレーション モードを開始し、プロファイルの設定を追加または削除できるようにします。

ステップ 3	**exit**
	
	例：
	`switch(config-port-prof)# exit`
	`switch(config)#`
		ポート プロファイル コンフィギュレーション モードを終了します。

ステップ 4	**show port-profile** 例： `switch(config)# show port-profile name`	（任意） ポート プロファイルの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、イーサネット インターフェイスに対して設定した ppEth という名前のポート プロファイルからコマンドを削除する方法を示したものです。

```
switch# configure terminal
switch(config)# port-profile ppEth
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport trunk allowed vlan 300-400
switch(config-port-prof)# flowcontrol receive on
switch(config-port-prof)# no speed 10000
switch(config-port-prof)#
```

特定のポート プロファイルのイネーブル化

手順の概要

1. **configure terminal**
2. **port-profile** [**type** {**ethernet** | **interface-vlan** | **port channel**}] *name*
3. **state enabled** *name*
4. **exit**
5. （任意） **show port-profile**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`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	**port-profile** [**type** {**ethernet**	**interface-vlan**	**port channel**}] *name*
			
			例：
			`switch(config)# port-profile type ethernet test`
			`switch(config-port-prof)# no shutdown`
			`switch(config-port-prof)#`
				指定したポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。

ステップ 3	**state enabled** *name*
	
	例：
	`switch(config-port-prof)# state enabled`
	`switch(config-port-prof)#`
		ポート プロファイルをイネーブルにします。

ステップ 4	**exit**
	
	例：
	`switch(config-port-prof)# exit`
	`switch(config)#`
		ポート プロファイル コンフィギュレーション モードを終了します。

ステップ 5	**show port-profile** 例： `switch(config)# show port-profile name`	（任意） ポート プロファイルの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、ポート プロファイル コンフィギュレーション モードを開始し、ポート プロファイルをイネーブルにする方法を示したものです。

```
switch# configure terminal
switch(config)# port-profile type ethernet test
switch(config-port-prof)# state enabled
switch(config-port-prof)#
```

ポート プロファイルの継承

ポート プロファイルを既存のポート プロファイルに継承できます。 スイッチでは 4 つのレベルの継承がサポートされています。

手順の概要

1. **configure terminal**
2. **port-profile** *name*
3. **inherit port-profile** *name*
4. **exit**
5. （任意） **show port-profile**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`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	**port-profile** *name*
	
	例：
	`switch(config)# port-profile test`
	`switch(config-port-prof)#`
		指定したポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。

ステップ 3	**inherit port-profile** *name*
	
	例：
	`switch(config-port-prof)#  inherit port-profile adam`
	`switch(config-port-prof)#`
		別のポート プロファイルを既存のポート プロファイルに継承します。 元のポート プロファイルは、継承されたポート プロファイルのすべての設定を想定します。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`switch(config-port-prof)# exit`
	`switch(config)#`
		ポート プロファイル コンフィギュレーション モードを終了します。

ステップ 5	**show port-profile** 例： `switch(config)# show port-profile name`	（任意） ポート プロファイルの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例では、adam という名前のポート プロファイルを test という名前のポート プロファイルに継承する方法を示します。

```
switch# configure terminal
switch(config)# port-profile test
switch(config-ppm)# inherit port-profile adam
switch(config-ppm)#
```

次の例は、イーサネット インターフェイスに対して設定した ppEth という名前のポート プロファイルに、インターフェイス コマンドを追加する方法を示したものです。

```
switch# configure terminal
switch(config)# port-profile ppEth
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport trunk allowed vlan 300-400
switch(config-port-prof)# flowcontrol receive on
switch(config-port-prof)# speed 10000
switch(config-port-prof)#
```

次の例は、イーサネット インターフェイスに対して設定した ppEth という名前のポート プロファイルを、test という名前の既存のポート プロファイルに継承する方法を示したものです。

```
switch# configure terminal
switch(config)# port-profile test
switch(config-port-prof)# inherit port-profile ppEth
switch(config-port-prof)#
```

次の例は、イーサネット インターフェイスに対して設定した ppEth という名前のポート プロファイルを、複数のイーサネット インターフェイスに適用する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/2-5
switch(config-if)# inherit port-profile ppEth
switch(config-if)#
```

次の例は、ppEth という名前の継承されたポート プロファイルを test という名前の既存のポート プロファイルから削除する方法を示したものです。

```
switch# configure terminal
switch(config)# port-profile test
switch(config-port-prof)# no inherit port-profile ppEth
switch(config-port-prof)#
```

継承されたポート プロファイルの削除

継承されたポート プロファイルを削除できます。

手順の概要

1. **configure terminal**
2. **port-profile** *name*
3. **no inherit port-profile** *name*
4. **exit**
5. （任意） **show port-profile**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`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	**port-profile** *name*
	
	例：
	`switch(config)# port-profile test`
	`switch(config-port-prof)#`
		指定したポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。

ステップ 3	**no inherit port-profile** *name*
	
	例：
	`switch(config-port-prof)#  no inherit port-profile adam`
	`switch(config-port-prof)#`
		このポート プロファイルから継承されたポート プロファイルを削除します。

ステップ 4	**exit**
	
	例：
	`switch(config-port-prof)# exit`
	`switch(config)#`
		ポートプロファイルコンフィギュレーションモードを終了します。

ステップ 5	**show port-profile** 例： `switch(config)# show port-profile name`	（任意） ポート プロファイルの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例では、adam という名前の継承されたポート プロファイルを test という名前のポート プロファイルから削除する方法を示します。

```
switch# configure terminal
switch(config)# port-profile test
switch(config-ppm)# no inherit port-profile adam
switch(config-ppm)#
```

一定範囲のインターフェイスへのポート プロファイルの割り当て

単独のインターフェイスまたはある範囲に属する複数のインターフェイスにポート プロファイルを割り当てることができます。 インターフェイスはすべて同じタイプであることが必要です。

手順の概要

1. **configure terminal**
2. **interface** [**ethernet** *slot/port* | **interface-vlan** *vlan-id* | **port-channel** *number*]
3. **inherit port-profile** *name*
4. **exit**
5. （任意） **show port-profile**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**interface** [**ethernet** *slot/port*	**interface-vlan** *vlan-id*	**port-channel** *number*]
			
			例：
			`switch(config)# interface ethernet 7/3-5, 10/2, 11/20-25`
			`switch(config-if)#`
				インターフェイスの範囲を選択します。

ステップ 3	**inherit port-profile** *name*
	
	例：
	`switch(config-if)# inherit port-profile adam`
	`switch(config-if)#`
		指定したポート プロファイルを、選択したインターフェイスに割り当てます。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`switch(config-port-prof)# exit`
	`switch(config)#`
		ポート プロファイル コンフィギュレーション モードを終了します。

ステップ 5	**show port-profile** 例： `switch(config)# show port-profile name`	（任意） ポート プロファイルの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、イーサネット インターフェイス 2/3 ～ 2/5、3/2、および 1/20 ～ 1/25 に adam という名前のポート プロファイルを割り当てる方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 2/3 to 2/5, 3/2, and 1/20 to 1/25
switch(config-if)# inherit port-profile adam
switch(config-if)#
```

一定範囲のインターフェイスからのポート プロファイルの削除

プロファイルを適用した一部またはすべてのインターフェイスから、ポート プロファイルを削除できます。

手順の概要

1. **configure terminal**
2. **interface** [**ethernet** *slot/port* | **interface-vlan** *vlan-id* | **port-channel** *number*]
3. **no inherit port-profile** *name*
4. **exit**
5. （任意） **show port-profile**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**interface** [**ethernet** *slot/port* | **interface-vlan** *vlan-id* | **port-channel** *number*]
	
	例：
	`switch(config)# interface ethernet 7/3-5, 10/2, 11/20-25`
	`switch(config-if)#`
		インターフェイスの範囲を選択します。

ステップ 3	**no inherit port-profile** *name*
	
	例：
	`switch(config-if)# no inherit port-profile adam`
	`switch(config-if)#`
		選択されたインターフェイスから指定されたポート プロファイルを削除します。

ステップ 4	**exit**
	
	例：
	`switch(config-port-prof)# exit`
	`switch(config)#`
		ポート プロファイル コンフィギュレーション モードを終了します。

ステップ 5	**show port-profile** 例： `switch(config)# show port-profile name`	（任意） ポート プロファイルの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、イーサネット インターフェイス 1/3 ～ 5 から adam という名前のポート プロファイルを削除する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/3-5
switch(config-if)# no inherit port-profile adam
switch(config-if)#
```

ポート プロファイルの設定例

次の例は、ポートプロファイルを設定して、イーサネットインターフェイスでそれを継承し、さらにそのポート プロファイルをイネーブルにする方法を示したものです。

```
switch(config)#
switch(config)# show running-config interface Ethernet1/14

!Command: show running-config interface Ethernet1/14
!Time: Thu Aug 26 07:01:32 2010

version 5.0(2)N1(1)

interface Ethernet1/14

switch(config)# port-profile type ethernet alpha
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport trunk allowed vlan 10-15
switch(config-port-prof)#
switch(config-port-prof)# show running-config port-profile alpha

!Command: show running-config port-profile alpha
!Time: Thu Aug 26 07:02:29 2010

version 5.0(2)N1(1)
port-profile type ethernet alpha
  switchport mode trunk
  switchport trunk allowed vlan 10-15


switch(config-port-prof)# int eth 1/14
switch(config-if)# inherit port-profile alpha
switch(config-if)#
switch(config-if)# port-profile type ethernet alpha
switch(config-port-prof)# state enabled
switch(config-port-prof)#
switch(config-port-prof)# sh running-config interface ethernet 1/14

!Command: show running-config interface Ethernet1/14
!Time: Thu Aug 26 07:03:17 2010

version 5.0(2)N1(1)

interface Ethernet1/14
  inherit port-profile alpha

switch(config-port-prof)# sh running-config interface ethernet 1/14 expand-port-profile

!Command: show running-config interface Ethernet1/14 expand-port-profile
!Time: Thu Aug 26 07:03:21 2010

version 5.0(2)N1(1)

interface Ethernet1/14
  switchport mode trunk
  switchport trunk allowed vlan 10-15

switch(config-port-prof)#
```

デバウンス タイマーの設定

イーサネットのデバウンス タイマーは、デバウンス時間（ミリ秒単位）を指定することによりイネーブル化でき、デバウンス時間に 0 を指定することによりディセーブル化できます。

show interface debounce コマンドを使用すれば、すべてのイーサネット ポートのデバウンス時間を表示できます。

デバウンス タイマーをイネーブル/ディセーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port*
3. switch(config-if)# **link debounce time** *milliseconds*

手順の詳細

	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*	指定したインターフェイスに対してインターフェイス 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)# **link debounce time** *milliseconds*	指定した時間（1 ～ 5,000 ミリ秒）でデバウンス タイマーをイネーブルにします。 0 ミリ秒を指定すると、デバウンス タイマーはディセーブルになります。

次の例は、イーサネットインターフェイスでデバウンスタイマーをイネーブルにして、デバウンス時間を 1000 ミリ秒に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)# link debounce time 1000
```

次の例は、イーサネットインターフェイスでデバウンスタイマーをディセーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# link debounce time 0
```

説明パラメータの設定

イーサネット ポートのインターフェイスのテキストでの説明を提供する手順は、次のとおりです。

手順の概要

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

手順の詳細

	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*	指定したインターフェイスに対してインターフェイス 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)# **description** *test*	インターフェイスの説明を指定します。

次の例は、インターフェイスの説明を「Server 3 Interface」に設定する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# description Server 3 Interface
```

イーサネット インターフェイスのディセーブル化と再起動

イーサネットインターフェイスは、シャットダウンして再起動することができます。この操作により、すべてのインターフェイス機能がディセーブル化され、すべてのモニタリング画面でインターフェイスがダウンしているものとしてマークされます。 この情報は、すべてのダイナミック ルーティング プロトコルを通じて、他のネットワーク サーバに伝達されます。 シャットダウンされたインターフェイスは、どのルーティング アップデートにも含まれません。

インターフェイスをディセーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port*
3. switch(config-if)# **shutdown**
4. switch(config-if)# **no shutdown**

手順の詳細

	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*	指定したインターフェイスに対してインターフェイス 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)# **shutdown**	インターフェイスをディセーブルにします。
ステップ 4	switch(config-if)# **no shutdown**	インターフェイスを再起動します。

次に、イーサネット ポートをディセーブルにする例を示します。

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

次に、イーサネット インターフェイスを再起動する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# no shutdown
```

インターフェイス情報の表示

定義済みインターフェイスに関する設定情報を表示するには、次のうちいずれかの手順を実行します。

コマンド	目的
switch# **show interface** *type slot*/*port*	指定したインターフェイスの詳細設定が表示されます。
switch# **show interface** *type slot*/*port* **capabilities**	指定したインターフェイスの機能に関する詳細情報が表示されます。 このオプションは、物理インターフェイスにしか使用できません。
switch# **show interface** *type slot*/*port* **transceiver**	指定したインターフェイスに接続されているトランシーバに関する詳細情報が表示されます。 このオプションは、物理インターフェイスにしか使用できません。
switch# **show interface brief**	すべてのインターフェイスのステータスが表示されます。

コマンド	目的
switch# **show interface debounce**	すべてのインターフェイスのデバウンス ステータスが表示されます。
switch# **show interface flowcontrol**	すべてのインターフェイスでフロー制御設定の詳細なリストを表示します。
show port--profile	ポート プロファイルに関する情報を表示します。

show interface コマンドはEXECモードから呼び出されます。このコマンドにより、インターフェイスの設定を表示することができます。 引数を入力せずにこのコマンドを実行すると、スイッチ内に設定されたすべてのインターフェイスの情報が表示されます。

次に、物理イーサネット インターフェイスを表示する例を示します。

```
switch# show interface ethernet 1/1
  Ethernet1/1 is up
  Hardware is 1000/10000 Ethernet, address is 000d.eca3.5f08 (bia 000d.eca3.5f08)
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 190/255, rxload 192/255
  Encapsulation ARPA
  Port mode is trunk
  full-duplex, 10 Gb/s, media type is 1/10g
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned on
  Rate mode is dedicated
  Switchport monitor is off
  Last clearing of "show interface" counters never
  5 minute input rate 942201806 bytes/sec, 14721892 packets/sec
  5 minute output rate 935840313 bytes/sec, 14622492 packets/sec
  Rx
    129141483840 input packets 0 unicast packets 129141483847 multicast packets
    0 broadcast packets 0 jumbo packets 0 storm suppression packets
    8265054965824 bytes
    0 No buffer 0 runt 0 Overrun
    0 crc 0 Ignored 0 Bad etype drop
    0 Bad proto drop
  Tx
    119038487241 output packets 119038487245 multicast packets
   0 broadcast packets 0 jumbo packets
    7618463256471 bytes
    0 output CRC 0 ecc
    0 underrun 0 if down drop     0 output error 0 collision 0 deferred
    0 late collision 0 lost carrier 0 no carrier
    0 babble
    0 Rx pause 8031547972 Tx pause 0 reset
```

次に、物理イーサネットの機能を表示する例を示します。

```
switch# show interface ethernet 1/1 capabilities
Ethernet1/1
  Model:                 734510033
  Type:                  10Gbase-(unknown)
  Speed:                 1000,10000
  Duplex:                full
  Trunk encap. type:     802.1Q
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off/on),tx-(off/on)
  Rate mode:             none
  QOS scheduling:        rx-(6q1t),tx-(1p6q0t)
```

```
  CoS rewrite:           no
  ToS rewrite:           no
  SPAN:                  yes
  UDLD:                  yes
  Link Debounce:         yes
  Link Debounce Time:    yes
  MDIX:                  no
  FEX Fabric:            yes
```

次に、物理イーサネット トランシーバを表示する例を示します。

```
switch# show interface ethernet 1/1 transceiver
Ethernet1/1
    sfp is present
    name is CISCO-EXCELIGHT
    part number is SPP5101SR-C1
    revision is A
    serial number is ECL120901AV
    nominal bitrate is 10300 MBits/sec
    Link length supported for 50/125mm fiber is 82 m(s)
    Link length supported for 62.5/125mm fiber is 26 m(s)
    cisco id is --
    cisco extended id number is 4
```

次に、インターフェイス ステータスの要約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 interface brief

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                  Ch #
--------------------------------------------------------------------------------
Eth1/1        200    eth  trunk  up      none                      10G(D) --
Eth1/2        1      eth  trunk  up      none                      10G(D) --
Eth1/3        300    eth  access down    SFP not inserted          10G(D) --
Eth1/4        300    eth  access down    SFP not inserted          10G(D) --
Eth1/5        300    eth  access down    Link not connected      1000(D) --
Eth1/6        20     eth  access down    Link not connected        10G(D) --
Eth1/7        300    eth  access down    SFP not inserted          10G(D) --
...
```

次の例は、リンクのデバウンス ステータスの表示方法を示しています（簡潔にするため、一部の出力が削除されています）。

```
switch# show interface debounce

--------------------------------------------------------------------------------
Port          Debounce time   Value(ms)
--------------------------------------------------------------------------------
...
Eth1/1        enable              100
Eth1/2        enable              100
Eth1/3        enable              100
...
```

次に、CDP ネイバーを表示する例を示します。

（注） 上記の例のとおり、CDP アドバタイズメントのデバイス ID フィールドには、デフォルトでホスト名とシリアル番号が表示されます。

```
switch# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID
d13-dist-1               mgmt0           148     S I      WS-C2960-24TC  Fas0/9
n5k(FLC12080012)         Eth1/5          8       S I s    N5K-C5020P-BA  Eth1/5
```

物理イーサネットのデフォルト設定

次の表に、すべての物理イーサネット インターフェイスのデフォルト設定を示します。

パラメータ	デフォルト設定
デバウンス	イネーブル、100 ミリ秒
デュプレックス	オート（全二重）
カプセル化	ARPA
MTU[1]	1500 バイト
ポート モード	アクセス
速度	オート（10000）

1 MTU を物理イーサネット インターフェイスごとに変更することはできません。 MTU の変更は、QoS クラスのマップを選択することにより行います。

第 4 章

VLAN の設定

この章の内容は、次のとおりです。

VLAN について

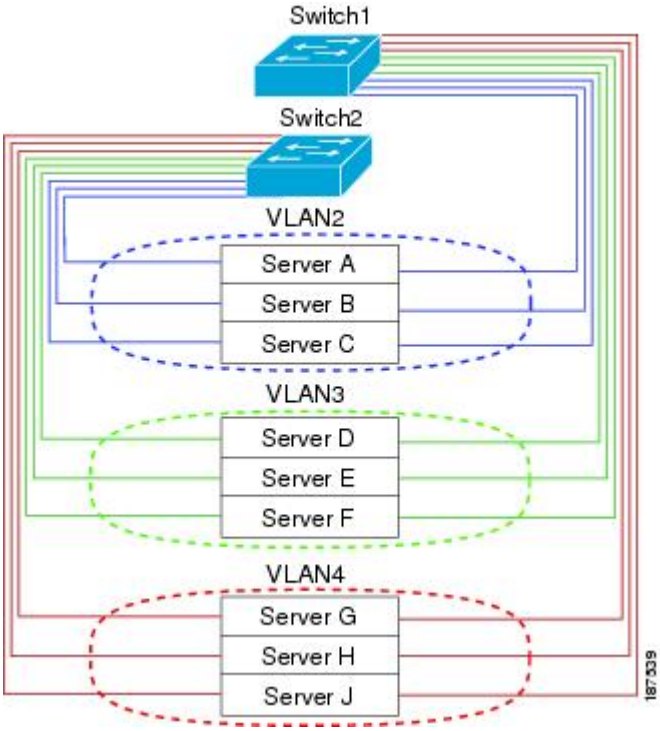
VLAN の概要

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によって論理的にセグメント化されているスイッチド ネットワーク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。

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

次の図は、論理ネットワークとしての VLAN を図示したものです。この図では、エンジニアリング部門のステーションはある VLAN に、マーケティング部門のステーションは別の VLAN に、会計部門のステーションはまた別の VLAN に割り当てられています。

図 *2*：論理的に定義されたネットワークとしての *VLAN*



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

新規作成された VLAN は、デフォルトでは動作可能な状態にあります。VLAN をディセーブルにする場合は、**shutdown** コマンドを使用します。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。

（注） VLAN トランキング プロトコル（VTP）モードはオフです。VTP BPDU は、スイッチのすべてのインターフェイスでドロップされます。これは、他のスイッチで VTP がオンになると VTP ドメインが分割されることによる影響です。

VLAN は、スイッチ仮想インターフェイス（SVI）として設定することもできます。この場合、VLAN のスイッチ ポートは、ルーティング システムまたはブリッジング システムへの仮想インターフェイスにより表されます。SVI は、ルーティング用として設定することができます。この場合 SVI では、VLAN に関連付けられたすべてのスイッチ ポートからのパケットを処理する場合や、スイッチのインバンド管理を行う場合にレイヤ 3 プロトコルを使用することができます。

VLAN 範囲の概要

Cisco Nexus 5000 シリーズ スイッチでは、IEEE 802.1Q 標準に従って VLAN 番号 1 ～ 4094 がサポートされます。 これらの VLAN は、範囲ごとにまとめられています。 スイッチでサポートできる VLAN の数には物理的な制限があります。 ハードウェアは、この使用可能範囲を VSAN とも共有します。 VLAN および VSAN の設定制限に関する詳細については、各スイッチに対応する設定制限についてのマニュアルを参照してください。

次の表は、VLAN の範囲に関する詳細をまとめたものです。

表 *4*： *VLAN* の範囲

VLAN 番号	範囲	用途
1	標準	シスコのデフォルトです。 この VLAN は使用できますが、変更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 ～ 4094	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。 • ステートは常にアクティブになります。 • VLAN は常にイネーブルになります。 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 個の VLAN および VLAN 4094 は、内部で使用するため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。

（注） 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。

Cisco NX-OS では、動作のために内部 VLAN を使用する必要がある、マルチキャストや診断などの機能用に、80 個の VLAN 番号のグループを割り当てています。 デフォルトでは、番号 3968 ～ 4047 の VLAN が内部使用に割り当てられます。 VLAN 4094 もスイッチの内部使用のために予約されています。

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

VLAN の作成、削除、変更

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

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

新しく作成した VLAN は、その VLAN にポートが割り当てられるまで使用されません。 すべてのポートはデフォルトで VLAN1 に割り当てられます。

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

- VLAN 名
- シャットダウンまたは非シャットダウン

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

（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、ドメイン間で VTP VLAN データベースを同期するための分散 VLAN データベース管理プロトコルです。 VTP ドメインは 1 つ以上のネットワーク スイッチで構成されます。これらのネットワーク スイッチは同じ VTP ドメイン名を共有し、トランク インターフェイスで接続されます。 スイッチは、1 つの VTP ドメインにだけ所属できます。 レイヤ 2 トランク インターフェイス、レイヤ 2 ポート チャネル、および Virtual Port Channel（vPC; 仮想ポート チャネル）は、

VTP 機能をサポートしています。 Cisco NX-OS Release 5.0(2)N1(1) で初めて、VTPv1 および VTP2 がサポートされました。 Cisco NX-OS Release 5.0(2)N2(1) 以降では、クライアント モードまたはサーバ モードの VTP を設定することができます。 NX-OS Release 5.0(2)N2(1) 以前は、VTP はトランスペアレント モードでのみ動作していました。

次のように、VTP モードには 4 種類あります。

- サーバモード：ユーザによる設定が可能です。VLANデータベースのバージョン番号の管理と、VLAN データベースの格納を行います。
- クライアントモード：ユーザによる設定はできません。設定情報はドメイン内にある他のスイッチから取得します。
- オフモード：VLANデータベースにアクセスすることはできますが（VTPはイネーブル）、VTP には関与できません。
- トランスペアレントモード：VTPには関与しません。ローカル設定が使用され、VTPパケットは他の転送ポートにリレーされます。 VLAN の変更により影響を受けるのは、ローカル スイッチのみです。 VTP トランスペアレント ネットワーク デバイスでは、VLAN 設定のアドバタイズは行われず、受信したアドバタイズに基づいて同期化されることもありません。

VTP の注意事項と制約事項

VTP 設定時の注意事項と制約事項は次のとおりです。

- VTP クライアントとして設定されたスイッチ上では、1 ～ 1005 の範囲の VLAN を作成することはできません。
- 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から VLAN 1 をディセーブルにすると、VTP は正常に機能しなくなります。
- VTP をイネーブルにした場合、バージョン 1 またはバージョン 2 のいずれかを設定する必要があります。 Cisco Nexus 5010 スイッチおよび Nexus 5020 スイッチでサポートされている VLAN の数は 512 です。 これらのスイッチが、他のスイッチを含む分散ネットワークに属している場合も、これと同じ制約事項が適用されます。

  Cisco Nexus 5010 スイッチおよび Nexus 5020 スイッチでサポートされている VLAN の数は 512 です。 これらのスイッチが、他のスイッチを含む分散ネットワークに属している場合も、VTP ドメインでの VLAN の上限数は 512 です。 Nexus 5010 スイッチまたは Nexus 5020 スイッチのクライアント/サーバは、VTP サーバからの追加の VLAN を認識すると、トランスペアレント モードに移行します。
- show running-configuration コマンドを実行しても、1 ～ 1000 の VLAN に関する VLAN 設定情報や VTP 設定情報は表示されません。
- vPC が導入されている場合、プライマリ vPC スイッチとセカンダリ vPC スイッチは同一の設定にする必要があります。 vPC では、VTP 設定パラメータに関してタイプ 2 整合性検査が実行されます。

- VTP アドバタイズメントは、Cisco Nexus 2000 シリーズ ファブリック エクステンダのポートからは送信されません。
- VTP プルーニングは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 モードで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 モードまたは VTP サーバ モードで設定されている場合、1002 ～1005 の VLAN は予約済みの VLAN となります。
- SNMP での VTP MIB オブジェクトに対する GET 操作および SET 操作のサポート状況は次のとおりです。
  - VTPv3 MIB オブジェクトに対しては、GET 操作と SET 操作のいずれもサポートされていません。
  - VTPv1 MIB オブジェクトおよび VTPv2 MIB オブジェクトに対しては、SET 操作がサポートされていません。
  - VTPv1 MIB オブジェクトおよび VTPv2 MIB オブジェクトに対しては、GET 操作がサポートされています。

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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vlan** {*vlan-id* | *vlan-range*}
3. switch(config-vlan)# **no vlan** {*vlan-id* | *vlan-range*}

手順の詳細

	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*}	単独の VLAN またはある範囲に属する複数の VLAN を作成します。 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。

- Name
- Shut down

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

手順の概要

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

手順の詳細

	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。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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。 インターフェイスは、物理イーサネット ポートでも EtherChannel でもかまいません。
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
```

VTP の設定

Cisco NX-OS Release 5.0(2)N2(1) 以降では、Cisco Nexus 5000 シリーズ スイッチ上で、クライアント モードまたはサーバ モードの VTP を設定することができます。 Cisco NX-OS Release 5.0(2)N2(1) 以前は、VTP はトランスペアレント モードでのみ動作していました。

VTPモード（サーバ（デフォルト）、クライアント、トランスペアレント、またはオフ）は、VTP をイネーブルにした後で設定することができます。 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。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

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

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

ステップ 3	**vtp domain** *domain-name* 例： `switch(config)# vtp domain accounting`	このデバイスを追加する VTP ドメインの名前を指定します。 デフォルトは空白です。
ステップ 4	**vtp version** {**1**	**2**} 例： `switch(config)# vtp version 2`	使用する VTP バージョンを設定します。デフォルトはバージョン 1 です。
ステップ 5	**vtp mode** {**client**	**server**| **transparent**| **off**} 例： `switch(config)# vtp mode transparent`	VTP モードを、クライアント、サーバ、トランスペアレント、またはオフに設定します。 NX-OS Release 5.0(2)N2(1) 以降では、クライアント モードまたはサーバ モードの VTP 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 6	**vtp file** *file-name* 例： `switch(config)# vtp file vtp.dat`	VTP 設定を保存する IFS ファイル システム ファイルの ASCII ファイル名を指定します。
ステップ 7	**vtp password** *password-value* 例： `switch(config)# vtp password cisco`	VTP 管理ドメイン用のパスワードを指定します。

ステップ 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、リビジョン番号など、デバイス上の VTP 設定に関する情報を表示します。
ステップ 10	**show vtp counters** 例： `switch# show vtp counters`	（任意） デバイス上の VTP アドバタイズメントに関する統計情報を表示します。
ステップ 11	**show vtp interface** 例： `switch# show vtp interface`	（任意） VTP がイネーブルになっているインターフェイスの一覧を表示します。
ステップ 12	**show vtp password** 例： `switch# show vtp password`	（任意） 管理 VTP ドメイン用のパスワードを表示します。
ステップ 13	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

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

```
switch(config)# show vtp status
VTP Status Information
----------------------
VTP Version                     : 2 (capable)
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 502
VTP Operating Mode              : Transparent
VTP Domain Name                 :
VTP Pruning Mode                : Disabled (Operationally Disabled)
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 Digest                      : 0xF5 0xF1 0xEC 0xE7 0x29 0x0C 0x2D 0x01
Configuration last modified by 60.10.10.1 at 0-0-00 00:00:00
VTP version running             : 1
```

VLAN 設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

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

第 5 章

プライベート VLAN の設定

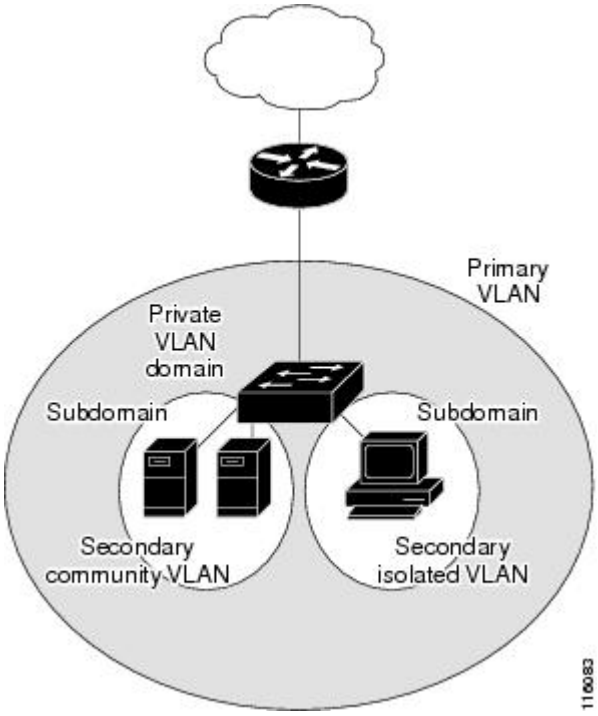
この章の内容は、次のとおりです。

プライベート VLAN について

プライベート VLAN（PVLAN）では VLAN のイーサネット ブロードキャスト ドメインがサブドメインに分割されるため、スイッチ上のポートを互いに分離することができます。 サブドメインは、1 つのプライマリ VLAN と 1 つ以上のセカンダリ VLAN とで構成されます（次の図を参照）。 1 つの PVLAN に含まれる VLAN はすべて、同じプライマリ VLAN を共有します。 セカンダリ VLAN ID は、各サブドメインの区別に使用されます。 セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかの場合があります。 独立 VLAN 上のホストは、そのプライマリ VLAN 上でアソシエートされている無差別ポートのみと通信できます。 コミュニティ VLAN 上の

ホストは、それぞれのホスト間およびアソシエートされている無差別ポートと通信できますが、他のコミュニティ VLAN にあるポートとは通信できません。

図 *3*：プライベート *VLAN* ドメイン



（注） VLAN をプライマリまたはセカンダリの PVLAN に変換する場合は、あらかじめその VLAN を作成しておく必要があります。

プライベート VLAN のプライマリ VLAN とセカンダリ VLAN

プライベート VLAN ドメインには、プライマリ VLAN が 1 つのみ含まれています。 プライベート VLAN ドメインの各ポートは、プライマリ VLAN のメンバです。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。 各無差別ポートには、複数のセカンダリ VLAN を関連付けることができるほか、セカンダリ VLAN をまったく関連付けないことも可能です。 無差別ポートとセカンダリ VLAN が同じプライマリ VLAN にある限り、セカンダリ VLAN は、複数の無差別ポートとアソシエートすることができます。 ロード バランシングまたは冗長性を持たせる目的で、これを行う必要が生じる場合があります。 無差別ポートとアソシエートされていないセカンダリ VLAN も、含めることができます。

  無差別ポートは、アクセス ポートまたはトランク ポートとして設定できます。

- 独立ポート：独立ポートは、セカンダリ独立 VLAN に属するホスト ポートです。 このポートは、同じ PVLAN ドメイン内の他のポートから完全に独立しています。ただし、関連付けられている無差別ポートと通信することはできます。 PVLAN は、無差別ポートからのトラフィックを除き、独立ポート宛のトラフィックをすべてブロックします。 独立ポートから受信されたトラフィックは、無差別ポートにだけ転送されます。 指定した独立 VLAN には、複数の独立ポートを含めることができます。 各ポートは、独立 VLAN にある他のすべてのポートから、完全に隔離されています。

  独立ポートは、アクセス ポートまたはトランク 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 ポートは、1 つのコミュニティ セカンダリ VLAN に属するホスト ポートです。 コミュニティ ポートは、同じコミュニティ VLAN にある他のポートおよびアソシエートされている無差別ポートと通信します。 これらのインターフェイスは、他のコミュニティにあるすべてのインターフェイス、および PVLAN ドメイン内のすべての独立ポートから分離されています。

  コミュニティ ポートは、アクセス ポートとして設定する必要があります。 独立トランクに対してコミュニティ VLAN をイネーブルにすることはできません。

（注） ファブリック エクステンダ（FEX）のトランク ポートは、FEX トランク ポートにすることも、FEX 独立トランク ポートにすることもできます。

（注） トランクは、無差別ポート、独立ポート、およびコミュニティ ポートの間でトラフィックを伝送する VLAN をサポートできるため、独立ポートとコミュニティ ポートのトラフィックはトランク インターフェイスを経由してスイッチと送受信されることがあります。

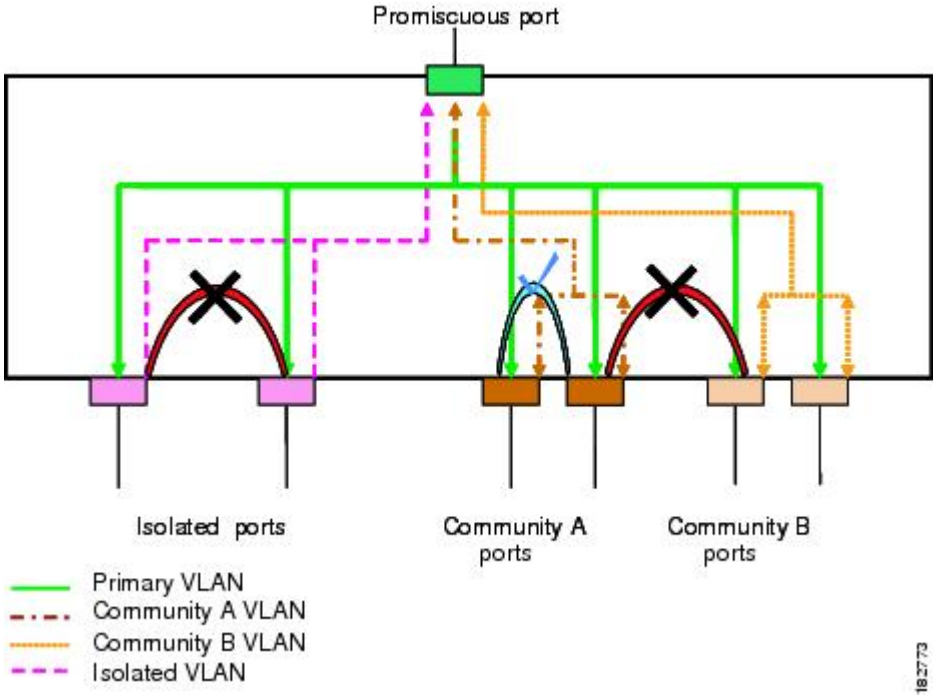
プライマリ、独立、およびコミュニティ プライベート VLAN

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

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

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

図 *4*：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 で受信したトラフィックによって隔離は行われず、転送は通常の VLAN として実行されます。

無差別アクセス ポートでは、ただ 1 つのプライマリ VLAN と複数のセカンダリ VLAN（コミュニティ VLAN および独立 VLAN）を処理できます。 無差別トランク ポートでは、複数のプライマリ VLAN のトラフィックを伝送できます。 無差別トランク ポートには、同じプライマリ VLAN に従属する複数のセカンダリ VLAN をマップすることができます。 無差別ポートを使用すると、さまざまなデバイスを PVLAN への「アクセス ポイント」として接続できます。 たとえば、すべての PVLAN サーバを管理ワークステーションから監視したりバックアップしたりするのに、無差別ポートを使用できます。

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

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 PVLAN の外部と通信できるようにするためには、セカンダリ VLAN をプライマリ VLAN に関連付ける必要があります。 アソシエーション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） 関連付けの操作が可能かどうかを確認する場合は、**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場合は、**no private-vlan** コマンドを使用します。 その VLAN におけるプライマリとセカンダリの関連付けはすべて一時停止されますが、インターフェイスは PVLAN モードのままです。 VLAN を PVLAN モードに戻すと、関連付けも元の状態に戻ります。

プライマリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN に関連付けられている PVLAN はすべて削除されます。 ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN と PVLAN との関連付けは一時停止します。この VLAN を再作成して以前のセカンダリ VLAN として設定すると、関連付けは元の状態に戻ります。

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

プライベート VLAN の無差別トランク

無差別トランク ポートでは、複数のプライマリ VLAN のトラフィックを伝送できます。 無差別トランク ポートには、同じプライマリ VLAN に従属する複数のセカンダリ VLAN をマップすることができます。 無差別ポートでは、プライマリ VLAN タグを使用してトラフィックの送受信が行われます。

プライベート VLAN の独立トランク

独立トランク ポートでは、複数の独立 PVLAN のトラフィックを伝送することができます。 コミュニティ VLAN のトラフィックは、独立トランク ポートによっては伝送されません。 独立トランク ポートでは、独立 VLAN タグを使用してトラフィックの送受信が行われます。 独立トランク ポートは、ホスト サーバに接続することを目的としたものです。

Cisco Nexus 2000 シリーズ FEX の独立 PVLAN ポートをサポートするためには、Cisco Nexus 5000 シリーズ スイッチにより FEX 上の独立ポート間の通信が回避される必要があります。転送はすべて、Cisco Nexus 5000 シリーズ スイッチを経由して行われます。

注意 FEX トランク ポートで PVLAN を設定する場合は、その前に FEX 独立トランク ポートをすべてディセーブルにしておく必要があります。 FEX 独立トランク ポートと FEX トランク ポートをともにイネーブルにすると、不要なネットワーク トラフィックが発生することがあります。

ユニキャスト トラフィックに対しては、他に影響を与えることなく、こうした通信を回避することができます。

マルチキャスト トラフィックに対しては、FEX によりフレームのレプリケーションが行われます。 FEX の独立 PVLAN ポート間での通信を回避するため、Cisco Nexus 5000 シリーズ スイッチではマルチキャスト フレームがファブリック ポート経由で返送されないようになっています。これにより、FEX 上の独立 VLAN と無差別ポートとの間での通信は行われません。 ただし、ホストインターフェイスは別のスイッチやルータに接続することを目的としたものではないため、FEX で無差別ポートをイネーブルにすることはできません。

プライベート VLAN 内のブロードキャスト トラフィック

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

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

プライベート VLAN ポートの分離

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

- 通信を防止するには、エンドステーションに接続されているインターフェイスのうち、選択したインターフェイスを、独立ポートとして設定します。 たとえば、エンド ステーションがサーバの場合、この設定により、サーバ間の通信が防止されます。
- デフォルト ゲートウェイおよび選択したエンド ステーション（バックアップ サーバなど）に接続されているインターフェイスを無差別ポートとして設定し、すべてのエンド ステーションがデフォルト ゲートウェイにアクセスできるようにします。

プライベート VLAN の設定に関する注意事項と制約事項

PVLAN を設定する場合は、次の注意事項に従ってください。

- 指定した VLAN をプライベート VLAN として割り当てる前に、VLAN を作成しておく必要があります。
- スイッチで PVLAN 機能を適用できるようにするには、あらかじめ PVLAN をイネーブルにしておく必要があります。
- PVLAN モードで動作しているポートがスイッチにある場合、PVLAN をディセーブルにすることはできません。
- マルチ スパニングツリー（MST）リージョン定義内から **private-vlan synchronize** コマンドを実行すると、プライマリ VLAN と同じ MST インスタンスにセカンダリ VLAN をマップすることができます。

- FEX トランク ポートを設定する場合は、その前にすべての FEX 独立トランク ポートをディセーブルにしておく必要があります。
- Cisco NX-OS Release 5.0(2)N2(1) 以降では、各 PVLAN トランク ポートに対するマッピングの数は最大 16 です。

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

（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。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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） スイッチ上に PVLAN モードで動作しているポートがある場合は、PVLAN をディセーブルにすることはできません。

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

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

プライベート VLAN としての VLAN の設定

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

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。

手順の概要

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

手順の詳細

	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、プライマリ VLAN を 1 つ設定する必要があります。 複数のコミュニティ VLAN と独立 VLAN を設定することができます。
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。

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

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

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

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

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

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

セカンダリVLAN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。 カンマ区切りの項目を複数指定することもできます。 各項目は、単一のセカンダリ VLAN ID、またはセカンダリ VLAN ID をハイフンでつないだ範囲にできます。
- *secondary-vlan-list* パラメータには、コミュニティ VALN ID を複数指定できるほか、独立 VLAN ID も 1 つ指定することができます。
- セカンダリ VLAN をプライマリ VLAN に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 VLAN とセカンダリ VLAN のいずれかを削除した場合、関連付けが設定されているポート上では、その VLAN は非アクティブになります。 **no private-vlan** コマンドを入力すると、VLAN は通常の VLAN モードに戻ります。 その VLAN におけるプライマリとセカンダリの関連付けはすべて一時停止されますが、インターフェイスは PVLAN モードのままです。 指定した VLAN を PVLAN モードに再変換すると、関連付けも元の状態に戻ります。

プライマリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN に関連付けられている PVLAN はすべて失われます。 ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN と PVLAN との関連付けは一時停止します。この VLAN を再作成して以前のセカンダリ VLAN として設定すると、関連付けは元の状態に戻ります。

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。

手順の概要

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

手順の詳細

	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。

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

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

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

（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。

手順の概要

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

手順の詳細

	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 のホスト ポートとして設定するポートを選択します。 このポートとしては、FEX のポートを選択できます（chassis オプションで指定）。
ステップ 3	switch(config-if)# **switchport mode private-vlan host**	選択したポートを PVLAN のホスト ポートとして設定します。
ステップ 4	switch(config-if)# **switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*}	選択したポートを、PVLAN のプライマリ VLAN とセカンダリ VLAN に関連付けます。 セカンダリ VLAN 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） PVLAN の関連付けをポートから削除します。

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たものです。

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

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

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。

手順の概要

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

手順の詳細

	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 の無差別ポートとして設定するポートを選択します。 物理インターフェイスが必要です。 このポートとして、FEX のポートを選択することはできません。
ステップ 3	switch(config-if)# **switchport mode private-vlan promiscuous**	選択したポートを PVLAN の無差別ポートとして設定します。 物理イーサネット ポートのみを、無差別ポートとしてイネーブルにできます。
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 から、マッピングをクリアします。

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

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

無差別トランク ポートの設定

PVLAN ドメインでは、無差別トランク ポートはプライマリ VLAN の一部です。 無差別トランク ポートでは、複数のプライマリ VLAN を伝送できます。 無差別トランク ポートには、同じプライマリ VLAN に従属する複数のセカンダリ VLAN をマップすることができます。

無差別ポートを設定する手順には 2 つのステップがあります。 1 つ目はポートを無差別ポートとして定義すること、2 つ目はセカンダリ VLAN とプライマリ VLAN とのマッピングを設定することです。 複数のマッピングを設定することにより、複数のプライマリ VLAN をイネーブルにすることができます。

（注） 各 PVLAN トランク ポートに対するマッピングの数は最大 16 です。

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。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 の無差別トランク ポートとして設定するポートを選択します。
ステップ 3	switch(config-if)# **switchport mode private-vlan trunk promiscuous**	選択したポートを PVLAN の無差別トランク ポートとして設定します。 物理イーサネット ポートのみを、無差別ポートとしてイネーブルにできます。 このポートとして、FEX のポートを選択することはできません。
ステップ 4	switch(config-if)# **switchport private-vlan mapping trunk** {*primary-vlan-id*} {*secondary-vlan-id*}	PVLAN のプライマリ VLAN およびセカンダリ VLAN に、選択したトランク ポートを関連付けます。 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。

	コマンドまたはアクション	目的
ステップ 5	switch(config-if)# **no switchport private-vlan mapping trunk** [*primary-vlan-id*]	（任意） ポートから PVLAN のマッピングを削除します。 *primary-vlan-id* が指定されない場合は、PVLAN のすべてのマッピングがポートから削除されます。

次の例は、イーサネット インターフェイス 1/1 を、PVLAN の無差別トランク ポートとして設定し、セカンダリ VLAN をプライマリ VLAN にマップする方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# switchport mode private-vlan trunk promiscuous
switch(config-if)# switchport private-vlan mapping trunk 5 100
switch(config-if)# switchport private-vlan mapping trunk 5 200
switch(config-if)# switchport private-vlan mapping trunk 6 300
```

独立トランク ポートの設定

PVLAN ドメインでは、独立トランクはセカンダリ VLAN の一部です。 独立トランク ポートは、複数の独立 VLAN を送受信できます。 指定されたプライマリ VLAN の 1 つの独立 VLAN のみを、独立トランク ポートに関連付けることができます。 独立トランク ポートを設定する手順には 2 つのステップがあります。 1 つ目はポートを独立トランク ポートとして定義すること、2 つ目は独立 VLAN とプライマリ VLAN の関連付けを設定することです。 複数の関連付けを設定することにより、複数の独立 VLAN をイネーブルにすることができます。

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。

手順の概要

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

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **interface** *type* [*chassis*/]*slot*/*port*	PVLAN の独立トランク ポートとして設定するポートを選択します。 このポートとしては、FEX のポートを選択できます（*chassis* オプションで指定）。
ステップ 3	switch(config-if)# **switchport mode private-vlan trunk** [**secondary**]	選択したポートを PVLAN のセカンダリ トランク ポートとして設定します。 （注） **secondary** キーワードは、指定しなかった場合でも指定したものと見なされます。
ステップ 4	switch(config-if)# **switchport private-vlan association trunk** {*primary-vlan-id*} {*secondary-vlan-id*}	PVLAN のプライマリ VLAN およびセカンダリ VLAN に、独立トランク ポートを関連付けます。 セカンダリ VLAN は独立 VLAN である必要があります。 特定のプライマリ VLAN の下でマップできる独立 VLAN は 1 つだけです。
ステップ 5	switch(config-if)# **no switchport private-vlan association trunk** [*primary-vlan-id*]	（任意） PVLAN の関連付けをポートから削除します。 *primary-vlan-id* が指定されない場合は、PVLAN のすべての関連付けがポートから削除されます。

次の例は、イーサネット インターフェイス 1/1 を、PVLAN の無差別トランク ポートとして設定し、セカンダリ VLAN をプライマリ VLAN にマップする方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# switchport mode private-vlan trunk secondary
switch(config-if)# switchport private-vlan association 5 100
switch(config-if)# switchport private-vlan association 6 200
```

FEX トランク ポートでのプライベート VLAN の設定

FEX トランク ポートでは PVLAN をイネーブルにしたりディセーブルにしたりすることができます。 FEX トランク ポートにより、PVLAN ドメインは、そこに接続されているすべてのホストに拡張されます。FEX トランク ポートを設定すると、Cisco NX-OS 5000 シリーズ スイッチに接続されているすべての FEX ポートがグローバルにその影響を受けます。

注意 FEX トランク ポートで PVLAN を設定する場合は、その前に FEX 独立トランク ポートをすべてディセーブルにしておく必要があります。 FEX 独立トランク ポートと FEX トランク ポートをともにイネーブルにすると、不要なネットワーク トラフィックが発生することがあります。

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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **system private-vlan fex trunk**
3. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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)# **system private-vlan fex trunk**	FEX トランク ポートで PVLAN 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、変更を継続的に保存します。

次の例は、FEX トランク ポートで PVLAN を設定する方法を示したものです。

```
switch# configure terminal
switch(config)# system private-vlan fex trunk
switch(config)# copy running-config startup-config
```

PVLAN トランキング ポートの許可 VLAN の設定

独立トランク ポートおよび無差別トランク ポートでは、PVLAN とともに通常の VLAN のトラフィックを伝送することができます。

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。

手順の概要

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

手順の詳細

	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 のホスト ポートとして設定するポートを選択します。このポートとしては、FEX のポートを選択できます（chassis オプションで指定）。
ステップ 3	switch(config-if)# **switchport private-vlan trunk allowed vlan** {*vlan-list* | **all** | **none** [**add** | **except** | **none** | **remove** {*vlan-list*}]}	プライベート トランク インターフェイスの許可 VLAN を設定します。 デフォルトの場合、PVLAN トランク インターフェイスで許可されるのは、マップされた VLAN または関連付けられた VLAN のみです。 （注） プライマリ VLAN は、許容 VLAN リストに明示的に追加する必要はありません。 プライマリ VLAN とセカンダリ VLAN との間で 1 回マッピングされると、自動的に追加されます。

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

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

プライベート VLAN でのネイティブ 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。 この設定によって、タグなしトラフィックおよび制御トラフィックは Cisco Nexus 5000 シリーズ スイッチを通過することができます。 セカンダリ VLAN は、無差別トランク ポートではネイティブ VLAN ID で設定できません。 プライマリ VLAN は、独立トランク ポートではネイティブ VLAN ID で設定できません。

（注） 1 つのトランクにより、複数の VLAN のトラフィックを伝送することができます。 ネイティブ VLAN に属するトラフィックは、トランクを通過する際カプセル化されません。他の VLAN のトラフィックは、それが属している VLAN を識別するためのタグでカプセル化されます。

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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** *type* [*chassis*/]*slot*/*port*
3. switch(config-if)# **switchport private-vlan trunk native** {**vlan** *vlan-id*}
4. （任意） switch(config-if)# **no switchport private-vlan trunk native** {**vlan** *vlan-id*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 のホスト ポートとして設定するポートを選択します。 このポートとしては、FEX のポートを選択できます（chassis オプションで指定）。
ステップ 3	switch(config-if)# **switchport private-vlan trunk native** {**vlan** *vlan-id*}	PVLAN トランクのネイティブ VLAN ID を設定します。 デフォルトは VLAN 1 です。
ステップ 4	switch(config-if)# **no switchport private-vlan trunk native** {**vlan** *vlan-id*}	（任意） PVLAN トランクからネイティブ VLAN ID を削除します。

プライベート VLAN 設定の確認

PVLAN の設定情報を表示する場合は、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。

次の例は、PVLAN 設定の表示方法を示したものです。

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

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

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

第 6 章

Cisco IP Phone サポートの設定

この章の内容は、次のとおりです。

Cisco IP Phone の概要

Cisco IP Phone は、統合型 3 ポート内蔵 10/100 スイッチを装備しています。 各ポートは、次のデバイスとの接続専用です。

- ポート 1 は、スイッチに接続します。
- ポート 2 は、内蔵 10/100/1000 インターフェイスで、Cisco IP Phone トラフィックを伝送します。
- ポート 3 は、PC またはその他のデバイスに接続します。

Cisco IP Phone の音声トラフィック

Cisco IP Phone は、音声トラフィックをレイヤ 3 の IP precedence 値およびレイヤ 2 の CoS 値と一緒に伝送します。この値はどちらもデフォルトで 5 に設定されています。 Cisco IP Phone 通話の音質は、音声トラフィックが不均一に送信される場合、劣化する可能性があります。

接続された Cisco IP Phone のレイヤ 2 アクセス ポートについては、音声トラフィック用として 1 つの VLAN を使用し、Cisco IP Phone に接続されたデバイスからのデータ トラフィック用として別の VLAN を使用するように設定することができます。

スイッチ上のレイヤ 2 アクセス ポートについては、Cisco Discovery Protocol（CDP）パケットを送信するように設定することができます。接続された Cisco IP Phone では、これらの CDP パケットの指示に基づき、次のいずれかの方法により音声トラフィックがスイッチへ送信されます。

- レイヤ 2 CoS プライオリティ値によるタグ付きの音声 VLAN による送信。
- レイヤ 2 CoS プライオリティ値によるタグ付きのアクセス VLAN による送信。
- タグなし（レイヤ 2 CoS プライオリティ値なし）のアクセス VLAN による送信。

（注） いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値（音声トラフィックはデフォルトで 5、音声制御トラフィックは 3）を伝送します。

Cisco IP Phone のデータ トラフィック

（注） Cisco IP Phone に接続されているデバイスからのタグなしトラフィックは、Cisco IP Phone のアクセス ポートの信頼状態にかかわらず、そのまま Cisco IP Phone を通過します。

Cisco IP Phone 上のアクセス ポートに接続されたデバイスからのタグ付きデータ トラフィック（フレーム タイプが 802.1Q または 802.1p のトラフィック）を処理する場合は、スイッチ上のレイヤ 2 アクセス ポートから CDP パケットが送信されるよう設定します。接続された Cisco IP Phone では、これらの CDP パケットの指示に基づいて、Cisco IP Phone 上のアクセス ポートが次のいずれかのモードに設定されます。

- 信頼モード：Cisco IP Phone のアクセス ポートを介して受信したトラフィックはすべて、そのまま Cisco IP Phone を通過します。
- 信頼できないモード：Cisco IP Phone のアクセス ポートを介して受信した 802.1Q フレームまたは 802.1p フレームのトラフィックはすべて、設定されたレイヤ 2 CoS 値でマーキングされます。 デフォルトのレイヤ 2 CoS 値は 0 です。 信頼できないモードがデフォルト設定です。

Cisco IP Phone の電源構成

ここでは、Cisco IP Phone 電源構成について説明します。

- Cisco IP Phone へのローカル電力供給
- Cisco IP Phone へのインライン パワー供給

Cisco IP Phone へのローカル電力供給

ローカル電源には 2 種類あります。

- Cisco IP Phone に接続されている電源装置

- Cisco IP Phone に接続されているツイストペア イーサネット ケーブルを通じてパッチ パネルを経由する電源装置

Cisco IP Phoneが、スイッチング モジュールのポート上でローカルに電力が供給されている場合、スイッチング モジュールはその存在を検出できません。 スーパーバイザ エンジンは、Cisco IP Phone の CDP メッセージを通じて Cisco IP Phone を検出します。

ローカルに電力が供給されているCisco IP Phoneがローカル電力を失った場合、そのモードがauto に設定されていると、スイッチング モジュールはその Cisco IP Phone を検出しスーパーバイザ エンジンにそれを通知したうえで、その Cisco IP Phone にインライン パワーを供給します。

Cisco IP Phone へのインライン パワー供給

インライン パワーは、インライン パワー ドーター カードをサポートするスイッチング モジュールにより供給される電力です。 インライン パワーは、ツイストペア イーサネット ケーブルを通じて Cisco IP Phone に供給されます。

（注） インライン パワーをサポートするスイッチング モジュールの詳細については、『Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes for Cisco NX-OS Release 5.0(3)N2(1)』を参照してください。 URL は、http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/ol_4164.htm です。

スイッチング モジュール ポートは、電力が供給されていない Cisco IP Phone を検出すると、スーパーバイザ エンジンに対して、電力が供給されていない Cisco IP Phone が存在すること、およびそれがどのモジュールおよびポートにあるかを通知します。 そのポートがauto モードに設定されている場合、スーパーバイザエンジンは、Cisco IP Phoneを動かすのに十分なシステム電力があるかどうかを判定します。 十分な電力がある場合は、スーパーバイザエンジンが、利用可能なシステム総電力量から、Cisco IP Phoneが必要とするデフォルトの電力割り当て量を差し引き、電力をポートに供給するように指示するメッセージをスイッチング モジュールに対して送信します。 Cisco IP Phoneに供給できる電力が不十分な場合、スーパーバイザエンジンは、ポートに電力を供給できないことを伝えるメッセージをスイッチング モジュールに送信します。

所要電力量はCisco IP Phoneによって異なる場合があります。 スーパーバイザ エンジンは最初に、デフォルトで設定されている 7 W（42 V で 167 mA）を、Cisco IP Phone に割り当てます。 Cisco IP Phone との CDP メッセージ交換によって正確な電力量が特定された段階で、スーパーバイザ エンジンは割り当て電力を加減します。

たとえば、デフォルトの電力割り当て量は 7 W です。 6.3 W を必要とする Cisco IP Phone がポートに接続されているとします。 スーパーバイザ エンジンは、この Cisco IP Phone に 7 W を割り当てた後、その電源をオンにします。 Cisco IP Phoneがいったん動作すれば、実際の所要電力量に関する CDP メッセージがスーパーバイザ エンジンに送信されます。 スーパーバイザ エンジンは電力割り当て量を所要量まで減らします。

Cisco IP Phone の電源を CLI または SNMP を通じてオフにしたり、取り外したりする場合、スーパーバイザエンジンはスイッチングモジュールに、ポートの電源をオフにするようにメッセージを送信します。 その分の電力は利用可能なシステム電力に戻されます。

注意 Cisco IP Phone のケーブルをポートに接続し、電源をオンにすると、スーパーバイザ エンジンは回線上でリンクがアップするまで 4 秒間待機します。 この 4 秒の間に Cisco IP Phone のケーブルを取り外しネットワーク デバイスを接続すると、そのネットワーク デバイスが破損することがあります。 ネットワーク デバイスを取り外し、別のネットワーク デバイスを接続する場合は、10 秒以上待機してから行うようにしてください。

音声トラフィックのサポートの設定

Cisco IP Phone による音声トラフィックの伝送方法を設定することができます。

- 音声 VLAN ID：CDP パケットを送信し、音声トラフィックを音声 VLAN ID およびレイヤ 2 CoS 値（デフォルトは 5）によるタグ付き 802.1Q フレームで伝送するように Cisco IP Phone を設定します。 指定できる VLAN ID は 1 ～ 4093 です。 スイッチは 802.1Q 音声トラフィックを音声 VLAN に入れます。
- dot1p：CDP パケットを送信し、音声トラフィックを VLAN ID 0 およびレイヤ 2 CoS 値（音声トラフィックに対するデフォルトは 5、音声制御トラフィックに対するデフォルトは 3）によるタグ付き 802.1p フレームで伝送するように Cisco IP Phone を設定します。 スイッチは 802.1p 音声トラフィックをアクセス VLAN に送ります。
- untagged：CDP パケットを送信し、タグなしの音声トラフィックを伝送するように Cisco IP Phone を設定します。 スイッチはタグなし音声トラフィックをアクセス VLAN に入れます。

いずれの設定の場合も、音声トラフィックによりレイヤ 3 IP precedence 値（デフォルトは 5）が伝送されます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet** *slot/port*
3. switch(config-if)# **switchport voice vlan** { *vlan-list* | **dotip** | **untagged** }
4. switch(config-if)# **exit**
5. （任意） switch(config-if)# **no switchport voice vlan**
6. （任意） switch# **show interfaces ethernet** *slot/port* **switchport**

手順の詳細

	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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **interface ethernet** *slot/port*	設定するポートを選択し、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 voice vlan** { *vlan-list* | **dotip** | **untagged** }	Cisco IP Phone が音声トラフィックを伝送する方法を設定します。 • vlan-list：VLAN ID を指定します。 有効な範囲は 1 ～ 3967 および 4048 ～ 4093 です。 • dot1p：これを指定すると、Cisco IP Phone ではプライオリティ タギングが使用され、音声トラフィックの 802.1P VLAN ID の値として 0 が使用されます。 • untagged：これを指定すると、Cisco IP Phone では音声トラフィックのフレームがタグ付けされません。
ステップ 4	switch(config-if)# **exit**	コンフィギュレーション モードを終了します。
ステップ 5	switch(config-if)# **no switchport voice vlan**	（任意） 設定を消去します。
ステップ 6	switch# **show interfaces ethernet** *slot/port* **switchport**	（任意） 音声トラフィックに関する設定を表示します。

次の例は、VLAN 3 を音声 VLAN として設定する方法を示したものです。

```
switch# config t
switch(config)# interface ethernet 1/28
switch(config-if)# switchport voice vlan 3
switch(config-if)#
```

次の例は、CDP パケットが送信されるようイーサネット ポートを設定する方法を示したものです。この CDP パケットの指示により、Cisco IP Phone からは音声トラフィックが 802.1p フレームで伝送されます。

```
switch# config t
switch(config)# interface ethernet 1/28
switch(config-if)# switchport voice vlan dot1p
switch(config-if)#
```

次の例は、CDP パケットが送信されるようイーサネット ポートを設定する方法を示したものです。この CDP パケットの指示により、Cisco IP Phone からはタグなしの音声トラフィックが伝送されます。

```
switch# config t
switch(config)# interface ethernet 1/28
switch(config-if)# switchport voice vlan untagged
switch(config-if)#
```

次の例は、イーサネット ポートの音声トラフィックを停止する方法を示したものです。

```
switch# config t
switch(config)# interface ethernet 1/28
switch(config-if)# no switchport voice vlan
switch(config-if)#
```

データ トラフィックのサポートの設定

Cisco IP Phone によるデータ トラフィックの伝送方法を設定することができます。

Cisco IP Phone によるデータ トラフィックの伝送方法を設定する際は、次の点に注意してください。

- CDP パケットを送信して、Cisco IP Phone 上のアクセス ポートと接続しているデバイスから受信したタグ付きトラフィックを Cisco IP Phone が信頼するように設定する場合は、cos キーワードおよび CoS 値を入力しないでください。
- CDP パケットを送信して、Cisco IP Phone 上のアクセス ポートと接続しているデバイスから受信したタグ付き入力トラフィックを Cisco IP Phone がマーキングするように設定する場合は、cos キーワードおよび CoS 値を入力してください（有効な値は 0 ～ 7 です）。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet** *slot/port*
3. switch(config-if)# **switchport voice vlan** { *vlan-list* | **dotip** | **untagged** }
4. switch(config-if)# **exit**
5. （任意） switch(config-if)# **no switchport voice vlan**
6. （任意） switch# **show interfaces ethernet** *slot/port* **switchport**

手順の詳細

	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*	設定するポートを選択し、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 voice vlan** { *vlan-list* | **dotip** | **untagged** }	Cisco IP Phone が音声トラフィックを伝送する方法を設定します。 • vlan-list：VLAN ID を指定します。 有効な範囲は 1 ～ 3967 および 4048 ～ 4093 です。

	コマンドまたはアクション	目的
		• dot1p：これを指定すると、Cisco IP Phone ではプライオリティ タギングが使用され、音声トラフィックの 802.1P VLAN ID の値として 0 が使用されます。 • untagged：これを指定すると、Cisco IP Phone では音声トラフィックのフレームがタグ付けされません。
ステップ 4	switch(config-if)# **exit**	コンフィギュレーション モードを終了します。
ステップ 5	switch(config-if)# **no switchport voice vlan**	（任意） 設定を消去します。
ステップ 6	switch# **show interfaces ethernet** *slot/port* **switchport**	（任意） 音声トラフィックに関する設定を表示します。

次の例は、タグ付きデータ トラフィックが信頼されるように Cisco IP Phone ポートを設定する方法を示したものです。

```
switch# config t
switch(config)# interface ethernet 1/28
switch(config-if)# switchport priority extend trust
switch(config-if)#
```

次の例は、データ トラフィックが CoS 値でマーキングされるように Cisco IP Phone ポートを設定する方法を示したものです。

```
switch# config t
switch(config)# interface ethernet 1/28
switch(config-if)# switchport priority extend cos 3
switch(config-if)#
```

次に、デフォルト設定に戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 1/28
switch(config-if)# no switchport priority extend
switch(config-if)#
```

インライン パワー サポートの設定

スイッチ上の Power over Ethernet（POE）ポートをイネーブルにしたりディセーブルにしたりすることができます。デフォルトでは、電源の割り当てが自動で行われます（auto）。各 POE ポートのデフォルトの電力は 15,400 mW です。

power inline auto コマンドを使用してポートの設定を行うと、そのポートでは、設定された速度およびデュプレックス設定に従って自動ネゴシエーションが実行され、（受電デバイスかどうかにかかわらず）接続されたデバイスの所要電力が特定されます。所要電力が特定されると、スイッ

チではインターフェイスをリセットすることなく、設定された速度およびデュプレックス設定に従ってインターフェイスのハードコードが行われます。

power inline never コマンドを使用してポートの設定を行うと、POE 対応ポートの検出および電力供給がディセーブルになり、そのポートは設定された速度およびデュプレックス設定に戻ります。

はじめる前に

POE 機能がイネーブルであることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature poe**
3. switch(config)# **interface ethernet** *slot/port*
4. switch(config-if)# **power inline** {{**auto** | **static** }[**max** *max-value*] | **never** }
5. switch(config-if)# **exit**
6. （任意） switch(config-if)# **no power inline**
7. （任意） switch# **show power inline ethernet** *slot/port*
8. （任意） switch(config)# **logging level poed***0-7*

手順の詳細

	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 poe**	スイッチの POE モードをイネーブルにします。
ステップ 3	switch(config)# **interface ethernet** *slot/port*	設定するポートを選択し、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)# **power inline** {{**auto**	**static** }[**max** *max-value*]	**never** }	インライン パワー サポートを設定します。 • auto：受電デバイス（PD）検出を設定します。十分な電力がある場合は、デバイスの検出後POEポートに電力を自動で割り当てることができます。 • static：これを指定すると、インライン パワー インターフェイスが最優先されます。 • max-value：（任意）インターフェイスごとの最大電力を設定します。設定できる最大電力の値は、4000 ～ 30000 mW です。 • never：デバイス検出とポートへの電力供給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 5	switch(config-if)# **exit**	コンフィギュレーション モードを終了します。
ステップ 6	switch(config-if)# **no power inline**	（任意） 設定を消去します。
ステップ 7	switch# **show power inline ethernet** *slot/port*	（任意） すべての POE ポートまたは指定した POE ポートに関する設定を表示します。
ステップ 8	switch(config)# **logging level poed***0-7*	（任意） POE イベント ロギングをイネーブルにします。

次の例は、POE の検出をディセーブルにし、POE ポートへの電力供給を停止する方法を示したものです。

```
switch# config t

switch(config)# interface ethernet 100/1/1
switch(config-if)# power inline never
switch(config-if)##
```

次の例は、POE の検出をイネーブルにし、POE ポートに対し自動で電力供給を行う方法を示したものです。

```
switch# config t

switch(config)# interface ethernet 100/1/1
switch(config-if)# power inline auto
switch(config-if)#
```

次の例は、イーサネット ポート 100/5/1 のインライン パワー設定を確認する方法を示したものです。

```
witch# show power inline ethernet 100/5/1
Interface  Admin    Oper     Power        Device
                            (Watts)
---------- ----- ---------- ------- --------------------
Eth5/1      auto  on           6.3   cisco phone device
```

次の例は、POE ロギング重大度の設定を表示する方法を示したものです。

```
switch# show logging level poed
Facility     Default Severity      Current Session Severity
--------     ----------------      ------------------------
poe                  5                       5
0(emergencies)     1(alerts)       2(critical)
3(errors)          4(warnings)     5(notifications)
6(information)     7(debugging)
```

第 7 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

この章の内容は、次のとおりです。

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

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

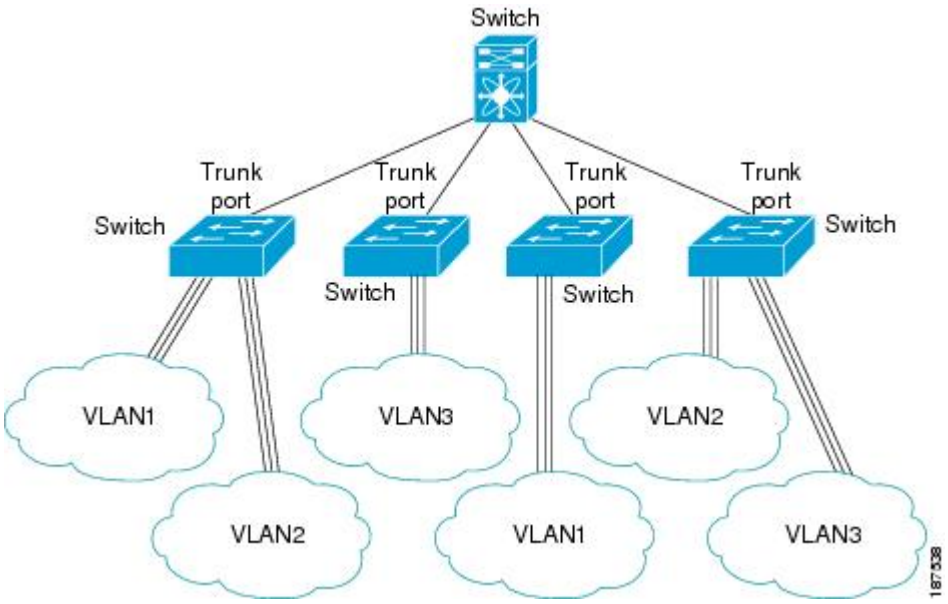
イーサネット インターフェイスは、次のように、アクセス ポートまたはトランク ポートとして設定できます。

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

図 *5*：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。

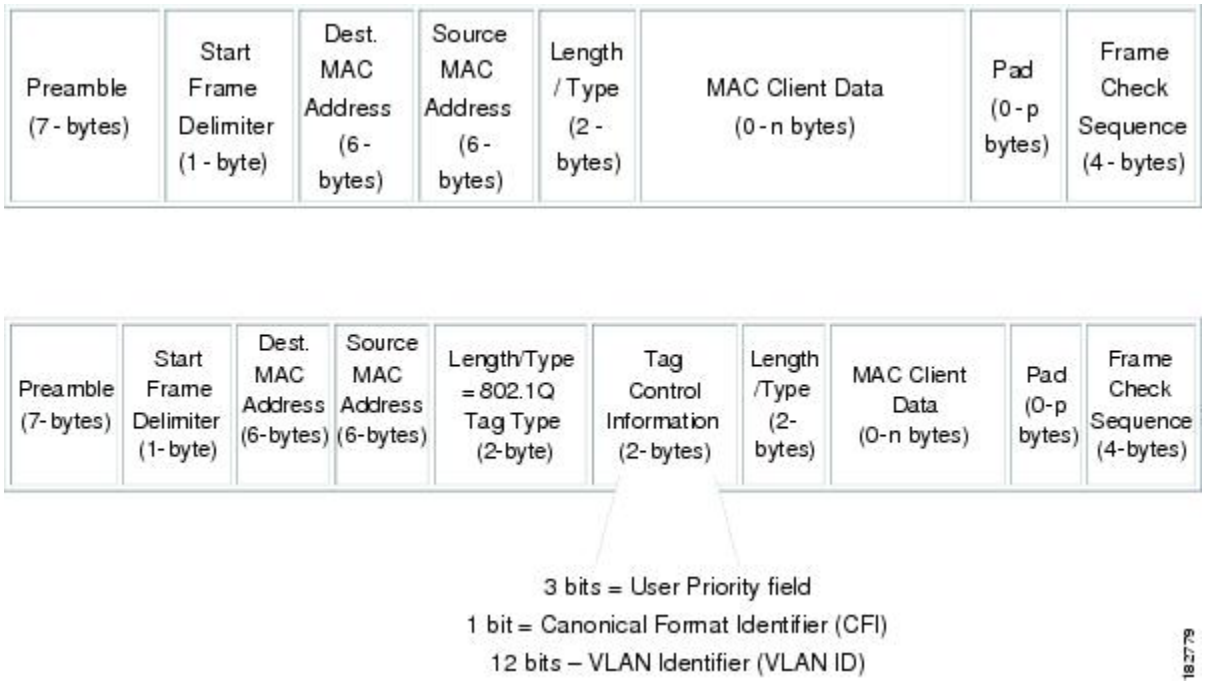
（注） イーサネット インターフェイスはアクセス ポートまたはトランク ポートとして動作できますが、両方のポート タイプとして同時に動作することはできません。

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 *6*：*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 の収束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高めるため、**vlan dot1q tag native** コマンドが導入されました。 この機能により、802.1Q トランク ポートから送信されるすべての

パケットが必ずタグ付けされるとともに、タグなしのパケットが 802.1Q トランク ポートで受信されないようにすることができるようになりました。

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

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

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

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

この機能は、直接接続されている Cisco Nexus 5000 シリーズ スイッチのすべてのイーサネット 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ています。 また、接続されている FEX のすべてのホスト インターフェイス ポートでもサポートされています。

（注） **vlan dot1q tag native** コマンドは、グローバル コンフィギュレーション モードで発行することによりイネーブルにすることができます。

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。

手順の概要

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

手順の詳細

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

はじめる前に

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

手順の概要

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

手順の詳細

	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 ポート タイプ エッジに設定し、BPDU フィルタリングおよび BPDU ガードをオンにします。 （注） このコマンドは、ホストに接続されたスイッチポートに対してのみ使用してください。

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。

手順の概要

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

手順の詳細

	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 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。

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

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

802.1Q トランク ポートのネイティブ VLAN の設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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。

	コマンドまたはアクション	目的
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。

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

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

トランキング ポートの許可 VLAN の設定

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

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

手順の概要

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

手順の詳細

	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。

	コマンドまたはアクション	目的
		（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。

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

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

ネイティブ 802.1Q VLAN の設定

通常は、ネイティブ VLAN ID で 802.1Q トランクを設定します。これによって、その VLAN 上のすべてのパケットからタギングが取り除かれます。 この設定によって、タグなしトラフィックおよび制御トラフィックは Cisco Nexus 5000 シリーズ スイッチを通過することができます。 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場合は、**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、トラフィック ポートのネイティブ VLAN のタグなし制御トラフィックは引き続き許可されます。

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

手順の概要

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

手順の詳細

	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 5000 シリーズ スイッチ上の全トランキング ポートを対象に、そのネイティブ VLAN すべてに対して dot1q（IEEE 802.1Q）タギングをイネーブルにします。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） スイッチ上の全トランキング ポートを対象に、そのネイティブ VLAN すべてに対して dot1q（IEEE 802.1Q）タギングをイネーブルにします。
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。

次の例は、スイッチ上の 802.1Q タギングをイネーブルにする方法を示したものです。

```
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。
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 8 章

ポート チャネルの設定

この章の内容は、次のとおりです。

ポート チャネルについて

ポート チャネルは、最大 16 個のインターフェイスを 1 つのグループにバンドルしたもので、帯域幅を広げ冗長性を高めることができます。 これらの集約された各物理インターフェイス間でトラフィックのロード バランシングも行います。 ポート チャネルの物理インターフェイスが少なくとも 1 つ動作していれば、そのポート チャネルは動作しています。

ポートチャネルは、互換性のあるインターフェイスをバンドルすることによって作成します。 スタティック ポート チャネルのほか、Link Aggregation Control Protocol（LACP）を実行するポートチャネルを設定して稼働させることができます。

変更した設定をポート チャネルに適用すると、そのポート チャネルのメンバ インターフェイスにもそれぞれ変更が適用されます。 たとえば、スパニングツリー プロトコル（STP）のパラメータをポート チャネルに設定すると、Cisco NX-OS ソフトウェアでは、これらのパラメータがポート チャネルの各インターフェイスに適用されます。

関連するプロトコルを使用せず、スタティック ポートチャネルを使用すれば、設定を簡略化できます。 IEEE 802.3ad に規定されている Link Aggregation Control Protocol（LACP）を使用すると、ポート チャネルをより効率的に使用することができます。 LACP を使用すると、リンクによってプロトコル パケットが渡されます。

関連トピック

LACP の概要，（106 ページ）

ポート チャネルの概要

Cisco NX-OS は、ポート チャネルを使用することにより、広い帯域幅、冗長性、チャネル全体のロード バランシングを実現しています。

最大 16 個のポートを 1 つのスタティック ポート チャネルに集約することができるほか、Link Aggregation Control Protocol（LACP）をイネーブルにすることもできます。 LACP によるポート チャネルを設定する手順は、スタティック ポート チャネルの場合とは若干異なります。

（注） Cisco NX-OS は、ポート チャネルに対するポート集約プロトコル（PAgP）をサポートしていません。

ポート チャネルは、個々のリンクを 1 つのチャネル グループにバンドルしたもので、それにより最大 16 個の物理リンクの帯域幅を集約した単一の論理リンクが作成されます。 ポート チャネル内のメンバー ポートに障害が発生すると、障害が発生したリンクで伝送されていたトラフィックはポート チャネル内のその他のメンバー ポートに切り替わります。

各ポートにはポート チャネルが 1 つだけあります。 ポート チャネル内のすべてのポートには互換性が必要です。つまり、回線速度が同じであり、かつ全二重方式で動作する必要があります。スタティック ポート チャネルを LACP なしで稼働すると、個々のリンクがすべて on チャネル モードで動作します。このモードを変更するには、LACP をイネーブルにする必要があります。

（注） チャネル モードを、on から active、または on から passive に変更することはできません。

ポート チャネル インターフェイスを作成することで、ポート チャネルを直接作成することができます。またチャネル グループを作成して個々のポートを 1 つに集約することもできます。 インターフェイスをチャネル グループに関連付ける際、ポート チャネルがなければ、Cisco NX-OSでは対応するポート チャネルが自動的に作成されます。 最初にポート チャネルを作成することもできます。 その場合、Cisco NX-OS では、ポート チャネルと同じチャネル数で空のチャネル グループが作成され、デフォルトの設定が適用されます。

（注） 少なくともメンバ ポートの 1 つがアップしており、かつそのポートのチャネルが有効であれば、ポート チャネルは動作上アップ状態にあります。 メンバ ポートがすべてダウンしていれば、ポート チャネルはダウンしています。

ポート チャネルの設定に関する注意事項と制約事項

ポート チャネルは、グローバル コンフィギュレーション モードまたはスイッチ プロファイル モードのいずれかで設定することができます。 Cisco NX-OS の設定同期化機能を介してポート チャネルの設定を行う際には、次の注意事項および制約事項を考慮してください。

- いったんスイッチ プロファイル モードで設定したポート チャネルを、グローバル コンフィギュレーション（config terminal）モードで設定することはできません。

（注） ポート チャネルに関する一部のサブコマンドは、スイッチ プロファイル モードでは設定できません。 ただしこれらのコマンドは、ポート チャネルがスイッチ プロファイル モードで作成、設定されている場合でも、グローバル コンフィギュレーション モードからであれば設定することができます。

たとえば、次のコマンドはグローバル コンフィギュレーション モードでのみ設定可能です。

switchport private-vlan association trunk *primary-vlan secondary-vlan*

- shutdown および no shutdown は、グローバル コンフィギュレーション モードとスイッチ プロファイル モードのどちらでも設定できます。
- ポート チャネルをグローバル コンフィギュレーション モードで作成した場合は、メンバ インターフェイスを含むチャネル グループも、グローバル コンフィギュレーション モードを使用して作成する必要があります。
- スイッチ プロファイル モードで設定されたポート チャネルには、スイッチ プロファイルの内部と外部どちらからもメンバにすることができます。
- メンバ インターフェイスをスイッチ プロファイルにインポートする場合は、そのメンバ インターフェイスに対応するポート チャネルがスイッチ プロファイル内に存在する必要があります。

スイッチ プロファイルの詳細については、『*Cisco NX-OS 5000 System Management Configuration Guide*』を参照してください。

互換性要件

ポート チャネル グループにインターフェイスを追加すると、Cisco NX-OS では、そのインターフェイスとチャネル グループとの互換性が確保されるように、特定のインターフェイス属性のチェックが行われます。 また Cisco NX-OS では、インターフェイスがポート チャネル集約に加えられることを許可する場合にも、事前にそのインターフェイスに関するさまざまな動作属性のチェックが行われます。

互換性チェックの対象となる動作属性は次のとおりです。

- ポート モード
- アクセス VLAN
- トランク ネイティブ VLAN
- 許可 VLAN リスト
- 速度

- 802.3x フロー制御設定
- MTU

  Cisco Nexus 5000 シリーズ スイッチでは、システム レベルの MTU のみサポートされます。この属性を個々のポートごとに変更できません。
- ブロードキャスト/ユニキャスト/マルチキャスト ストーム制御設定
- プライオリティ フロー制御
- タグなし CoS

Cisco NX-OS で使用される互換性チェックの全リストを表示する場合は、**show port-channel compatibility-parameters** コマンドを使用します。

チャネル モードセットを on に設定したインターフェイスだけをスタティック ポート チャネルに追加できます。 また LACP を実行するポート チャネルには、チャネル モードが active または passive に設定されたインターフェイスだけを追加することもできますこれらの属性は個別のメンバ ポートに設定できます。

インターフェイスがポートチャネルに追加されると、次の各パラメータはそのポートチャネルに関する値に置き換えられます。

- 帯域幅
- MAC アドレス
- STP

インターフェイスがポートチャネルに追加されても、次に示すインターフェイス パラメータは影響を受けません。

- 説明
- CDP
- LACP ポート プライオリティ
- デバウンス

channel-group force コマンドを使用して、ポートをチャネル グループへ強制的に追加できるようにした場合、パラメータは次のように処理されます。

- インターフェイスがポートチャネルに追加されると、次のパラメータは削除され、代わってポートチャネルに関する値が指定されます。ただしこの変更は、インターフェイスに関する実行コンフィギュレーションには反映されません。
  - QoS
  - 帯域幅
  - 遅延
  - STP
  - サービス ポリシー

- ACL

- インターフェイスがポート チャネルに追加またはポート チャネルから削除されても、次のパラメータはそのまま維持されます。
  - ビーコン
  - 説明
  - CDP
  - LACP ポート プライオリティ
  - デバウンス
  - UDLD
  - シャットダウン
  - SNMP トラップ

ポート チャネルを使ったロード バランシング

Cisco NX-OS では、フレーム内のアドレスから生成されたバイナリ パターンの一部を数値に圧縮変換し、それを基にチャネル内のリンクを 1 つ選択することによって、ポート チャネルを構成するすべての動作中インターフェイス間でトラフィックのロードバランシングが行われます。ポートチャネルではデフォルトでロードバランシングが行われます。また、基本設定では、次の基準によってリンクが選択されます。

- レイヤ 2 フレームの場合は、送信元および宛先の MAC アドレスを使用します。
- レイヤ 3 フレームの場合は、送信元および宛先の MAC アドレスと送信元および宛先の Internet Protocol（IP）アドレスを使用します。
- レイヤ 4 フレームの場合は、送信元および宛先の MAC アドレスと送信元および宛先の IP アドレスを使用します。

（注） レイヤ 4 フレームに対しては、必要に応じて送信元および宛先のポート番号を指定することもできます。

次のいずれかに基づいてポートチャネル全体でのロードバランシングが行われるようにスイッチを設定することができます。

- 宛先 MAC アドレス
- 送信元 MAC アドレス
- 送信元および宛先 MAC アドレス
- 宛先 IP アドレス

- 送信元 IP アドレス
- 送信元および宛先 IP アドレス
- 宛先 TCP/UDP ポート番号
- 送信元 TCP/UDP ポート番号
- 送信元および宛先 TCP/UDP ポート番号

表 *5*：ポート チャネルにおけるロードバランシングの基準

設定	レイヤ 2 基準	レイヤ 3 基準	レイヤ 4 基準
宛先 MAC	宛先 MAC	宛先 MAC	宛先 MAC
送信元 MAC	送信元 MAC	送信元 MAC	送信元 MAC
送信元/宛先 MAC	送信元/宛先 MAC	送信元/宛先 MAC	送信元/宛先 MAC
宛先 IP	宛先 MAC	宛先 MAC、宛先 IP	宛先 MAC、宛先 IP
送信元 IP	送信元 MAC	送信元 MAC、送信元 IP	送信元 MAC、送信元 IP
送信元/宛先 IP	送信元/宛先 MAC	送信元/宛先 MAC、送信元/宛先 IP	送信元/宛先 MAC、送信元/宛先 IP
宛先 TCP/UDP ポート	宛先 MAC	宛先 MAC、宛先 IP	宛先 MAC、宛先 IP、宛先ポート
送信元 TCP/UDP ポート	送信元 MAC	送信元 MAC、送信元 IP	送信元 MAC、送信元 IP、送信元ポート
送信元および宛先 TCP/UDP ポート	送信元/宛先 MAC	送信元/宛先 MAC、送信元/宛先 IP	送信元/宛先 MAC、送信元/宛先 IP、送信元/宛先ポート

ファブリック エクステンダの設定は個別には行えません。ファブリック エクステンダの設定は、Nexus 5000 シリーズで定義されます。 ポート チャネル ロード バランシング プロトコルにおいて、Nexus 5000 シリーズで設定された内容に応じてファブリック エクステンダ上で自動的に設定されるポート チャネル ロードバランシング オプションについては下記の表を参照してください。

次の表は、各設定の基準をまとめたものです。

表 *6*：***Cisco Nexus 2232*** ファブリック エクステンダおよび ***Cisco Nexus 2248*** ファブリック エクステンダにおけるポート チャネルでのロードバランシングの基準

設定	レイヤ 2 基準	レイヤ 3 基準	レイヤ 4 基準
宛先 MAC	送信元/宛先 MAC	送信元/宛先 MAC	送信元/宛先 MAC
送信元 MAC	送信元/宛先 MAC	送信元/宛先 MAC	送信元/宛先 MAC
送信元/宛先 MAC	送信元/宛先 MAC	送信元/宛先 MAC	送信元/宛先 MAC
宛先 IP	送信元/宛先 MAC	送信元/宛先 MAC、送信元/宛先 IP	送信元/宛先 MAC、送信元/宛先 IP
送信元 IP	送信元/宛先 MAC	送信元/宛先 MAC、送信元/宛先 IP	送信元/宛先 MAC、送信元/宛先 IP
送信元/宛先 IP	送信元/宛先 MAC	送信元/宛先 MAC、送信元/宛先 IP	送信元/宛先 MAC、送信元/宛先 IP
宛先 TCP/UDP ポート	送信元/宛先 MAC	送信元/宛先 MAC、送信元/宛先 IP	送信元/宛先 MAC、送信元/宛先 IP、送信元/宛先ポート
送信元 TCP/UDP ポート	送信元/宛先 MAC	送信元/宛先 MAC、送信元/宛先 IP	送信元/宛先 MAC、送信元/宛先 IP、送信元/宛先ポート
送信元および宛先 TCP/UDP ポート	送信元/宛先 MAC	送信元/宛先 MAC、送信元/宛先 IP	送信元/宛先 MAC、送信元/宛先 IP、送信元/宛先ポート

設定においてロードバランシングの基準が最多となるようなオプションを使用してください。たとえば、ポート チャネルのトラフィックが 1 つの MAC アドレスにだけ送られ、ポート チャネルでのロード バランシングの基準としてその宛先 MAC アドレスが使用されている場合、ポート チャネルでは常にそのポート チャネル内の同じリンクが選択されます。したがって、送信元アドレスまたはIPアドレスを使用すると、結果的により優れたロードバランシングが行われることになります。

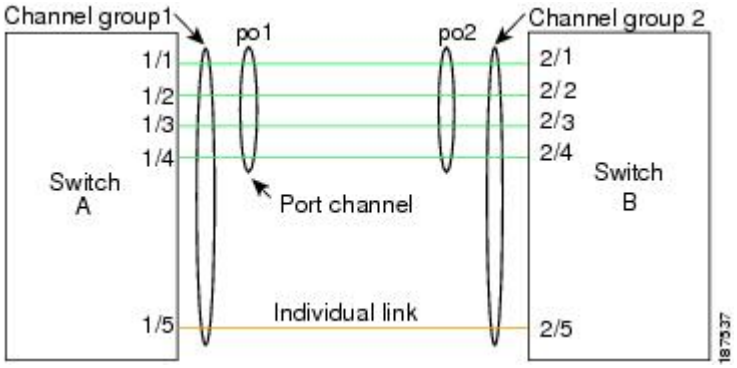
LACP の概要

LACP の概要

（注） LACP 機能を設定して使用にする場合は、あらかじめ LACP 機能をイネーブルにしておく必要があります。

次の図は、個々のリンクを個別リンクとして機能させるだけでなく LACP ポート チャネルおよびチャネル グループに組み込む方法を示したものです。

図 7：個々のリンクをポート チャネルに組み込む



LACP を使用すると、スタティック ポート チャネルの場合と同じように、最大 16 個のインターフェイスを 1 つのチャネル グループにバンドルすることができます。

（注） ポート チャネルを削除すると、関連付けられたチャネル グループも Cisco NX-OS によって自動的に削除されます。 すべてのメンバ インターフェイスは以前の設定に戻ります。

LACP 設定が 1 つでも存在する限り、LACP をディセーブルにはできません。

LACP ID パラメータ

LACP では次のパラメータが使用されます。

- LACP システム プライオリティ：LACP を稼働している各システムは、LACP システム プライオリティ値を持っています。 このパラメータのデフォルト値である 32768 をそのまま使用するか、1 ～ 65535 の範囲で値を設定できます。 LACP は、このシステム プライオリティと MAC アドレスを組み合わせてシステム ID を生成します。また、システム プライオリティを他のデバイスとのネゴシエーションにも使用します。 システム プライオリティ値が大きいほど、プライオリティは低くなります。

（注） LACP システム ID は、LACP システム プライオリティ値と MAC アドレスを組み合わせたものです。

- LACP ポート プライオリティ：LACP を使用するように設定された各ポートには、LACP ポート プライオリティが割り当てられます。デフォルト値である 32768 をそのまま使用するか、1 ～ 65535 の範囲で値を設定できます。 LACP では、ポート プライオリティおよびポート番号によりポート ID が構成されます。 また、互換性のあるポートのうち一部を束ねることができない場合に、どのポートをスタンバイ モードにし、どのポートをアクティブ モードにするかを決定するのに、ポート プライオリティを使用します。 LACP では、ポート プライオリティ値が大きいほど、プライオリティは低くなります。 指定ポートが、より低い LACP プライオリティを持ち、ホット スタンバイ リンクではなくアクティブ リンクとして選択される可能性が最も高くなるように、ポート プライオリティを設定できます。
- LACP 管理キー：LACP は、LACP を使用するように設定された各ポート上のチャネル グループ番号に等しい管理キー値を自動的に設定します。 管理キーにより、他のポートとともに集約されるポートの機能が定義されます。 他のポートとともに集約されるポートの機能は、次の要因によって決まります。
  - ポートの物理特性（データ レート、デュプレックス機能、ポイントツーポイントまたは共有メディア ステートなど）
  - ユーザが作成した設定に関する制約事項

チャネル モード

ポート チャネルの個別インターフェイスは、チャネル モードで設定します。 プロトコルを使用せずにスタティック ポート チャネルを稼働すると、そのチャネル モードは常に on に設定されます。 デバイス上で LACP をグローバルにイネーブルにした後、各チャネルの LACP をイネーブルにします。それには、各インターフェイスのチャネル モードを active または passive に設定します。 LACP チャネル グループを構成する個々のリンクについて、どちらかのチャネル モードを設定できます。

（注） active または passive のチャネル モードで、個々のインターフェイスを設定するには、まず、LACP をグローバルにイネーブルにする必要があります。

次の図は、チャネル モードをまとめたものです。

表 7: ポート チャネルにおける個々のリンクのチャネル モード

チャネル モード	説明
passive	ポートをパッシブなネゴシエーション状態にする LACP モード。この状態では、ポートは受信した LACP パケットに応答はしますが、LACP ネゴシエーションを開始することはありません。
active	ポートをアクティブ ネゴシエーション ステートにする LACP モード。この場合ポートでは LACPパケットを送信することにより、他のポートとのネゴシエーションが開始されます。
on	すべてのスタティック ポート チャネル（つまり LACP を稼働していないポート チャネル）は、このモードのままになります。 LACP をイネーブルにする前にチャネル モードを active または passive に変更しようとすると、デバイスがエラー メッセージを返します。 チャネルで LACP をイネーブルにするには、そのチャネルのインターフェイスでチャネル モードを active または passive に設定します。 LACP は、on状態のインターフェイスとネゴシエートする場合、LACP パケットを受信しないため、そのインターフェイスと個別のリンクを形成します。つまり、LACP チャネル グループには参加しません。

passive と active のどちらのモードでも、ポート速度やトランキング ステートなどの基準に基づいてポート チャネルを構成可能かどうかを判定するため、LACP によるポート間のネゴシエーションが行われます。 passive モードは、リモート システム、つまり、パートナーが、LACP をサポートしているかどうかが不明な場合に便利です。

次の例に示したとおり、ポートは、異なる LACP モードであっても、それらのモード間で互換性があれば、LACP ポート チャネルを構成することができます。

- active モードのポートは、active モードの別のポートとともにポート チャネルを正しく形成できます。
- active モードのポートは、passive モードの別のポートとともにポート チャネルを形成できます。
- passive モードのポート同士ではポート チャネルを構成できません。これは、どちらのポートもネゴシエーションを開始しないためです。

- on モードのポートは LACP を実行していません。

LACP マーカー レスポンダ

ポート チャネルを使用すると、リンク障害やロード バランシング動作に伴って、データ トラフィックが動的に再配信される場合があります。 LACP では、マーカー プロトコルを使用して、こうした再配信によってフレームが重複したり順序が変わったりしないようにします。 Cisco NX-OS は、マーカー レスポンダだけをサポートしています。

LACP がイネーブルのポート チャネルとスタティック ポート チャネルの相違点

次の表は、LACP がイネーブルのポート チャネルとスタティック ポート チャネルとの主な相違点をまとめたものです。

表 *8* : *LACP* がイネーブルのポート チャネルとスタティック ポート チャネル

構成	LACP がイネーブルにされた EtherChannel	スタティック EtherChannel
適用されるプロトコル	グローバルにイネーブル化	なし
リンクのチャネル モード	次のいずれか。 • Active • Passive	on モードのみ
チャネルを構成する最大リンク数	16	16

ポート チャネルの設定

ポート チャネルの作成

チャネル グループを作成する前にポート チャネルを作成します。 Cisco NX-OS は、対応するチャネル グループを自動的に作成します。

（注） LACP ベースのポート チャネルを使用する場合は、LACP をイネーブルにする必要があります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface port-channel** *channel-number*
3. switch(config)# **no interface port-channel** *channel-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 port-channel** *channel-number*	設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。指定できる範囲は 1 ～ 4096 です。チャネル グループがまだ存在していなければ、Cisco NX-OS によって自動的に作成されます。
ステップ 3	switch(config)# **no interface port-channel** *channel-number*	ポート チャネルを削除し、関連するチャネル グループを削除します。

次の例は、ポート チャネルの作成方法を示したものです。

```
switch# configure terminal
switch (config)# interface port-channel 1
```

ポート チャネルへのポートの追加

新規のチャネル グループ、または他のポートがすでに属しているチャネル グループにポートを追加できます。 ポート チャネルがない場合は、Cisco NX-OS によってこのチャネル グループに関連付けられたポート チャネルが作成されます。

（注） LACP ベースのポート チャネルを使用する場合は、LACP をイネーブルにする必要があります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port*
3. （任意） switch(config-if)# **switchport mode trunk**
4. （任意） switch(config-if)# **switchport trunk** {**allowed vlan** *vlan-id* | **native vlan** *vlan-id*}
5. switch(config-if)# **channel-group** *channel-number*
6. （任意） switch(config-if)# **no channel-group**

手順の詳細

	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*	チャネル グループに追加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 trunk**	（任意） 指定したインターフェイスをトランク ポートとして設定します。
ステップ 4	switch(config-if)# **switchport trunk** {**allowed vlan** *vlan-id* | **native vlan** *vlan-id*}	（任意） トランク ポートに必要なパラメータを設定します。
ステップ 5	switch(config-if)# **channel-group** *channel-number*	チャネル グループ内にポートを設定し、モードを設定します。 channel-number の指定できる範囲は 1 ～ 4096 です。 ポート チャネルがない場合は、Cisco NX-OS によってこのチャネル グループに関連付けられたポート チャネルが作成されます。 これを、暗黙的なポート チャネル作成と言います。
ステップ 6	switch(config-if)# **no channel-group**	（任意） チャネル グループからポートを削除します。チャネル グループから削除されたポートは元の設定に戻ります。

次に、イーサネット インターフェイス 1/4 をチャネル グループ 1 に追加する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# switchport mode trunk
switch(config-if)# channel-group 1
```

ポート チャネルを使ったロード バランシングの設定

デバイス全体に適用されるポート チャネル用のロードバランシング アルゴリズムを設定できます。

（注） LACP ベースのポート チャネルを使用する場合は、LACP をイネーブルにする必要があります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **port-channel load-balance ethernet** {[**destination-ip** | **destination-mac** | **destination-port** | **source-dest-ip** | **source-dest-mac** | **source-dest-port** | **source-ip** | **source-mac** | **source-port**] crc-poly}
3. （任意） switch(config)# **no port-channel load-balance ethernet**
4. （任意） switch# **show port-channel load-balance**

手順の詳細

	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)# **port-channel load-balance ethernet** {[**destination-ip** | **destination-mac** | **destination-port** | **source-dest-ip** | **source-dest-mac** | **source-dest-port** | **source-ip** | **source-mac** | **source-port**] crc-poly}	デバイスのロード バランシング アルゴリズムを指定します。指定可能なアルゴリズムはデバイスによって異なります。 デフォルトは source-dest-mac です。 Cisco NX-OS Release 5.0(3)N2(1) 以降、Cisco Nexus 5500 プラットフォーム スイッチでは、ハッシュ パラメータでの圧縮に使用できる 8 種類のハッシュ多項式がサポートされています。 ポート チャネルからの出力トラフィックに対するハッシュ パラメータの種類によっては、多項式が異なると負荷分散の結果も異なる場合があります。 デフォルトのハッシュ多項式は CRC8a です。 変数は次のように設定できます。 • CRC8a • CRC8b • CRC8c • CRC8d • CRC8e • CRC8f • CRC8g

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **no port-channel load-balance ethernet**	（任意） ロードバランシング アルゴリズムをデフォルトの source-dest-mac に戻します。
ステップ 4	switch# **show port-channel load-balance**	（任意） ポート チャネル ロードバランシング アルゴリズムを表示します。

次の例は、ポート チャネルに対して送信元 IP によるロード バランシングを設定する方法を示したものです。

```
switch# configure terminal
switch (config)# port-channel load-balance ethernet source-ip
```

（注） source-dest-ip、source-dest-mac、source-dest-port の各キーワードは、Cisco NX-OS の 4.0(1a)N1 より以前のリリースの場合、それぞれ source-destination-ip、source-destination-mac、source-destination-port です。

マルチキャスト トラフィックに対するハードウェア ハッシュの設定

デフォルトでは、スイッチのどのポートにおける入力マルチキャスト トラフィックでも、特定のポート チャネル メンバが選択され、トラフィックが出力されます。 マルチキャスト トラフィックに対してハードウェア ハッシュを設定すると、帯域幅について発生しうる問題を軽減することができるほか、入力マルチキャスト トラフィックの効率的なロードバランシングを実現することもできます。 ハードウェア ハッシュをイネーブルにする場合は、**hardware multicast hw-hash** コマンドを使用します。 デフォルトに戻す場合は、**no hardware multicast hw-hash** コマンドを使用します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface port-channel** *channel-number*
3. switch(config-if)# **hardware multicast hw-hash**

手順の詳細

	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 port-channel** *channel-number*	ポートチャネルを選択し、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)# **hardware multicast hw-hash**	指定したポート チャネルに対してハードウェア ハッシュを設定します。

次の例は、ポート チャネルに対してハードウェア ハッシュを設定する方法を示したものです。

```
switch# configure terminal
switch (config)# interface port-channel 21
switch(config-if)# hardware multicast hw-hash
```

次の例は、ポート チャネルからハードウェア ハッシュを削除する方法を示したものです。

```
switch# configure terminal
switch (config)# interface port-channel 21
switch(config-if)# no hardware multicast hw-hash
```

LACP のイネーブル化

LACP はデフォルトではディセーブルです。LACP の設定を開始するには、LACP をイネーブルにする必要があります。 LACP 設定が 1 つでも存在する限り、LACP をディセーブルにはできません。

LACP は、LAN ポート グループの機能を動的に学習し、残りの LAN ポートに通知します。 LACP では、適合する複数のイーサネット リンクが検出されると、これらのリンクが 1 つのポート チャネルにグループ化されます。 次に、ポート チャネルは単一ブリッジ ポートとしてスパニングツリーに追加されます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature lacp**
3. （任意） switch(config)# **show feature**

手順の詳細

	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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **feature lacp**	スイッチ上で LACP をイネーブルにします。
ステップ 3	switch(config)# **show feature**	（任意） イネーブルにされた機能を表示します。

次に、LACP をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature lacp
```

ポートに対するチャネル モードの設定

LACP ポート チャネルのそれぞれのリンクのチャネル モードを active または passive に設定できます。 このチャネル コンフィギュレーション モードを使用すると、リンクは LACP で動作可能になります。

関連するプロトコルを使用せずにポート チャネルを設定すると、リンク両端のすべてのインターフェイスでは on チャネル モードが維持されます。

はじめる前に

LACP 機能がイネーブルになっていることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port*
3. switch(config-if)# **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]
4. switch(config-if)# **no channel-group** *number* **mode**

手順の詳細

	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)# **channel-group** *channel-number* [**force**] [**mode** {**on**	**active**	**passive**}]	ポート チャネルのリンクのポート モードを指定します。 LACP をイネーブルにしたら、各リンクまたはチャネル全体を active または passive に設定します。

	コマンドまたはアクション	目的
		force：これを指定すると、チャネル グループにLAN ポートが強制的に追加されます。 このオプションは、Cisco NX-OS Release 5.0(2)N2(1) で使用できます。 mode：インターフェイスのポート チャネル モードを指定します。 active：これを指定すると、LACP をイネーブルにした時点で、指定したインターフェイス上で LACP がイネーブルになります。 インターフェイスはアクティブ ネゴシエーション ステートになります。この場合ポートでは、LACPパケットを送信することにより、他のポートとのネゴシエーションが開始されます。 on：（デフォルト モード）これを指定すると、すべてのスタティック ポートチャネル（LACPを稼働していないポートチャネル）に対して、このモードが維持されます。 passive：LACPデバイスが検出された場合にのみ、LACP をイネーブルにします。 インターフェイスはパッシブ ネゴシエーション ステートになります。この場合ポートでは、受信した LACP パケットへの応答は行われますが、LACP ネゴシエーションは開始されません。 関連するプロトコルを使用せずにポート チャネルを実行する場合、チャネル モードは常に on です。
ステップ 4	switch(config-if)# **no channel-group** *number* **mode**	指定インターフェイスのポート モードを on に戻します

次に、チャネル グループ 5 のイーサネット インターフェイス 1/4 で、LACP がイネーブルなインターフェイスを active ポート チャネル モードに設定する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# channel-group 5 mode active
```

次の例は、チャネル グループ 5 にインターフェイスを強制的に追加する方法を示したものです。

```
switch(config)# interface ethernet 1/1
switch(config-if)# channel-group 5 force
switch(config-if)#
```

LACP 高速タイマー レートの設定

LACP タイマー レートを変更することにより、LACP タイムアウトの時間を変更することができます。 **lacp rate** コマンドを使用すれば、LACP がサポートされているインターフェイスに LACP 制御パケットを送信する際のレートを設定できます。 タイムアウト レートは、デフォルトのレート（30秒）から高速レート（1秒）に変更することができます。 このコマンドは、LACPがイネーブルになっているインターフェイスでのみサポートされます。

はじめる前に

LACP 機能がイネーブルになっていることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port*
3. switch(config-if)# **lacp rate fast**

手順の詳細

	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ます。インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **lacp rate fast**	LACP がサポートされているインターフェイスに LACP 制御パケットを送信する際のレートとして高速レート（1 秒）を設定します。

次の例は、イーサネット インターフェイス 1/4 に対して LACP 高速レートを設定する方法を示したものです。

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

switch(config-if)# lacp rate fast
```

次の例は、イーサネット インターフェイス 1/4 の LACP レートをデフォルトのレート（30 秒）に戻す方法を示したものです。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# no lacp rate fast
```

LACP のシステム プライオリティおよびシステム ID の設定

LACP システム ID は、LACP システム プライオリティ値と MAC アドレスを組み合わせたものです。

はじめる前に

LACP 機能がイネーブルになっていることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **lacp system-priority** *priority*
3. （任意） switch# **show lacp system-identifier**

手順の詳細

	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)# **lacp system-priority** *priority*	LACP で使用するシステム プライオリティを設定します。指定できる範囲は 1 ～ 65535 で、値が大きいほどプライオリティは低くなります。 デフォルト値は 32768 です。
ステップ 3	switch# **show lacp system-identifier**	（任意） LACP システム識別子を表示します。

次に、LACP システム プライオリティを 2500 に設定する例を示します。

```
switch# configure terminal
switch(config)# lacp system-priority 2500
```

LACP ポート プライオリティの設定

LACP ポート チャネルの各リンクに対して、ポート プライオリティの設定を行うことができます。

はじめる前に

LACP 機能がイネーブルになっていることを確認します。

手順の概要

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

手順の詳細

	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)# **lacp port-priority** *priority*	LACP で使用するポート プライオリティを設定します。 指定できる範囲は 1 ～ 65535 で、値が大きいほどプライオリティは低くなります。 デフォルト値は 32768 です。

次に、イーサネット インターフェイス 1/4 の LACP ポート プライオリティを 40000 に設定する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# lacp port priority 40000
```

LACP グレースフル コンバージェンス

はじめる前に

- LACP 機能をイネーブルにします。
- ポート チャネルが管理上のダウン状態になっていることを確認します。
- 正しい VDC を使用していることを確認します。 正しい VDC に切り替えるには、**switchto vdc** コマンドを入力します。

手順の概要

1. **configure terminal**
2. **interface port-channel** *number*
3. **shutdown**
4. **no lacp graceful-convergence**
5. **no shutdown**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *number*
	
	例：
	`switch(config)# interface port-channel 1`
	`switch(config) #`
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**shutdown**
	
	例：
	`switch(config-if)# shutdown`
	`switch(config-if) #`
		ポート チャネルを管理シャットダウンします。

ステップ 4	**no lacp graceful-convergence**
	
	例：
	`switch(config-if)# no lacp graceful-convergence`
	`switch(config-if) #`
		指定したポート チャネルの LACP グレースフル コンバージェンスをディセーブルにします。

ステップ 5	**no shutdown**
	
	例：
	`switch(config-if)# no shutdown`
	`switch(config-if) #`
		ポート チャネルを管理上のアップ状態にします。

ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次の例は、ポート チャネルの LACP グレースフル コンバージェンスをディセーブルにする方法を示したものです。

```
switch# configure terminal
switch(config) # interface port-channel 1
switch(config-if) # shutdown
switch(config-if) # no lacp graceful-convergence
switch(config-if) # no shutdown
switch(config-if) #
```

LACP グレースフル コンバージェンスの再イネーブル化

はじめる前に

- LACP 機能をイネーブルにします。
- ポート チャネルが管理上のダウン状態になっていることを確認します。
- 正しい VDC を使用していることを確認します。 正しい VDC に切り替えるには、**switchto vdc** コマンドを入力します。

手順の概要

1. **configure terminal**
2. **interface port-channel** *number*
3. **shutdown**
4. **lacp graceful-convergence**
5. **no shutdown**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *number*
	
	例：
	`switch(config)# interface port-channel 1`
	`switch(config) #`
		設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**shutdown**
	
	例：
	`switch(config-if)# shutdown`
	`switch(config-if) #`
		ポート チャネルを管理シャットダウンします。

ステップ 4	**lacp graceful-convergence**
	
	例：
	`switch(config-if)# lacp graceful-convergence`
	`switch(config-if) #`
		指定したポート チャネルの LACP グレースフル コンバージェンス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 5	**no shutdown**
	
	例：
	`switch(config-if)# no shutdown`
	`switch(config-if) #`
		ポート チャネルを管理上のアップ状態にします。

ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次の例は、ポート チャネルの LACP グレースフル コンバージェンスをディセーブルにする方法を示したものです。

```
switch# configure terminal
switch(config) # interface port-channel 1
switch(config-if) # shutdown
switch(config-if) # lacp graceful-convergence
switch(config-if) # no shutdown
switch(config-if) #
```

ポート チャネル設定の確認

ポート チャネルの設定情報を表示する場合は、次のいずれかの操作を行います。

コマンド	目的
switch# **show interface port-channel** *channel-number*	ポート チャネル インターフェイスのステータスを表示します。
switch# **show feature**	イネーブルにされた機能を表示します。
switch# **show resource**	システムで現在利用可能なリソースの数を表示します。
switch# **show lacp** {**counters** | **interface** *type slot/port* | **neighbor** | **port-channel** | **system-identifier**}	LACP 情報を表示します。
switch# **show port-channel compatibility-parameters**	ポート チャネルに追加するためにメンバ ポート間で同じにするパラメータを表示します。
switch# **show port-channel database** [**interface port-channel** *channel-number*]	1 つ以上のポート チャネル インターフェイスの集約状態を表示します。

コマンド	目的
switch# **show port-channel summary**	ポート チャネル インターフェイスの概要を表示します。
switch# **show port-channel traffic**	ポートチャネルのトラフィック統計情報を表示します。
switch# **show port-channel usage**	使用済みおよび未使用のチャネル番号の範囲を表示します。
switch# **show port-channel database**	現在実行中のポートチャネル機能に関する情報を表示します。
switch# **show port-channel load-balance**	ポートチャネルによるロードバランシングについての情報を表示します。

ロードバランシング発信ポート ID の確認

コマンドに関する注意事項

show port-channel load-balance コマンドを使用すると、ポート チャネルにおいて特定のフレームがいずれのポートにハッシュされるかを確認することができます。 正確な結果を取得するためには、VLAN および宛先 MAC を指定する必要があります。

（注） ポート チャネル内にポートが 1 つしかない場合などには、一部のトラフィック フローはハッシュの対象になりません。

ロードバランシング発信ポートIDを表示する場合は、次の表に記載されているいずれかの操作を実行します。

コマンド	目的
switch# **show port-channel load-balance forwarding-path interface port-channel** *port-channel-id* **vlan** vlan-id **dst-ip src-ip dst-mac src-mac l4-src-port** *port-id* **l4-dst-port** *port-id*	発信ポート ID を表示します。

例

次に示すのは、**show port-channel load-balance** コマンドを実行した場合の出力例です。

switch#**show port-channel load-balance forwarding-path interface port-channel** *10* **vlan** *1* **dst-ip** *1.225.225.225* **src-ip** *1.1.10.10* **src-mac** *aa:bb:cc:dd:ee:ff* **l4-src-port** *0* **l4-dst-port** *1*

```
Missing params will be substituted by 0's.Load-balance Algorithm on switch:
source-dest-portcrc8_hash: 204 Outgoing port id: Ehernet1/1 Param(s) used
to calculate load-balance:
dst-port: 1
src-port: 0
dst-ip: 1.225.225.225
src-ip: 1.1.10.10
dst-mac: 0000.0000.0000
src-mac: aabb.ccdd.eeff
```

第 9 章

仮想ポート チャネルの設定

この章の内容は、次のとおりです。

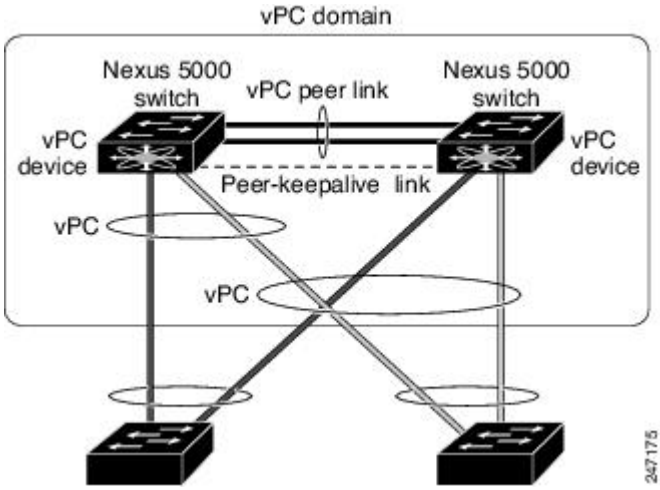
vPC について

vPC の概要

仮想ポート チャネル（vPC）を使用すると、物理的には 2 台の異なる Cisco Nexus 5000 シリーズ スイッチまたは Cisco Nexus 2000 シリーズ ファブリック エクステンダに接続されている複数のリンクを、第 3 のデバイスからは単一のポート チャネルとして認識されるようにすることができます（次の図を参照）。 第 3 のデバイスには、スイッチやサーバなどあらゆるネットワーキング デバイスが該当します。 Cisco NX-OS Release 4.1(3)N1(1) 以降では、ファブリック エクステンダに接続された Cisco Nexus 5000 シリーズ スイッチを含む vPC トポロジを設定することができます。 vPC では、マルチパス機能を使用することができます。この機能では、ノード間の複数のパラレ

ルパスをイネーブルにし、さらには存在する代替パスでトラフィックのロードバランシングを行うことにより、冗長性が確保されます。

図 *8*：*vPC* のアーキテクチャ



EtherChannel の設定は、次のいずれかを使用して行います。

- プロトコルなし
- Link Aggregation Control Protocol（LACP）

vPC ピア リンク チャネルなど、vPC で EtherChannel を設定した場合、それぞれのスイッチでは 1 つの EtherChannel に最大 16 個のアクティブ リンクをまとめることができます。 ファブリック エクステンダ上で vPC を設定した場合、各 EtherChannel で使用できるポートは 1 つだけです。

（注） vPC の機能を設定したり実行したりするには、まず vPC 機能をイネーブルにする必要があります。

vPC 機能をイネーブルにするためには、vPC 機能を実現する 2 つの vPC ピア スイッチの vPC ドメインにピアキープアライブ リンクおよびピアリンクを作成する必要があります。

vPC ピア リンクを作成する場合は、まず一方の Cisco Nexus 5000 シリーズ スイッチ上で、2 つ以上の Ethernet ポートを使用して EtherChannel を設定します。 さらに他方のスイッチ上で、2 つ以上の Ethernet ポートを使用して別の EtherChannel を設定します。 これら 2 つの EtherChannel を接続することにより、vPC ピア リンクが作成されます。

（注） vPC ピアリンク EtherChannel はトランクとして設定することが推奨されます。

vPC ドメインには、両方の vPC ピア デバイス、vPC ピアキープアライブ リンク、vPC ピア リンク、および vPC ドメイン内にあってダウンストリーム デバイスに接続されているすべての

EtherChannel が含まれます。 各 vPC ピア デバイスに設定できる vPC ドメイン ID は 1 つだけです。

（注） EtherChannel を使用する vPC デバイスはすべて、両方の vPC ピア デバイスに接続する必要があります。

vPC には次のような特長があります。

- 単独のデバイスが、2 つのアップストリーム デバイスを介して EtherChannel を使用できるようになります。
- スパニングツリー プロトコル（STP）のブロック ポートが不要になります。
- ループフリーなトポロジが実現されます。
- 利用可能なすべてのアップリンク帯域幅を使用します。
- リンクまたはスイッチに障害が発生した場合、高速コンバージェンスが実行されます。
- リンク レベルの復元力を提供します。
- ハイ アベイラビリティが保証されます。

用語

vPC の用語

vPC で使用される用語は、次のとおりです。

- vPC：vPC ピア デバイスとダウンストリーム デバイスの間の結合された EtherChannel。
- vPC ピア デバイス：vPC ピア リンクと呼ばれる特殊な EtherChannel により接続されることで対をなす個々のデバイス。
- vPC ピア リンク：vPC ピア デバイス間の状態を同期するために使用されるリンク。
- vPC メンバ ポート：vPC に属するインターフェイス。
- ホスト vPC ポート：vPC に属するファブリック エクステンダのホスト インターフェイス。
- vPC ドメイン：このドメインには、両方の vPC ピア デバイス、vPC ピアキープアライブ リンク、vPC 内にあってダウンストリーム デバイスに接続されているすべてのポート チャネルが含まれます。 また、このドメインは、vPC グローバル パラメータを割り当てるために使用する必要があるコンフィギュレーション モードに関連付けられています。 vPC ドメイン ID は、両スイッチで同じであることが必要です。
- vPC ピアキープアライブ リンク：ピアキープアライブ リンクでは、さまざまな vPC ピア Cisco Nexus 5000 シリーズ デバイスのモニタリングが行われます。 ピアキープアライブ リンクは、vPC ピア デバイス間での設定可能なキープアライブ メッセージの定期的な送信を行います。

vPCs ピアキープアライブ リンク上を移動するデータまたは同期トラフィックはありません。このリンクを流れるトラフィックは、送信元スイッチが稼働しており、vPC を実行していることを知らせるメッセージだけです。

ファブリック エクステンダの用語

Cisco Nexus 2000 シリーズ ファブリック エクステンダで使用される用語は、次のとおりです。

- ファブリック インターフェイス：ファブリック エクステンダから親スイッチへの接続に特化した 10 ギガビット イーサネットのアップリンク ポートです。 ファブリック インターフェイスは他の目的には使用できません。 親スイッチに直接接続する必要があります。
- EtherChannel ファブリック インターフェイス：ファブリック エクステンダから親スイッチへの EtherChannel アップリンク接続です。 この接続は、単一論理チャネルにバンドルされているファブリック インターフェイスで構成されます。
- ホスト インターフェイス：サーバ接続またはホスト接続に使用するイーサネット インターフェイスです。 これらのポートは、ファブリック エクステンダのモデルに応じて、1 ギガビット イーサネット インターフェイスになる場合と、10 ギガビット イーサネット インターフェイスになる場合があります。
- EtherChannel ホスト インターフェイス：ファブリック エクステンダのホスト インターフェイスからサーバ ポートへの EtherChannel ダウンリンク接続です。

（注） リリース 4.1(3)N1(1) では、EtherChannel ホスト インターフェイスはただ 1 つのホスト インターフェイスで構成され、Link Aggregation Control Protocol（LACP）EtherChannel として設定することも非 LACP EtherChannel として設定することもできます。

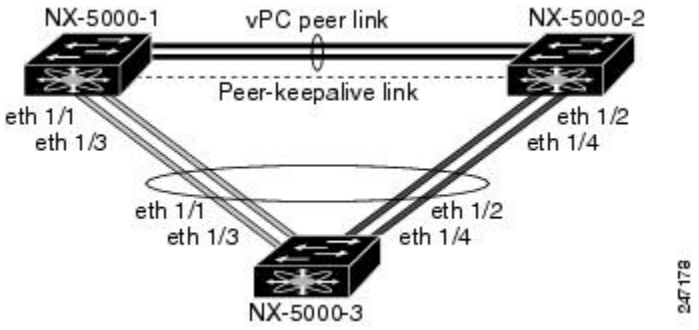
サポートされている vPC トポロジ

Cisco Nexus 5000 シリーズ スイッチの vPC トポロジ

vPC では Cisco Nexus 5000 シリーズ スイッチのペア、または Cisco Nexus 5500 シリーズ スイッチのペアを、別のスイッチまたはサーバに直接接続することができます。 vPC ピア スイッチは同じタイプであることが必要です。たとえば、Nexus 5000 シリーズ スイッチ同士、または Nexus 5500 シリーズ スイッチ同士を接続することはできますが、vPC トポロジにおいて Nexus 5000 シリーズ スイッチを Nexus 5500 シリーズ スイッチに接続することはできません。 各 Cisco Nexus 5000 シリーズ スイッチに接続できるインターフェイスは最大 8 個で、vPC ペアに対して 16 個のインターフェイスをバンドルすることができます。 次の図に示したトポロジは、10 ギガビット イーサネッ

トアップリンク インターフェイスまたは 1 ギガビット イーサネット アップリンク インターフェイスにより接続された 2 台のスイッチまたはサーバに対して vPC 機能を実現したものです。

図 *9*：スイッチ間の *vPC* トポロジ



（注） Cisco Nexus 5010 スイッチの最初の 8 ポートおよび Cisco Nexus 5020 スイッチの最初の 16 ポートでは、1 ギガビット ポートと 10 ギガビット ポートとを切り替えることができます。 これらのポートに対して vPC 機能は実現する場合は、1 ギガビット モードを使用します。

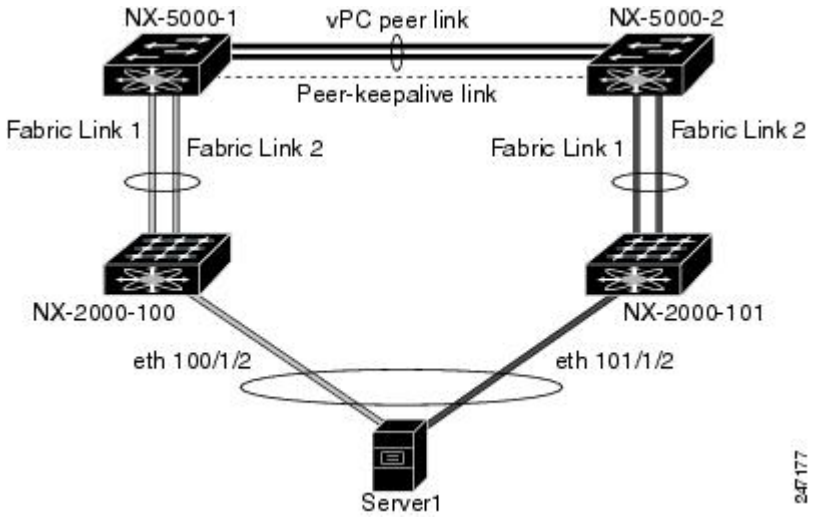
Cisco Nexus 5000 シリーズ スイッチのペアに接続するスイッチには、標準ベースのイーサネット スイッチであればいずれも使用できます。 このような構成を持つ環境としては、2 台のスイッチが vPC を介して Cisco Nexus 5000 シリーズ スイッチのペアに接続されたブレード シャーシや Cisco Nexus 5000 シリーズ スイッチのペアに接続されたユニファイド コンピューティング システムなどが一般的です。

シングル ホーム ファブリック エクステンダの vPC トポロジ

下の図のように、Cisco Nexus 5000 シリーズ スイッチに接続した Cisco Nexus 2000 シリーズ ファブリック エクステンダのペアに、vPC で 2 台、4 台、またはそれ以上のネットワーク アダプタが設定されたサーバを接続することができます。各ファブリックエクステンダには、FEXモデルに応じて、1 台以上のネットワーク アダプタ インターフェイスを接続できます。 図 10 はその具体例として、Cisco Nexus 2148T ファブリック エクステンダを使用して構成したトポロジを示したものです。サーバから各ファブリック エクステンダへのリンクはそれぞれ 1 つだけです。 Cisco Nexus 2248TP ファブリック エクステンダまたは Cisco Nexus 2232PP ファブリック エクステンダを使用したトポロジは、サーバから各ファブリック エクステンダに対して複数のリンクを設定して構成することもできます。

下図に示したトポロジでは、1 ギガビット イーサネット アップリンク インターフェイスを持つデュアル ホーム サーバに対して vPC 機能が実現されています。

図 *10*：シングル ホーム ファブリック エクステンダの *vPC* トポロジ



Cisco Nexus 5000 シリーズ スイッチは、このトポロジで最大 12 台の設定済みシングル ホーム ファブリック エクステンダ（ポート数は 576）をサポートできますが、この構成による vPC では 480 576 台のデュアル ホーム ホスト サーバを設定することかできます。

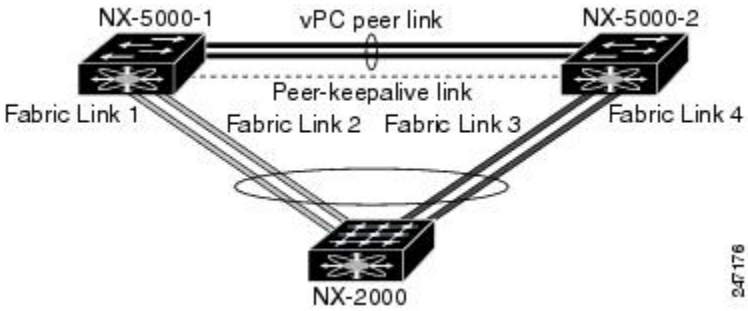
（注） Cisco Nexus 2148T ファブリック エクステンダは、ホスト インターフェイスでの EtherChannel はサポートしていません。そのため、1 つの EtherChannel で設定できるサーバからのリンクは最大 2 つで、各リンクは別々のファブリック エクステンダに接続されます。

デュアル ホーム ファブリック エクステンダの vPC トポロジ

Cisco Nexus 2000 シリーズ ファブリック エクステンダを、アップストリームにある 2 台の Cisco Nexus 5000 シリーズ スイッチ、およびダウンストリームにある複数のシングル ホーム サーバに

接続することができます。 次の図に示したトポロジは、1 ギガビット イーサネット アップリンク インターフェイスでそれぞれ別々に接続されたサーバに対して vPC 機能を実現したものです。

図 *11*：デュアルホーム接続 ファブリック エクステンダ *vPC* トポロジ



Cisco Nexus 5000 シリーズ スイッチは、このトポロジで最大 12 台の設定済みデュアル ホーム ファブリック エクステンダをサポートできます。 この構成では、最大 576 台のシングル ホーム サーバを接続できます。

vPC ドメイン

vPC ドメインを作成するには、まず各 vPC ピア スイッチに対し、1 ～ 1000 の範囲にある値を使用して vPC ドメイン ID を作成する必要があります。 この ID は、対象となるすべての vPC ピア デバイス上で同じであることが必要です。

EtherChannel および vPC ピア リンクは、LACP を使用するかまたはプロトコルなしのいずれかで設定できます。 LACP では EtherChannel における設定不一致の検査を実行できるため、ピアリンク上では可能な限り、LACP を使用することが推奨されます。

vPC ピア スイッチでは、設定した vPC ドメイン ID に基づいて、一意の vPC システム MAC アドレスが自動的に割り当てられます。 各 vPC ドメインには一意の MAC アドレスがあり、vPC に関連する特定の処理の際に固有識別子として使用されます。ただしスイッチで vPC システム MAC アドレスが使用されるのは、LACP などリンク関連の処理に限ります。 連続したネットワーク内の vPC ドメインはそれぞれ、一意のドメイン ID を使用して作成することが推奨されます。 ただし、Cisco NX-OS ソフトウェアでアドレスを割り当てる代わりに、vPC ドメインに特定の MAC アドレスを設定することもできます。

vPC ピア スイッチでは、設定した vPC ドメイン ID に基づいて、一意の vPC システム MAC アドレスが自動的に割り当てられます。 スイッチで vPC システム MAC アドレスが使用されるのは、LACP や BPDU などリンク関連の処理に限ります。 vPC ドメインに特定の MAC アドレスを設定することもできます。

どちらのピアにも同じ vPC ドメイン ID を設定することが推奨されます。またドメイン ID はネットワーク内で一意であることが必要です。 たとえば、2 つの異なる vPC（一方がアクセス スイッチ、もう一方が集約スイッチ）がある場合は、それぞれの vPC に固有のドメイン ID を割り当ててください。

vPC ドメインを作成すると、その vPC ドメインのシステム プライオリティが Cisco NX-OS ソフトウェアによって自動的に作成されます。 vPC ドメインに特定のシステム プライオリティを手動で設定することもできます。

（注） システム プライオリティを手動で設定する場合は、必ず両方の vPC ピア スイッチ上に同じプライオリティ値を割り当てるようにしてください。 両側の vPC ピア スイッチに異なるシステム プライオリティ値が割り当てられている場合、vPC は稼働しません。

ピアキープアライブ リンクとメッセージ

Cisco NX-OS ソフトウェアでは、vPC ピア間のピアキープアライブ リンクを使用して、設定可能なキープアライブ メッセージが定期的に送信されます。 これらのメッセージを送信するためには、ピア スイッチ間にレイヤ 3 接続が必要です。ピアキープアライブ リンクがアップ状態で稼働していなければ、システムでは vPC ピア リンクをアップすることができません。

一方の vPC ピア スイッチに障害が発生すると、vPC ピア リンクのもう一方の側にある vPC ピア スイッチでは、ピアキープアライブ メッセージを受信しなくなることによってその障害を検知します。 vPC ピアキープアライブ メッセージのデフォルトの時間間隔は 1 秒です。 この時間間隔は、400 ミリ秒～ 10 秒の範囲で設定することができます。 タイムアウト値は、3 ～ 20 秒の範囲内で設定可能で、デフォルトのタイムアウト値は 5 秒です。 ピアキープアライブのステータスの確認は、ピアリンクがダウンした場合にのみ行われます。

vPC ピアキープアライブは、Cisco Nexus 5000 シリーズ スイッチ上の管理 VRF でもデフォルトの VRF でも伝送できます。 管理 VRF を使用するようスイッチを設定した場合は、mgmt 0 インターフェイスの IP アドレスがキープアライブ メッセージの送信元および宛先となります。 デフォルトの VRF を使用するようスイッチを設定した場合は、vPC キープアライブ メッセージの送信元アドレスおよび宛先アドレスとしての役割を果たす SVI を作成する必要があります。 ピアキープアライブ メッセージに使用される送信元 IP アドレスと宛先 IP アドレスがどちらもネットワーク上で一意であり、かつそれらの IP アドレスがその vPC ピアキープアライブ リンクに関連付けられている VRF から到達可能であることを確認してください。

（注） Cisco Nexus 5000 シリーズ スイッチの vPC ピアキープアライブ リンクは、管理 VRF で mgmt 0インターフェイスを使用して実行されるように設定することが推奨されます。デフォルトの VRF を設定する場合は、vPC ピアキープアライブ メッセージの伝送に vPC ピア リンクが使用されないようにしてください。

vPC ピア リンクの互換パラメータ

多くの設定パラメータおよび動作パラメータが、vPC 内のすべてのインターフェイスで同じでなければなりません。 vPC 機能をイネーブルにし、さらに両方の vPC ピア スイッチ上でピア リンクを設定すると、シスコ ファブリック サービス（CFS）メッセージにより、ローカル vPC ピア

スイッチに関する設定のコピーがリモート vPC ピア スイッチへ送信されます。 これによりシステムでは、2 つのスイッチ間で重要な設定パラメータに違いがないかどうか判定が行われます。

vPC 内のすべてのインターフェイスで設定されている値を表示するには、**show vpc consistency-parameters** コマンドを入力します。 表示される設定は、vPC ピア リンクおよび vPC の稼働を制限する可能性のある設定だけです。

vPC に関する互換性チェックのプロセスは、正規の EtherChannel に関する互換性チェックとは異なります。

同じでなければならない設定パラメータ

ここで説明する設定パラメータは、vPC ピア リンクの両側のスイッチ上で設定が同じであることが必要です。

（注） ここで説明する動作パラメータおよび設定パラメータは、vPC内のすべてのインターフェイスで一致している必要があります。

vPC 内のすべてのインターフェイスで設定されている値を表示するには、**show vpc consistency-parameters** コマンドを入力します。 表示される設定は、vPC ピア リンクおよび vPC の稼働を制限する可能性のある設定だけです。

スイッチでは、vPC インターフェイス上でこれらのパラメータに関する互換性チェックが自動的に行われます。 インターフェイス別のパラメータはインターフェイスごとに整合性を保っていることが必要であり、グローバル パラメータはグローバルに整合性を保っていることが必要です。

- ポート チャネル モード：on、off、active
- チャネルごとのリンク速度
- チャネルごとのデュプレックス モード
- チャネルごとのトランク モード：
  - ネイティブ VLAN
  - トランク上の許可 VLAN
  - ネイティブ VLAN トラフィックのタギング
- Spanning Tree Protocol（STP; スパニングツリー プロトコル）モード
- マルチ スパニングツリーの STP 領域コンフィギュレーション（MST）
- VLAN ごとのイネーブル/ディセーブル状態
- STP グローバル設定：
  - Bridge Assurance 設定
  - ポートタイプ設定：vPCインターフェイスはすべて標準ポートとして設定することが推奨されます

- ループ ガード設定

- STP インターフェイス設定：
  - ポート タイプ設定
  - ループ ガード
  - ルート ガード

- ファブリック エクステンダの vPC トポロジの場合、上記のインターフェイス レベル パラメータはすべて、両側スイッチのホストインターフェイスに対して設定を同じにする必要があります。
- EtherChannel ファブリック インターフェイス上で設定されたファブリック エクステンダの FEX 番号（ファブリック エクステンダの vPC トポロジの場合）。

これらのうち、イネーブルでないパラメータや一方のスイッチでしか定義されていないパラメータは、vPC の整合性検査では無視されます。

（注） どの vPC インターフェイスもサスペンド モードになっていないことを確認するには、**show vpc brief** コマンドおよび **show vpc consistency-parameters** コマンドを入力して、syslog メッセージをチェックします。

同じにすべき設定パラメータ

次に挙げるパラメータのいずれかが両側の vPC ピア スイッチ上で設定が一致しないと、誤設定に伴ってトラフィック フローに望ましくない動作が発生する可能性があります。

- MAC エージング タイマー
- スタティック MAC エントリ
- VLAN インターフェイス：vPC ピア リンクの両端にある各スイッチの VLAN インターフェイスは同じ VLAN 用に設定されている必要があり、さらにそれらの管理モードおよび動作モードも同じであることが必要です。 ピア リンクの一方のスイッチでのみ設定されている VLAN では、vPC またはピア リンクを使用したトラフィックの転送は行われません。 VLAN はすべて、プライマリ vPC スイッチとセカンダリ vPC スイッチの両方で作成する必要があります。両方で作成されていない場合、VLAN は停止することになります。
- プライベート VLAN 設定
- ACL のすべての設定とパラメータ
- Quality of Service（QoS）の設定およびパラメータ：ローカル パラメータです。グローバル パラメータは同じであることが必要です
- STP インターフェイス設定：

- BPDU フィルタ
- BPDU ガード
- コスト
- リンク タイプ
- プライオリティ
- VLAN（Rapid PVST+）

すべての設定パラメータについて互換性があることを確認するためにも、vPC の設定後は各 vPC ピア スイッチの設定を表示することが推奨されます。

グレースフル タイプ 1 検査

Cisco NX-OS Release 5.0(2)N2(1) 以降では、整合性検査で不整合が検出された場合、セカンダリ vPC スイッチ上でのみ vPC がダウン状態になります。プライマリ vPC スイッチ上の VLAN はアップ状態が維持されるため、トラフィックを中断することなくタイプ 1 の設定を実行することができます。この機能は、グローバル タイプ 1 不整合の場合にも、インターフェイス別タイプ 1 不整合の場合にも使用されます。

この機能は、デュアルアクティブ FEX ポートに対しては無効です。タイプ 1 の不一致が発生すると、両側スイッチのこれらのポートでは VLAN が停止します。

VLAN ごとの整合性検査

Cisco NX-OS Release 5.0(2)N2(1) 以降では、VLAN 上でスパニングツリーのイネーブル/ディセーブルが切り替わるたびに、いくつかのタイプ 1 整合性検査が VLAN ごとに実行されます。この整合性検査に合格しない VLAN は、プライマリ スイッチおよびセカンダリ スイッチでダウン状態になりますが、その他の VLAN は影響を受けません。

vPC 自動リカバリ

Cisco NX-OS Release 5.0(2)N2(1) 以降では、次のような状況が発生すると、vPC 自動リカバリ機能により vPC リンクが再イネーブル化されます。

両側の vPC ピア スイッチでリロードが実行され、かつ一方のスイッチのみリブートした場合、自動リカバリによってそのスイッチがプライマリ スイッチとして機能し、一定時間が経過した後に vPC リンクがアップ状態になります。このシナリオにおけるリロード遅延時間は、240 ～ 3600 秒の範囲で設定できます。

ピアリンクの障害に伴ってセカンダリ vPC スイッチ上の vPC がディセーブルになり、さらにプライマリ vPC スイッチで障害が発生するか、またはトラフィックが転送できなくなると、セカンダリ スイッチでは vPC が再イネーブル化されます。このシナリオの場合、vPC ではキープアライブが 3 回連続して検出されないのを待ってから vPC リンクが回復します。

vPC 自動リカバリ機能は、デフォルトではディセーブルです。

vPC ピア リンク

vPC ピア リンクは、vPC ピア デバイス間の状態を同期するために使用されるリンクです。

（注） vPC ピア リンクを設定する場合は、あらかじめピアキープアライブ リンクを設定しておく必要があります。設定しておかないと、ピア リンクは機能しません

vPC ピア リンクの概要

vPC ピアとして設定できるのは、対をなす 2 台のスイッチです。それぞれのスイッチは互いに、他方の vPC ピアに対してのみ vPC ピアとして機能します。 vPC ピア スイッチには、他のスイッチへの非 vPC リンクを設定することもできます。

適正な設定を行うため、各スイッチに EtherChannel を設定し、さらに vPC ドメインを設定します。 各スイッチの EtherChannel をピア リンクとして割り当てます。 冗長性を確保できるよう、EtherChannel には少なくとも 2 つの専用ポートを設定することが推奨されます。これにより、vPC ピア リンクのインターフェイスの 1 つに障害が発生すると、スイッチは自動的にフォールバックし、そのピア リンクの別のインターフェイスが使用されます。

（注） EtherChannel はトランク モードで設定することが推奨されます。

多くの動作パラメータおよび設定パラメータは、vPC ピア リンクにより接続されている各スイッチ上で同じ値であることが必要です。 各スイッチは管理プレーンから完全に独立しているため、重要なパラメータについてスイッチ同士に互換性があることを確認する必要があります。 vPC ピア スイッチには、独立したコントロール プレーンがあります。 vPC ピア リンクの設定が完了したら、各 vPC ピア スイッチの設定を表示し、それらの設定に互換性があることを確認してください。

（注） vPC ピア リンクによって接続されている 2 つのスイッチでは必ず、同一の動作パラメータおよび設定パラメータが設定されている必要があります。

vPC ピア リンクを設定する際、vPC ピア スイッチでは、接続されたスイッチの一方がプライマリ スイッチ、もう一方がセカンダリ スイッチとなるようにネゴシエーションが行われます。デフォルトの場合、Cisco NX-OS ソフトウェアでは、最小の MAC アドレスを基にプライマリ スイッチが選択されます。 特定のフェールオーバー条件の下でのみ、このソフトウェアは各スイッチ（つまり、プライマリ スイッチとセカンダリ スイッチ）に対して別々の処理を行います。 プライマリ スイッチに障害が発生した場合、システムが回復した時点でセカンダリ スイッチがプライマリ スイッチとして動作し、元々のプライマリ スイッチがセカンダリ スイッチとなります。

ただし、どちらの vPC スイッチをプライマリ スイッチにするか設定することもできます。 一方の vPC スイッチをプライマリ スイッチにするためロール プライオリティを再設定する場合は、まずプライマリ vPC スイッチとセカンダリ vPC スイッチのそれぞれに対してロール プライオリティを適切な値に設定し、**shutdown** コマンドを入力して両スイッチの vPC ピア リンクである EtherChannel をシャットダウンした後、**no shutdown** コマンドを入力して両スイッチの EtherChannel を再度イネーブルにします。

ピア間では、vPC リンクを介して認識された MAC アドレスの同期も行われます。

設定情報は、Cisco Fabric Service over Ethernet（CFSoE）プロトコルを使用して vPC ピア リンクを転送されます。 両方のスイッチで設定されているこれらの VLAN の MAC アドレスはすべて、vPC ピア スイッチ間で同期されています。 この同期に、CFSoE が使用されます

vPC ピア リンクに障害が発生すると、ソフトウェアでは、両方のスイッチが稼働していることを確認するため、vPC ピア スイッチ間のリンクであるピアキープアライブ リンクを使用してリモート vPC ピア スイッチのステータス確認が行われます、vPC ピア スイッチが稼働している場合は、セカンダリ vPC スイッチにあるすべて vPC ポートがディセーブルになります。 さらにデータは、EtherChannel において依然アクティブ状態にあるリンクに転送されます。

ソフトウェアは、ピアキープアライブ リンクを介してキープアライブ メッセージが返されない場合、vPC ピア スイッチに障害が発生したと認識します。

vPC ピア スイッチ間では、別途用意されたリンク（vPC ピアキープアライブ リンク）を使用して、設定可能なキープアライブ メッセージが送信されます。 vPC ピアキープアライブ リンク上のキープアライブ メッセージにより、障害が vPC ピア リンク上でだけ発生したのか、vPC ピア スイッチ上で発生したのかが判断されます。 キープアライブ メッセージは、ピア リンク内のすべてのリンクで障害が発生した場合にだけ使用されます。

vPC 番号

vPC ドメイン ID と vPC ピア リンクを作成すると、ダウンストリーム スイッチを各 vPC ピア スイッチに接続するための EtherChannel を作成することができます。 ダウントストリーム スイッチ上で EtherChannel を 1 つだけ作成し、そのポートの半分をプライマリ vPC ピア スイッチ用、残りの半分をセカンダリ vPC ピア スイッチ用として使用します。

各 vPC ピア スイッチ上では、ダウンとリーム スイッチに接続された EtherChannel に同じ vPC 番号を割り当てます。 vPC の作成時にトラフィックが中断されることはほとんどありません。 設定を簡素化するため、各 EtherChannel に対してその EtherChannel と同じ番号の vPC ID 番号を割り当てることもできます（EtherChannel 10 に対しては vPC ID 10 を割り当てるなど）。

（注） vPC ピア スイッチからダウンストリーム スイッチに接続する EtherChannel に割り当てる vPC 番号は、両側の vPC ピア スイッチで同じであることが必要です。

その他の機能との vPC の相互作用

vPC と LACP

Link Aggregation Control Protocol（LACP）では、vPC ドメインのシステム MAC アドレスに基づいて、その vPC に対する LACP Aggregation Group（LAG）ID が構成されます。

LACP は、ダウンストリーム スイッチからのチャネルも含め、すべての vPC EtherChannel 上で使用できます。 vPC ピア スイッチの各 EtherChannel のインターフェイスに対しては、LACP をアクティブモードで設定することが推奨されます。 この設定により、スイッチ、単方向リンク、およびマルチホップ接続の間の互換性をより簡単に検出できるようになり、実行時の変更およびリンク障害に対してダイナミックな応答が可能になります。

vPC ピア リンクは、16 個の EtherChannel インターフェイスをサポートしています。

（注） システム プライオリティを手動で設定する場合は、必ず両側の vPC ピア スイッチ上に同じプライオリティ値を割り当てるようにしてください。 両側の vPC ピア スイッチに異なるシステム プライオリティ値が割り当てられている場合、vPC は稼働しません。

vPC ピア リンクと STP

vPC 機能の初回起動時には、STP は再コンバージェンスします。 STP は、vPC ピア リンクを特殊なリンクとして扱い、常に vPC ピア リンクを STP のアクティブ トポロジに含めます。

すべての vPC ピア リンク インターフェイスを STP ネットワーク ポート タイプに設定して、すべての vPC リンク上で Bridge Assurance が自動的にイネーブルになるようにすることを推奨します。また、vPC ピア リンク上ではどの STP 拡張機能もイネーブルにしないことが推奨されます。

一連のパラメータは、vPC ピア リンクの両端の vPC ピア スイッチ上で設定を同じにする必要があります。

STP は分散型です。つまり、このプロトコルは、両端の vPC ピア スイッチ上で継続的に実行されます。 ただし、セカンダリ vPC ピア スイッチ上の vPC インターフェイスの STP プロセスは、プライマリ スイッチとして選択されている vPC ピア スイッチ上での設定により制御されます。

プライマリ vPC スイッチでは、Cisco Fabric Services over Ethernet（CFSoE）を使用して、vPC セカンダリ ピア スイッチ上の STP 状態の同期化が行われます。

vPC ピア スイッチ間では、プライマリ スイッチとセカンダリ スイッチを設定して 2 つのスイッチを STP 用に調整する提案/ハンドシェイク合意が vPC マネージャによって実行されます。 さらにプライマリ vPC ピア スイッチにより、プライマリ スイッチおよびセカンダリ スイッチの vPC インターフェイスに対する STP プロトコルの制御が行われます。

ブリッジ プロトコル データ ユニット（BPDU）では、代表ブリッジ ID フィールドの STP ブリッジ ID として、vPC に対して設定された MAC アドレスが使用されます。 これら vPC インターフェイスの BPDU は vPC プライマリ スイッチにより送信されます。

（注） vPC ピア リンクの両側での設定を表示して、設定が同じであることを確認してください。 vPC に関する情報を表示する場合は、**show spanning-tree** コマンドを使用します。

vPC と ARP

Cisco NX-OS では、Cisco Fabric Services over Ethernet（CFSoE）プロトコルが持つ信頼性の高い転送メカニズムによって、vPC ピア間のテーブルの同期が管理されます。 vPC ピア間でアドレス テーブルの高速コンバージェンスをサポートするためには、**ip arp synchronize** コマンドをイネーブルにする必要があります。 このコンバージェンスは、ピアリンク ポート チャネルがフラップした場合や vPC ピアがオンラインに戻った場合に、ARP テーブルの復元に伴う遅延の解消を目的としたものです。

パフォーマンスを向上させるためにも、ARP 同期機能はイネーブルにすることが推奨されます。デフォルトではディセーブルです。

ARP 同期がイネーブルかどうかを確認する場合は、次のコマンドを入力します。

```
switch# show running
```

ARP 同期をイネーブルにする場合は、次のコマンドを入力します。

```
switch(config-vpc-domain) # ip arp synchronize
```

CFSoE

Cisco Fabric Services over Ethernet（CFSoE）は、vPC ピア デバイスの動作を同期化するために使用される信頼性の高い状態転送メカニズムです。 CFSoE は、vPC にリンクされている、STP、IGMP などの多くの機能のメッセージとパケットを伝送します。 情報は、CFS/CFSoE プロトコル データ ユニット（PDU）に入れて伝送されます。

CFSoE は、vPC 機能をイネーブルにすると、デバイスによって自動的にイネーブルになります。何も設定する必要はありません。 vPC の CFSoE 分散には、IP を介してまたは CFS リージョンに分散する機能は必要ありません。 CFSoE 機能が vPC 上で正常に機能するために必要な設定は一切ありません。

show mac address-table コマンドを使用すれば、CFSoE が vPC ピア リンクのために同期する MAC アドレスを表示できます。

（注） **no cfs eth distribute** コマンドと **no cfs distribute** コマンドは入力しないでください。 vPC 機能に対しては CFSoE をイネーブルにする必要があります。 vPC がイネーブルの場合にこれらのコマンドのいずれかを入力すると、エラー メッセージが表示されます。

show cfs application コマンドを入力すると、出力に「Physical-eth」と表示されます。これは、CFSoE を使用しているアプリケーションを表します。

VRF に関する注意事項と制約事項

vPC には、次の注意事項と制約事項があります。

- vPC ピアリンクおよび vPC インターフェイスを設定する場合は、あらかじめ vPC 機能をイネーブルにしておく必要があります。
- システムにおいて vPC ピア リンクを構成するためには、その前にピアキープアライブ リンクを設定しておく必要があります。
- vPC ピアリンクは、少なくとも 2 つの 10 ギガビット イーサネット インターフェイスを使用して構成する必要があります。
- vPC では Cisco Nexus 5000 シリーズ スイッチのペア、または Cisco Nexus 5500 シリーズ スイッチのペアを、別のスイッチまたはサーバに直接接続することができます。 vPC ピア スイッチは同じタイプであることが必要です。たとえば、Nexus 5000 シリーズ スイッチ同士、または Nexus 5500 シリーズ スイッチ同士を接続することはできますが、vPC トポロジにおいて Nexus 5000 シリーズ スイッチを Nexus 5500 シリーズ スイッチに接続することはできません。
- vPC に使用できるのは、ポート チャネルのみです。 vPC は、通常のポート チャネル上（スイッチ間 vPC トポロジ）、ポート チャネルのファブリック インターフェイス上（ファブリック エクステンダの vPC トポロジ）、およびポート チャネルのホスト インターフェイス上（ホスト インターフェイスの vPC トポロジ）で設定できます。
- ファブリック エクステンダは、ホスト インターフェイスの vPC トポロジのメンバになることもファブリック エクステンダの vPC トポロジのメンバになることも可能ですが、同時に両方のメンバになることはできません。
- 両側の vPC ピア スイッチを設定する必要があります。ただし vPC ピア デバイス間で設定が自動的に同期化されることはありません。
- 必要な設定パラメータが、vPC ピア リンクの両側で互換性を保っているかチェックしてください。
- vPC の設定中に、最小限のトラフィックの中断が発生する可能性があります。
- vPC 内の LACP を使用するポート チャネルはすべて、アクティブ モードのインターフェイスで設定することが推奨されます。

vPC の設定

vPC のイネーブル化

vPC を設定して使用する場合は、事前に vPC 機能をイネーブルにしておく必要があります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature vpc**
3. （任意） switch# **show feature**
4. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 vpc**	スイッチで vPC をイネーブルにします。
ステップ 3	switch# **show feature**	（任意） スイッチ上でイネーブルになっている機能を表示します。
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、vPC 機能をイネーブルにする方法を示します。

```
switch# configure terminal
switch(config)# feature vpc
```

vPC のディセーブル化

vPC 機能をディセーブルにできます。

（注） vPC 機能をディセーブルにすると、Cisco Nexus 5000 シリーズ スイッチ上のすべての vPC 設定がクリアされます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **no feature vpc**
3. （任意） switch# **show feature**
4. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 feature vpc**	スイッチで vPC をディセーブルにします。
ステップ 3	switch# **show feature**	（任意） スイッチ上でイネーブルになっている機能を表示します。
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、vPC 機能をディセーブルにする方法を示します。

```
switch# configure terminal
switch(config)# no feature vpc
```

vPC ドメインの作成

両側の vPC ピア スイッチに対して、同じ vPC ドメイン ID を作成する必要があります。 このドメイン ID を基に、vPC システムの MAC アドレスが自動的に構成されます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。手順は次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain** *domain-id*
3. （任意） switch# **show vpc brief**
4. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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)# **vpc domain** *domain-id*	スイッチに対して vPC ドメインを作成し、vpc-domain コンフィギュレーション モードを開始します。 *domain-id* のデフォルト値はありません。指定できる値の範囲は 1 ～ 1000 です。 （注） 既存の vPC ドメインに対して vpc-domain コンフィギュレーション モードを開始する場合は、**vpc domain** コマンドを使用することもできます。
ステップ 3	switch# **show vpc brief**	（任意） 各 vPC ドメインに関する要約情報を表示します。
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、vPC ドメインを作成する例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
```

vPC キープアライブ リンクと vPC キープアライブ メッセージの設定

キープアライブ メッセージを伝送するピアキープアライブ リンクの宛先 IP を設定できます。 必要に応じて、キープアライブ メッセージのその他のパラメータも設定できます。

Cisco NX-OS Release 5.0(3)N1(1) 以降、Cisco Nexus 5500 プラットフォーム スイッチでは、レイヤ 3 モジュールを備え基本ライセンスまたは LAN Enterprise ライセンスがインストールされた VRF Lite がサポートされています。 これにより、VRF を作成し、その VRF に特定のインターフェイスを割り当てることができます。 旧リリースでは、管理 VRF、デフォルト VRF という 2 つの VRF がデフォルトで作成されます。 管理 VRF とデフォルト VRF には mgmt0 インターフェイスおよびすべての SVI インターフェイスが配置されます。

Cisco NX-OS ソフトウェアは、vPC ピア間でピアキープアライブ リンクを使用して、設定可能なキープアライブ メッセージを定期的に送信します。 これらのメッセージを送信するには、ピア デバイス間にレイヤ 3 接続が必要です。 ピアキープアライブ リンクが起動および動作していないと、システムは vPC ピア リンクを開始できません。

ピアキープアライブ メッセージに使用される送信元 IP アドレスと宛先の IP アドレスの両方が、ネットワーク内で一意であることを確認してください。また、vPC ピアキープアライブ リンクに関連付けられている Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）から、これらの IP アドレスが到達可能であることを確認してください。

（注） vPC ピアキープアライブ リンクを使用する際は、個別の VRF インスタンスを設定して、各 vPC ピア スイッチからその VRF にレイヤ 3 ポートを接続することが推奨されます。 ピア リンク自体を使用して vPC ピアキープアライブ メッセージを送信しないでください。 VRF の作成および設定に関する詳細については、『Cisco Nexus 5000 Series NX-OS Unicast Routing Configuration Guide, Release 5.0(3)N1(1)』を参照してください。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

システムで vPC ピア リンクを形成できるようにするには、まず vPC ピアキープアライブ リンクを設定する必要があります。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。手順は次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain** *domain-id*
3. switch(config-vpc-domain)# **peer-keepalive destination** *ipaddress* [**hold-timeout** *secs* | **interval** *msecs* {**timeout** *secs*} | **precedence** {*prec-value* | **network** | **internet** | **critical** | **flash-override** | **flash** | **immediate priority** | **routine**} | **tos** {*tos-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**} | **tos-byte** *tos-byte-value*} | **source** *ipaddress* | **vrf** {*name* | **management vpc-keepalive**}]
4. （任意） switch(config-vpc-domain)# **vpc peer-keepalive destination** *ipaddress* **source** *ipaddress*
5. （任意） switch# **show vpc peer-keepalive**
6. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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)# **vpc domain** *domain-id*	スイッチ上に vPC ドメインが存在しない場合はそれを作成し、vpc-domain 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-vpc-domain)# **peer-keepalive destination** *ipaddress* [**hold-timeout** *secs*	**interval** *msecs* {**timeout** *secs*}	**precedence** {*prec-value*	**network**	**internet**	**critical**	**flash-override**	**flash**	**immediate priority**	**routine**}	**tos** {*tos-value*	**max-reliability**	**max-throughput**	**min-delay**	**min-monetary-cost**	**normal**}	**tos-byte**	vPC ピアキープアライブ リンクのリモート エンドの IPv4 アドレスを設定します。 （注） vPC ピアキープアライブ リンクを設定するまで、vPC ピア リンクは構成されません。 管理ポートと VRF がデフォルトです。

	コマンドまたはアクション	目的
	tos-byte-value} | **source** *ipaddress* | **vrf** {*name* | **management vpc-keepalive**}]	
ステップ 4	switch(config-vpc-domain)# **vpc peer-keepalive destination** *ipaddress* **source** *ipaddress*	（任意） vPC ピアキープアライブ リンクに対し、個別の VRF インスタンスを設定して、各 vPC ピア デバイスからその VRF にレイヤ 3 ポートを接続します。
ステップ 5	switch# **show vpc peer-keepalive**	（任意） キープアライブ メッセージのコンフィギュレーションに関する情報を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ピアキープアライブ リンクの宛先 IP アドレスを設定する方法を示したものです。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# peer-keepalive destination 10.10.10.42
```

次に、プライマリとセカンダリの vPC デバイス間でピア キープアライブ リンク接続を設定する例を示します。

```
switch(config)# vpc domain 100
switch(config-vpc-domain)# peer-keepalive destination 192.168.2.2 source 192.168.2.1
Note:--------:: Management VRF will be used as the default VRF ::--------
switch(config-vpc-domain)#
```

次の例は、vPC ピアキープアライブ リンクに対して、vpc_keepalive という名前の VRF インスタンスを別途設定する方法、およびその新しい VRF を検査する方法を示したものです。

次の例は、vPC ピアキープアライブ リンクに対して、vpc_keepalive という名前の VRF インスタンスを別途設定する方法、およびその新しい VRF を検査する方法を示したものです。

```
vrf context vpc_keepalive
interface Ethernet1/31
  switchport access vlan 123
interface Vlan123
  vrf member vpc_keepalive
  ip address 123.1.1.2/30
  no shutdown
vpc domain 1
  peer-keepalive destination 123.1.1.1 source 123.1.1.2 vrf
vpc_keepalive

L3-NEXUS-2# sh vpc peer-keepalive

vPC keep-alive status           : peer is alive
--Peer is alive for             : (154477) seconds, (908) msec
--Send status                   : Success
--Last send at                  : 2011.01.14 19:02:50 100 ms
--Sent on interface             : Vlan123
```

```
--Receive status               : Success
--Last receive at              : 2011.01.14 19:02:50 103 ms
--Received on interface        : Vlan123
--Last update from peer         : (0) seconds, (524) msec

vPC Keep-alive parameters
--Destination                  : 123.1.1.1
--Keepalive interval           : 1000 msec
--Keepalive timeout            : 5 seconds
--Keepalive hold timeout       : 3 seconds
--Keepalive vrf                : vpc_keepalive
--Keepalive udp port           : 3200
--Keepalive tos                : 192

The services provided by the switch , such as ping, ssh, telnet,
radius, are VRF aware. The VRF name need to be configured or
specified in order for the correct routing table to be used.
L3-NEXUS-2# ping 123.1.1.1 vrf vpc_keepalive
PING 123.1.1.1 (123.1.1.1): 56 data bytes
64 bytes from 123.1.1.1: icmp_seq=0 ttl=254 time=3.234 ms
64 bytes from 123.1.1.1: icmp_seq=1 ttl=254 time=4.931 ms
64 bytes from 123.1.1.1: icmp_seq=2 ttl=254 time=4.965 ms
64 bytes from 123.1.1.1: icmp_seq=3 ttl=254 time=4.971 ms
64 bytes from 123.1.1.1: icmp_seq=4 ttl=254 time=4.915 ms

--- 123.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 3.234/4.603/4.971 ms
```

vPC ピア リンクの作成

vPC ピア リンクを作成する場合は、指定した vPC ドメインのピア リンクとする EtherChannel を各スイッチ上で指定します。 冗長性を確保するため、トランク モードで vPC ピア リンクとして指定する EtherChannel を設定し、各 vPC ピア スイッチで個別のモジュールの 2 つのポートを使用することを推奨します。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。手順は次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface port-channel** *channel-number*
3. switch(config-if)# **vpc peer-link**
4. （任意） switch# **show vpc brief**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 port-channel** *channel-number*	このスイッチの vPC ピア リンクとして使用する EtherChannel を選択し、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)# **vpc peer-link**	選択した EtherChannel を vPC ピア リンクとして設定し、vpc-domain 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# **show vpc brief**	（任意） vPC ピア リンクに関する情報など、各 vPC の情報を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ピア リンクを設定する方法を示します。

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# vpc peer-link
```

設定の互換性の検査

両側の vPC ピア スイッチに vPC ピア リンクを設定した後に、すべての vPC インターフェイスで設定に整合性があるかどうかの検査を行います。

（注） Cisco NX-OS Release 5.0(2)N1(1) 以降では、次の QoS パラメータでタイプ 2 整合性検査がサポートされています。

- Network QoS：MTU および Pause
- Input Queuing：Bandwidth および Absolute Priority
- Output Queuing：Bandwidth および Absolute Priority

タイプ 2 の不一致の場合、vPC は停止しません。 タイプ 1 の不一致が検出されると vPC は停止します。

パラメータ	デフォルト設定
switch# **show vpc consistency-parameters** {**global** | **interface port-channel** *channel-number*}	すべての vPC インターフェイス全体で一貫している必要があるパラメータのステータスを表示します。

次の例は、すべての vPC インターフェイスの間で必須設定の互換性が保たれているかチェックする方法を示します。

```
switch# show vpc consistency-parameters global
     Legend:
         Type 1 : vPC will be suspended in case of mismatch
Name                        Type  Local Value            Peer Value

------------- ----  ---------------------- -----------------------
QoS                         2     ([], [], [], [], [],   ([], [], [], [], [],
                                   [])                    [])

Network QoS (MTU)           2     (1538, 0, 0, 0, 0, 0)  (1538, 0, 0, 0, 0, 0)
Network Qos (Pause)         2     (F, F, F, F, F, F)     (1538, 0, 0, 0, 0, 0)
Input Queuing (Bandwidth)   2     (100, 0, 0, 0, 0, 0)   (100, 0, 0, 0, 0, 0)
Input Queuing (Absolute     2     (F, F, F, F, F, F)     (100, 0, 0, 0, 0, 0)
Priority)
Output Queuing (Bandwidth)  2     (100, 0, 0, 0, 0, 0)   (100, 0, 0, 0, 0, 0)
Output Queuing (Absolute    2     (F, F, F, F, F, F)     (100, 0, 0, 0, 0, 0)
Priority)
STP Mode                    1     Rapid-PVST             Rapid-PVST
STP Disabled                1     None                   None
STP MST Region Name         1     ""                     ""
STP MST Region Revision     1     0                      0
STP MST Region Instance to  1
  VLAN Mapping

STP Loopguard               1     Disabled               Disabled
STP Bridge Assurance        1     Enabled                Enabled
STP Port Type, Edge         1     Normal, Disabled,      Normal, Disabled,
BPDUFilter, Edge BPDUGuard        Disabled               Disabled
STP MST Simulate PVST       1     Enabled                Enabled
Allowed VLANs               -     1,624                  1
Local suspended VLANs       -     624                    -
switch#
```

次の例は、1 つの EtherChannel インターフェイスについて必須設定の互換性があるかどうか検査する方法を示したものです。

```
switch#  show vpc consistency-parameters interface port-channel 20

    Legend:
        Type 1 : vPC will be suspended in case of mismatch
Name                        Type  Local Value            Peer Value
-------------               ----  ---------------------- -----------------------
Fex id                      1     20                     20
STP Port Type               1     Default                Default
STP Port Guard              1     None                   None
STP MST Simulate PVST       1     Default                Default
mode                        1     on                     on
Speed                       1     10 Gb/s                10 Gb/s
Duplex                      1     full                   full
Port Mode                   1     fex-fabric             fex-fabric
Shut Lan                    1     No                     No
Allowed VLANs               -     1,3-3967,4048-4093     1-3967,4048-4093
```

vPC 自動リカバリのイネーブル化

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain** *domain-id*
3. switch(config-vpc-domain)# **auto-recovery reload-delay** *delay*

手順の詳細

	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)# **vpc domain** *domain-id*	既存の vPC ドメインに対して vpc-domain 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-vpc-domain)# **auto-recovery reload-delay** *delay*	自動リカバリ機能をイネーブルにし、リロード遅延時間を設定します。 デフォルトではディセーブルになっています。

次の例は、vPC ドメイン 10 で自動リカバリ機能をイネーブルにし、遅延時間を 240 秒に設定する方法を示したものです。

```
switch(config)# vpc domain 10
switch(config-vpc-domain)# auto-recovery reload-delay 240
Warning:
 Enables restoring of vPCs in a peer-detached state after reload, will wait for 240 seconds
 (by default) to determine if peer is un-reachable
```

次の例は、vPC ドメイン 10 における自動リカバリ機能のステータスを表示する方法を示したものです。

```
switch(config-vpc-domain)# show running-config vpc
!Command: show running-config vpc
!Time: Tue Dec  7 02:38:44 2010

version 5.0(2)N2(1)

feature vpc
vpc domain 10
  peer-keepalive destination 10.193.51.170
  auto-recovery
```

復元遅延時間の設定

Cisco NX-OS Release 5.0(3)N1(1) 以降では、ピアの隣接関係が確立され VLAN インターフェイスが再びアップ状態になるまで vPC の再稼働を遅延させるための復元タイマーを設定することができ

ます。 この機能により、vPCが再びトラフィックの受け渡しをし始める前にルーティングテーブルが収束できなかった場合のパケットのドロップを回避できます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。手順は次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain** *domain-id*
3. switch(config-vpc-domain)# **delay restore** *time*
4. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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)# **vpc domain** *domain-id*	スイッチ上に vPC ドメインが存在しない場合はそれを作成し、vpc-domain 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-vpc-domain)# **delay restore** *time*	vPC が復元されるまでの遅延時間を設定します。 復元時間は、復元された vPC ピア デバイスが稼働するまで遅延時間（単位は秒）です。 有効な範囲は 1 ～ 3600 です。 デフォルトは 30 秒です。
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、vPC リンクに対する復元遅延時間の設定方法を示したものです。

```
switch(config)# vpc domain 1
switch(config-vpc-domain)# delay restore 10
switch(config-vpc-domain)#
```

vPC ピア リンク障害発生時における VLAN インターフェイスのシャットダウン回避

vPC ピアリンクが失われると、vPC セカンダリ スイッチによりその vPC メンバ ポートおよび SVI インターフェイスが一時停止されます。 また、vPC セカンダリ スイッチのすべての VLAN に対して、レイヤ 3 転送はすべてディセーブルになります。 ただし、特定の SVI インターフェイスを一時停止の対象から除外することができます。

はじめる前に

VLAN インターフェイスが設定済みであることを確認します。

-

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain** *domain-id*
3. switch(config-vpc-domain))# **dual-active exclude interface-vlan** *range*

手順の詳細

	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)# **vpc domain** *domain-id*	スイッチ上に vPC ドメインが存在しない場合はそれを作成し、vpc-domain 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-vpc-domain))# **dual-active exclude interface-vlan** *range*	vPC ピアリンクが失われた場合でもアップ状態を維持する必要がある VLAN インターフェイスを指定します。 range：シャットダウンしないようにする VLAN インターフェイスの範囲を指定します。 有効な範囲は 1 ～ 4094 です。

次の例は、vPC ピア リンクに障害が発生した場合でも vPC ピア スイッチの VLAN 10 に対してインターフェイスのアップ状態を維持する方法を示したものです。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# dual-active exclude interface-vlan 10
switch(config-vpc-domain)#
```

VRF 名の設定

ping、ssh、telnet、radius などのスイッチ サービスは VRF 対応です。 適切なルーティング テーブルを使用するためには、VRF 名を設定する必要があります。

VRF 名を指定することができます。

手順の概要

1. switch# **ping** *ipaddress* **vrf** *vrf-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **ping** *ipaddress* **vrf** *vrf-name*	使用する仮想ルーティングおよび転送（VRF）を指定します。 VRF 名は、長さが最大 32 文字で、大文字と小文字は区別されます。

次の例は、vpc_keepalive という名前の VRF を指定する方法を示したものです。

```
switch# ping 123.1.1.1 vrf vpc_keepalive
PING 123.1.1.1 (123.1.1.1): 56 data bytes
64 bytes from 123.1.1.1: icmp_seq=0 ttl=254 time=3.234 ms
64 bytes from 123.1.1.1: icmp_seq=1 ttl=254 time=4.931 ms
64 bytes from 123.1.1.1: icmp_seq=2 ttl=254 time=4.965 ms
64 bytes from 123.1.1.1: icmp_seq=3 ttl=254 time=4.971 ms
64 bytes from 123.1.1.1: icmp_seq=4 ttl=254 time=4.915 ms

--- 123.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 3.234/4.603/4.971 ms
```

vPC への VRF インスタンスのバインド

VRF インスタンスを vPC にバインドすることができます。 VRF ごとに予約済みの VLAN が 1 つ必要です。 このコマンドを使用しないと、非 vPC VLAN 内のレシーバやレイヤ 3 インターフェイスに接続されているレシーバでは、マルチキャスト トラフィックを受信できない場合があります。 非 vPC VLAN は、ピアリンク上をトランクされない VLAN です。

はじめる前に

スイッチで使用するインターフェイスを表示する場合は、**show interfaces brief** コマンドを使用します。 VRF を vPC にバインドするためには、未使用の VLAN を使用する必要があります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc bind-vrf** *vrf-name* **vlan** *vlan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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)# **vpc bind-vrf** *vrf-name* **vlan** *vlan-id*	VRF インスタンスを vPC にバインドし、vPC にバインドする VLAN を指定します。 指定できる VLAN ID の範囲は 1 ～ 3967 および 4049 ～ 4093 です。

次の例は、VLAN 2 を使用して vPC をデフォルトの VRF にバインドする方法を示したものです。

```
switch(config)# vpc bind-vrf default vlan vlan2
```

vPC のゲートウェイ MAC アドレスを宛先とするレイヤ 3 転送のイネーブル化

Cisco NX-OS Release 5.0(3)N1(1) 以降、Cisco Nexus 5500 プラットフォーム スイッチにはこの機能が適用されます。

vPC ピアゲートウェイ機能により、vPC ピアのルータ MAC アドレスを宛先とするパケットに対し、vPC スイッチをアクティブなゲートウェイとして使用することができます。 これにより vPC ピアリンクを経由することなくローカルな転送が可能になります。 このシナリオでは、この機能によってピアリンクの使用が最適化され、トラフィック損失が回避されます。

仮想ポート チャネル（vPC）のゲートウェイ MAC アドレスを宛先とするパケットに対しては、レイヤ 3 転送をイネーブルにすることかできます。

（注） この機能は、両側の vPC ピア スイッチで設定する必要があります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain** *domain-id*
3. switch(config-vpc-domain))# **peer-gateway** *range*

手順の詳細

	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)# **vpc domain** *domain-id*	スイッチ上に vPC ドメインが存在しない場合はそれを作成し、vpc-domain 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-vpc-domain))# **peer-gateway** *range*	仮想ポート チャネル（vPC）のゲートウェイ MAC アドレスを宛先とするパケットに対してレイヤ 3 転送をイネーブルにします。

次の例は、vPC ピア ゲートウェイをイネーブルにする方法を示したものです。

```
switch(config)# vpc domain 20
switch(config-vpc-domain)# peer-gateway
switch(config-vpc-domain)#
```

vPC トポロジにおけるセカンダリ スイッチの孤立ポートの一時停止

セカンダリ vPC ピア リンクがダウンした場合、非仮想ポート チャネル（vPC）ポートを一時停止することができます。 非 vPC ポート（孤立ポート）とは、vPC に属していないポートです。

はじめる前に

vPC 機能がイネーブルであることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet** *slot*/*port*
3. switch(config-if)# **vpc orphan-port suspend**
4. switch(config-if)# **exit**
5. （任意） switch# **show vpc orphan-port**
6. （任意） switch# **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **interface ethernet** *slot*/*port*	設定するポートを指定し、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)# **vpc orphan-port suspend**	セカンダリ スイッチがダウンした場合に、指定したポートを一時停止します。 （注） **vpc-orphan-port suspend** コマンドは、物理ポート上でのみサポートされています。
ステップ 4	switch(config-if)# **exit**	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	switch# **show vpc orphan-port**	（任意） 孤立ポートの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、孤立ポートを一時停止する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet ⅛0
switch(config-if)# vpc orphan-port suspend
```

次の例は、vPC には属していないポートのうち、vPC に属しているポートと同じ VLAN を共有するポートの表示方法を示したものです。

```
switch# configure terminal
switch(config)# show vpc orphan-ports
Note:
--------::Going through port database. Please be patient.::--------
VLAN Orphan Ports
------- -------------------------
1 Po600
2 Po600
3 Po600
4 Po600
5 Po600
6 Po600
7 Po600
8 Po600
9 Po600
10 Po600
11 Po600
12 Po600
13 Po600
14 Po600
...
```

EtherChannel ホスト インターフェイスの作成

Cisco Nexus 2000 シリーズ ファブリック エクステンダからダウンストリーム サーバに接続するため、EtherChannel ホスト インターフェイスを作成することができます。 ファブリック エクステンダのモデルによっては、EtherChannel ホスト インターフェイス 1 つにつきメンバにできるホスト インターフェイスは 1 つだけです。 Cisco Nexus 2148T では、個々のファブリック エクステンダに対してメンバにできるインターフェイスは 1 つだけですが、新しいファブリック エクステンダでは、それぞれに対して同じポートチャネルを最大 8 個までメンバにすることができます。 EtherChannel ホスト インターフェイスでファブリック エクステンダのトポロジを使用する vPC を設定するためには、その EtherChannel ホスト インターフェイスを作成する必要があります。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

接続されているファブリック エクステンダがオンラインになっていることを確認します。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。手順は次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet** *chassis*/*slot*/*port*
3. switch(config-if)# **channel-group** *channel-number* **mode** {**active** | **passive** | **on**}
4. （任意） switch# **show port-channel summary**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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** *chassis*/*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)# **channel-group** *channel-number* **mode** {**active** | **passive** | **on**}	選択したホスト インターフェイスで EtherChannel ホスト インターフェイスを作成します。
ステップ 4	switch# **show port-channel summary**	（任意） 各 EtherChannel ホスト インターフェイスに関する情報を表示します。

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

次の例は、EtherChannel ホスト インターフェイスの設定方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 101/1/20
switch(config-if)# channel-group 7 mode active
```

他のポート チャネルの vPC への移行

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。手順は次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface port-channel** *channel-number*
3. switch(config-if)# **vpc** *number*
4. （任意） switch# **show vpc brief**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 port-channel** *channel-number*	vPC に配置してダウンストリーム スイッチに接続するポート チャネルを選択し、インターフェイス コンフィギュレーション モードを開始します。 （注） vPC は、通常のポート チャネル上（物理 vPC トポロジ）、ポート チャネルのファブリック インターフェイス上（ファブリック エクステンダの vPC トポロジ）、およびポート チャネルのホスト インターフェイス上（ホスト インターフェイスの vPC トポロジ）で設定できます。

	コマンドまたはアクション	目的
ステップ 3	switch(config-if)# **vpc** *number*	選択したポート チャネルを vPC に配置してダウンストリーム スイッチに接続するように設定します。 指定できる範囲は 1 ～ 4096 です。 vPC ピア スイッチからダウンストリーム デバイスに接続するポート チャネルに割り当てる vPC *number* は、両側の vPC ピア スイッチで同じであることが必要です。
ステップ 4	switch# **show vpc brief**	（任意） 各 vPC に関する情報を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、ダウンストリームデバイスに接続されるポートチャネルを設定する方法を示します。

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# vpc 5
```

vPC ドメイン MAC アドレスの手動での設定

（注） system-mac の設定を行うかどうかは任意です。 この項では、必要に応じてシステムの MAC アドレスを設定する方法について説明します。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。手順は次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain** *domain-id*
3. switch(config-vpc-domain)# **system-mac** *mac-address*
4. （任意） switch# **show vpc role**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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)# **vpc domain** *domain-id*	スイッチ上にある既存の vPC ドメインを選択するか、または新規の vPC ドメインを作成して、vpc-domain コンフィギュレーション モードを開始します。 *domain-id* のデフォルト値はありません。指定できる値の範囲は 1 ～ 1000 です。
ステップ 3	switch(config-vpc-domain)# **system-mac** *mac-address*	指定した vPC ドメインに割り当てる MAC アドレスを aaaa.bbbb.cccc の形式で入力します。
ステップ 4	switch# **show vpc role**	（任意） vPC システムの MAC アドレスを表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ドメインの MAC アドレスを設定する方法を示したものです。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-if)# system-mac 23fb.4ab5.4c4e
```

システム プライオリティの手動での設定

vPC ドメインを作成すると、vPC システム プライオリティが自動的に作成されます。 ただし、vPC ドメインのシステム プライオリティは手動で設定することもできます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。手順は次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain** *domain-id*
3. switch(config-vpc-domain)# **system-priority** *priority*
4. （任意） switch# **show vpc brief**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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)# **vpc domain** *domain-id*	スイッチ上にある既存の vPC ドメインを選択するか、または新規の vPC ドメインを作成して、vpc-domain コンフィギュレーション モードを開始します。 *domain-id* のデフォルト値はありません。指定できる値の範囲は 1 ～ 1000 です。
ステップ 3	switch(config-vpc-domain)# **system-priority** *priority*	指定した vPC ドメインに割り当てるシステム プライオリティを入力します。 指定できる値の範囲は、1 ～ 65535 です。 デフォルト値は 32667 です。
ステップ 4	switch# **show vpc brief**	（任意） vPC ピア リンクに関する情報など、各 vPC の情報を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ピア リンクを設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-if)# system-priority 4000
```

vPC ピア スイッチのロールの手動による設定

デフォルトの場合、Cisco NX-OS では、vPC ドメインおよび vPC ピア リンクの両側を設定した後、プライマリおよびセカンダリの vPC ピア スイッチが選択されます。 ただし、vPC のプライマリ スイッチとして、特定の vPC ピア スイッチを選択することもできます。 選択したら、プライマリ スイッチにする vPC ピア スイッチに、他の vPC ピア スイッチより小さいロール値を手動で設定します。

vPC はロールのプリエンプションをサポートしていません。 プライマリ vPC ピア スイッチに障害が発生すると、セカンダリ vPC ピア スイッチが、vPC プライマリ デバイスの機能を引き継ぎます。 ただし、以前のプライマリ vPC が再び稼働しても、機能のロールは元に戻りません。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。手順は次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain** *domain-id*
3. switch(config-vpc-domain)# **role priority** *priority*
4. （任意） switch# **show vpc brief**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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)# **vpc domain** *domain-id*	スイッチ上にある既存の vPC ドメインを選択するか、または新規の vPC ドメインを作成して、vpc-domain コンフィギュレーション モードを開始します。 *domain-id* のデフォルト値はありません。指定できる値の範囲は 1 ～ 1000 です。
ステップ 3	switch(config-vpc-domain)# **role priority** *priority*	vPC システム プライオリティとして使用するロール プライオリティを指定します。 指定できる値の範囲は、1 ～ 65535 です。 デフォルト値は 32667 です。
ステップ 4	switch# **show vpc brief**	（任意） vPC ピア リンクに関する情報など、各 vPC の情報を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ピア リンクを設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-if)# role priority 4000
```

vPC 設定の確認

vPC の設定情報を表示する場合は、次のコマンドを使用します。

コマンド	目的
switch# **show feature**	vPC がイネーブルかどうかを表示します。

コマンド	目的
switch# **show port-channel capacity**	設定されている EtherChannel の数、およびスイッチ上でまだ使用可能な EtherChannel の数を表示します。
switch# **show running-config vpc**	vPC の実行コンフィギュレーションの情報を表示します。
switch# **show vpc brief**	vPC に関する簡単な情報を表示します。
switch# **show vpc consistency-parameters**	すべての vPC インターフェイス全体で一貫している必要があるパラメータのステータスを表示します。
switch# **show vpc peer-keepalive**	ピアキープアライブ メッセージの情報を表示します。
switch# **show vpc role**	ピア ステータス、ローカル スイッチのロール、vPC システムの MAC アドレスとシステム プライオリティ、およびローカル vPC スイッチの MAC アドレスとプライオリティを表示します。
switch# **show vpc statistics**	vPC に関する統計情報を表示します。 （注） このコマンドは、現在作業している vPC ピア デバイスの vPC 統計情報しか表示しません。

スイッチの出力に関する詳細については、ご使用の Cisco Nexus シリーズ スイッチに関するコマンド リファレンスを参照してください。

グレースフル タイプ 1 検査ステータスの表示

グレースフル タイプ 1 整合性検査の現在のステータスを表示する場合は、**show vpc brief** コマンドを入力します。

```
switch# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Per-vlan consistency status     : success
Type-2 consistency status       : success
vPC role                          : secondary
Number of vPCs configured       : 34
Peer Gateway                      : Disabled
Dual-active excluded VLANs      : -
```

```
Graceful Consistency Check      : Enabled

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1
```

グローバル タイプ 1 不整合の表示

グローバル タイプ 1 不整合が発生すると、セカンダリ スイッチの vPC はダウンします。 次の例は、スパニングツリー モードでの不一致に伴って生じたこのタイプの不整合を示したものです。

一時停止した vPC VLAN のステータスを表示する場合は、セカンダリ スイッチに対して **show vpc** コマンドを入力します。

```
switch(config)# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                   : 10
Peer status                     : peer adjacency formed ok
vPC keep-alive status           : peer is alive
Configuration consistency status: failed
Per-vlan consistency status     : success
Configuration consistency reason: vPC type-1 configuration incompatible - STP
                                  Mode inconsistent
Type-2 consistency status       : success
vPC role                        : secondary
Number of vPCs configured       : 2
Peer Gateway                    : Disabled
Dual-active excluded VLANs      : -
Graceful Consistency Check      : Enabled

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1-10

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
20     Po20        down*  failed      Global compat check failed -
30     Po30        down*  failed      Global compat check failed -
```

不整合のステータスを表示する場合は、プライマリ スイッチに対して **show vpc** コマンドを入力します（プライマリ vPC の VLAN は一時停止しません）。

```
switch(config)# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                   : 10
Peer status                     : peer adjacency formed ok
vPC keep-alive status           : peer is alive
Configuration consistency status: failed
Per-vlan consistency status     : success
Configuration consistency reason: vPC type-1 configuration incompatible - STP Mo
de inconsistent
Type-2 consistency status       : success
vPC role                        : primary
Number of vPCs configured       : 2
Peer Gateway                    : Disabled
Dual-active excluded VLANs      : -
Graceful Consistency Check      : Enabled
```

```
vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1-10

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
20     Po20        up     failed      Global compat check failed 1-10
30     Po30        up     failed      Global compat check failed 1-10
```

インターフェイス別タイプ 1 不整合の表示

インターフェイス別タイプ 1 不整合が発生すると、セカンダリ スイッチの vPC ポートはダウンしますが、プライマリ スイッチの vPC ポートはアップ状態が維持されます。次の例は、スイッチポート モードでの不一致に伴って生じたこのタイプの不整合を示したものです。

一時停止した vPC VLAN のステータスを表示する場合は、セカンダリ スイッチに対して **show vpc brief** コマンドを入力します。

```
switch(config-if)# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Per-vlan consistency status     : success
Type-2 consistency status       : success
vPC role                          : secondary
Number of vPCs configured       : 2
Peer Gateway                      : Disabled
Dual-active excluded VLANs      : -
Graceful Consistency Check      : Enabled

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
20     Po20        up     success     success                    1
30     Po30        down*  failed      Compatibility check failed -
                                        for port mode
```

不整合のステータスを表示する場合は、プライマリ スイッチに対して **show vpc brief** コマンドを入力します（プライマリ vPC の VLAN は一時停止しません）。

```
switch(config-if)# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Per-vlan consistency status     : success
```

```
Type-2 consistency status       : success
vPC role                        : primary
Number of vPCs configured       : 2
Peer Gateway                    : Disabled
Dual-active excluded VLANs      : -
Graceful Consistency Check      : Enabled

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ -----------------------------------------------
1    Po1    up     1

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
20     Po20        up     success     success                    1
30     Po30        up     failed      Compatibility check failed 1
                                        for port mode
```

VLAN ごとの整合性ステータスの表示

VLAN ごとの整合性ステータスまたは不整合のステータスを表示する場合は、**show vpc consistency-parameters vlans** コマンドを入力します。

次の例では最初に、不整合が発生する前の（整合性がある状態での）VLAN のステータスが表示されています。 その後で **no spanning-tree vlan 5** コマンドを入力することにより、プライマリ スイッチとセカンダリ スイッチとの間に不整合が生じます。

show vpc brief コマンドを実行して、プライマリ スイッチおよびセカンダリ スイッチの VLAN の整合性ステータスを表示します。

```
switch(config-if)# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                   : 10
Peer status                     : peer adjacency formed ok
vPC keep-alive status           : peer is alive
Configuration consistency status: success
Per-vlan consistency status     : success
Type-2 consistency status       : success
vPC role                        : secondary
Number of vPCs configured       : 2
Peer Gateway                    : Disabled
Dual-active excluded VLANs      : -
Graceful Consistency Check      : Enabled

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ -----------------------------------------------
1    Po1    up     1-10

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
20     Po20        up     success     success                    1-10
30     Po30        up     success     success                    1-10
```

no spanning-tree vlan 5 コマンドを実行することにより、プライマリ VLAN とセカンダリ VLAN との間に不整合が生じます。

```
switch(config)# no spanning-tree vlan 5
```

セカンダリ スイッチに対して **show vpc brief** コマンドを実行すると、VLAN ごとの整合性ステータスが Failed と表示されます。

```
switch(config)# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Per-vlan consistency status       : failed
Type-2 consistency status         : success
vPC role                          : secondary
Number of vPCs configured         : 2
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1-4,6-10

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
20     Po20        up     success     success                    1-4,6-10
30     Po30        up     success     success                    1-4,6-10
```

プライマリ スイッチに対して **show vpc brief** コマンドを実行しても、VLAN ごとの整合性ステータスが Failed と表示されます。

```
switch(config)# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Per-vlan consistency status       : failed
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 2
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1-4,6-10

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
20     Po20        up     success     success                    1-4,6-10
30     Po30        up     success     success                    1-4,6-10
```

次の例では、STP Disabled という不整合が表示されています。

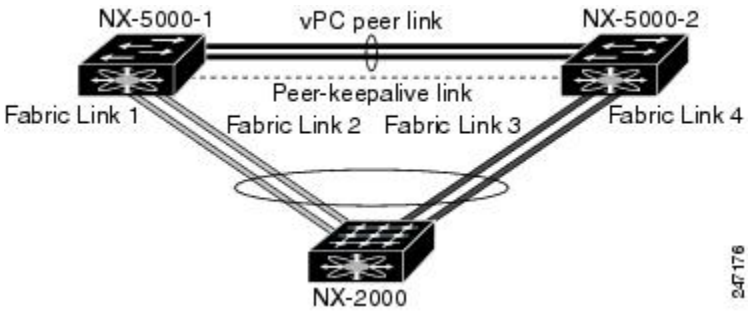
```
switch(config)# show vpc consistency-parameters vlans

Name                          Type  Reason Code              Pass Vlans

-------------                 ----  ---------------------- ------------------------
STP Mode                      1     success                0-4095
STP Disabled                  1     vPC type-1             0-4,6-4095
                                    configuration
                                    incompatible - STP is
                                    enabled or disabled on
                                     some or all vlans
STP MST Region Name           1     success                0-4095
STP MST Region Revision       1     success                0-4095
STP MST Region Instance to    1     success                0-4095
 VLAN Mapping
STP Loopguard                 1     success                0-4095
STP Bridge Assurance          1     success                0-4095
STP Port Type, Edge           1     success                0-4095
BPDUFilter, Edge BPDUGuard
STP MST Simulate PVST         1     success                0-4095
Pass Vlans                    -                            0-4,6-4095
```

vPC の設定例

デュアル ホーム ファブリック エクステンダにおける vPC の設定例

次の例は、スイッチ NX-5000-1 でピアキープアライブ メッセージを伝送するため、下図のような管理 VRF を使用したデュアル ホーム ファブリック エクステンダの vPC トポロジを設定する方法を示したものです。

図 *12* : *vPC* の設定例



はじめる前に

Cisco Nexus 2000 シリーズ ファブリック エクステンダの NX-2000-100 が接続され、かつオンラインになっていることを確認します。

手順の概要

1. vPC および LACP をイネーブルにします。
2. vPC ドメインを作成し、vPC ピアキープアライブ リンクを追加します。
3. vPC ピア リンクを 2 ポートの EtherChannel として設定します。
4. ファブリック エクステンダの識別子（100 など）を作成します。
5. ファブリック エクステンダ 100 に対してファブリック EtherChannel リンクを設定します。
6. 他のすべての手順と同様、両側の Nexus 5000 シリーズ スイッチで、ファブリック エクステンダ 100 の各ホスト インターフェイス ポートを設定します。
7. 設定を保存します。

手順の詳細

ステップ 1 vPC および LACP をイネーブルにします。

```
NX-5000-1# configure terminal
NX-5000-1(config)# feature lacp
NX-5000-1(config)# feature vpc
```

ステップ 2 vPC ドメインを作成し、vPC ピアキープアライブ リンクを追加します。

```
NX-5000-1(config)# vpc domain 1
NX-5000-1(config-vpc-domain)# peer-keepalive destination 10.10.10.237
NX-5000-1(config-vpc-domain)# exit
```

ステップ 3 vPC ピア リンクを 2 ポートの EtherChannel として設定します。

```
NX-5000-1(config)# interface ethernet 1/1-2
NX-5000-1(config-if-range)# switchport mode trunk
NX-5000-1(config-if-range)# switchport trunk allowed vlan 20-50
NX-5000-1(config-if-range)# switchport trunk native vlan 20
NX-5000-1(config-if-range)# channel-group 20 mode active
NX-5000-1(config-if-range)# exit
NX-5000-1(config)# interface port-channel 20
NX-5000-1(config-if)# vpc peer-link
NX-5000-1(config-if)# exit
```

ステップ 4 ファブリック エクステンダの識別子（100 など）を作成します。

```
NX-5000-1(config)# fex 100
NX-5000-1(config-fex)# pinning max-links 1
NX-5000-1(fex)# exit
```

ステップ 5 ファブリック エクステンダ 100 に対してファブリック EtherChannel リンクを設定します。

```
NX-5000-1(config)# interface ethernet 1/20
NX-5000-1(config-if)# channel-group 100
NX-5000-1(config-if)# exit
NX-5000-1(config)# interface port-channel 100
NX-5000-1(config-if)# switchport mode fex-fabric
NX-5000-1(config-if)# vpc 100
NX-5000-1(config-if)# fex associate 100
NX-5000-1(config-if)# exit
```

ステップ 6 他のすべての手順と同様、両側の Nexus 5000 シリーズ スイッチで、ファブリック エクステンダ 100 の各ホスト インターフェイス ポートを設定します。

```
NX-5000-1(config)# interface ethernet 100/1/1-48
NX-5000-1(config-if)# switchport mode access
NX-5000-1(config-if)# switchport access vlan 50
NX-5000-1(config-if)# no shutdown
NX-5000-1(config-if)# exit
```

ステップ 7 設定を保存します。

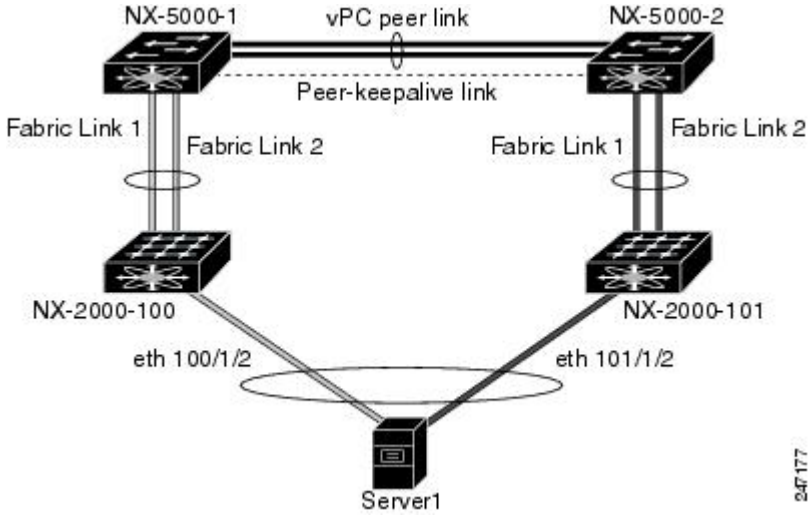
```
NX-5000-1(config)# copy running-config startup-config
```

NX-5000-2 スイッチに対して上記の手順を繰り返します。

シングル ホーム ファブリック エクステンダにおける vPC の設定例

次の例は、スイッチ NX-5000-1 でピアキープアライブ メッセージを伝送するため、下図のようなデフォルト VRF を使用したシングル ホーム ファブリック エクステンダの vPC トポロジを設定する方法を示したものです。

図 *13*：*vPC* の設定例



（注） 次の例は、ファブリック エクステンダの NX-2000-100 に接続された NX-5000-1 の設定方法だけを示したものです。 NX-5000-1 の vPC ピアである、ファブリック エクステンダの NX-2000-101 に接続された NX-5000-2 についても、これらの手順を繰り返す必要があります。

はじめる前に

Cisco Nexus 2000 シリーズ ファブリック エクステンダの NX-2000-100 と NX-2000-101 が接続され、かつオンラインになっていることを確認します。

手順の概要

1. vPC および LACP をイネーブルにします。
2. SVI インターフェイスをイネーブルにし、vPC ピアキープアライブ リンクで使用する VLAN および SVI を作成します。
3. vPC ドメインを作成し、vPC ピアキープアライブ リンクをデフォルト VRF に追加します。
4. vPC ピア リンクを 2 ポートの EtherChannel として設定します。
5. ファブリック エクステンダの NX-2000-100 を設定します。
6. ファブリック エクステンダの NX-2000-100 に対して、ファブリック EtherChannel リンクを設定します。
7. ファブリック エクステンダの NX-2000-100 に vPC サーバ ポートを設定します。
8. 設定を保存します。

手順の詳細

ステップ 1 vPC および LACP をイネーブルにします。

```
NX-5000-1# configure terminal
NX-5000-1(config)# feature lacp
NX-5000-1(config)# feature vpc
```

ステップ 2 SVI インターフェイスをイネーブルにし、vPC ピアキープアライブ リンクで使用する VLAN および SVI を作成します。

```
NX-5000-1(config)# feature interface-vlan
NX-5000-1(config)# vlan 900
NX-5000-1(config-vlan)# int vlan 900
NX-5000-1(config-if)# ip address 10.10.10.236 255.255.255.0
NX-5000-1(config-if)# no shutdown
NX-5000-1(config-if)# exit
```

ステップ 3 vPC ドメインを作成し、vPC ピアキープアライブ リンクをデフォルト VRF に追加します。

```
NX-5000-1(config)# vpc domain 30
NX-5000-1(config-vpc-domain)# peer-keepalive destination 10.10.10.237 source 10.10.10.236 vrf
default
NX-5000-1(config-vpc-domain)# exit
```

（注） VLAN 900 は、vPC ピアキープアライブ メッセージが伝送されるため、vPC ピアリンク上をトランク**されない**ようにする必要があります。 vPC ピアキープアライブ メッセージを伝送できるように、NX-5000-1 スイッチと NX-5000-2 スイッチの間には代替パスが必要です。

ステップ 4 vPC ピア リンクを 2 ポートの EtherChannel として設定します。

```
NX-5000-1(config)# interface ethernet 1/1-2
NX-5000-1(config-if-range)# switchport mode trunk
NX-5000-1(config-if-range)# switchport trunk allowed vlan 20-50
NX-5000-1(config-if-range)# switchport trunk native vlan 20
NX-5000-1(config-if-range)# channel-group 30 mode active
NX-5000-1(config-if-range)# exit
NX-5000-1(config)# interface port-channel 30
NX-5000-1(config-if)# vpc peer-link
NX-5000-1(config-if)# exit
```

ステップ 5 ファブリック エクステンダの NX-2000-100 を設定します。

```
NX-5000-1(config)# fex 100
NX-5000-1(config-fex)# pinning max-links 1
NX-5000-1(fex)# exit
```

ステップ 6 ファブリック エクステンダの NX-2000-100 に対して、ファブリック EtherChannel リンクを設定します。

```
NX-5000-1(config)# interface ethernet 1/20-21
NX-5000-1(config-if)# channel-group 100
NX-5000-1(config-if)# exit
NX-5000-1(config)# interface port-channel 100
NX-5000-1(config-if)# switchport mode fex-fabric
NX-5000-1(config-if)# fex associate 100
NX-5000-1(config-if)# exit
```

ステップ 7 ファブリック エクステンダの NX-2000-100 に vPC サーバ ポートを設定します。

```
NX-5000-1(config-if)# interface ethernet 100/1/1
NX-5000-1(config-if)# switchport mode trunk
NX-5000-1(config-if)# switchport trunk native vlan 100
NX-5000-1(config-if)# switchport trunk allowed vlan 100-105
NX-5000-1(config-if)# channel-group 600
NX-5000-1(config-if)# no shutdown
NX-5000-1(config-if)# exit
NX-5000-1(config)# interface port-channel 600
NX-5000-1(config-if)# vpc 600
NX-5000-1(config-if)# no shutdown
NX-5000-1(config-if)# exit
```

ステップ 8 設定を保存します。

```
NX-5000-1(config)# copy running-config startup-config
```

vPC のデフォルト設定

次の表は、vPC パラメータのデフォルト設定をまとめたものです。

表 *9*：デフォルト *vPC* パラメータ

パラメータ	デフォルト
vPC システム プライオリティ	32667
vPC ピアキープアライブ メッセージ	ディセーブル
vPC ピアキープアライブ間隔	1 秒
vPC ピアキープアライブ タイムアウト	5 秒
vPC ピアキープアライブ UDP ポート	3200

第 10 章

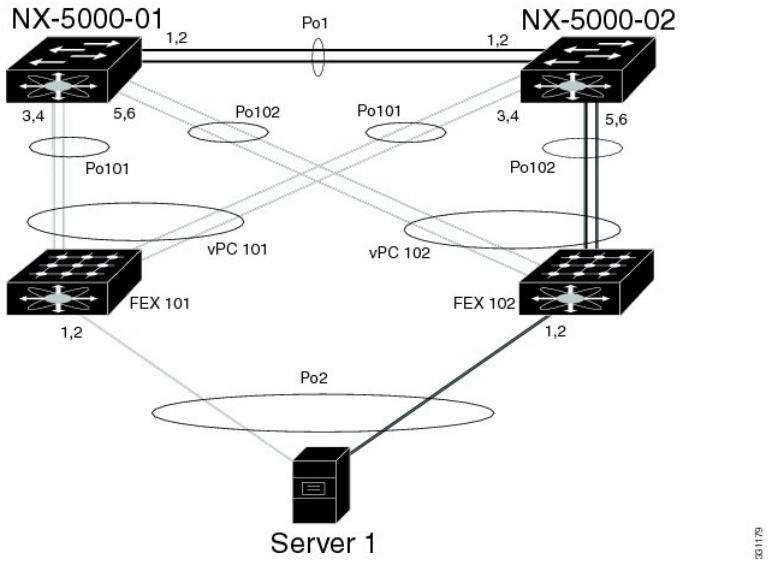
拡張仮想ポート チャネルの設定

この章の内容は、次のとおりです。

拡張 vPC について

拡張仮想ポート チャネルの概要

仮想ポート チャネル（vPC）機能により、ホストから 2 つのファブリック エクステンダ（FEX）へのデュアル ホーム接続または FEX から 2 つのスイッチへのデュアルホーム接続が可能になります。 拡張 vPC 機能、つまり、2 レイヤ vPC により、次の図のように 2 つのデュアル ホーミング トポロジを同時に組み合わせることができます。



拡張 vPC では、ホストから FEX、および FEX からスイッチへのパスがアクティブとなり、使用可能なすべてのパスがアクティブとなり、イーサネット トラフィックを伝送し、使用可能な帯域幅を最大限に活用し、両方のレベルで冗長性を提供します。

vPC については、仮想ポート チャネルの設定, （125 ページ）を参照してください。

サポートされているプラットフォームとトポロジ

サポートされているプラットフォーム

拡張 vPC は、NX-OS Release 5.1(3)N1(1) 以降のリリースを実行している Cisco Nexus 5500 プラットフォーム でサポートされます。

すべての Cisco Nexus 2000 シリーズ ファブリック エクステンダは、拡張 vPC と組み合わせて使用できます。

拡張 vPC は、スイッチでレイヤ 3 機能と互換性があります。

サポートされているトポロジとサポートされていないトポロジ

拡張 vPC では、次のトポロジをサポートしています。

- 単一の FEX に接続されているシングルホーム接続サーバ
- ポート チャネルによって単一の FEX に接続されているデュアルホーム接続サーバ
- ポート チャネルによって FEX のペアに接続されているデュアルホーム接続サーバ

  このトポロジにより、vPC ドメインで同一のスイッチ ペアに接続されている 2 つの FEX への接続が可能になります。 スタティック ポート チャネルと LACP ベースのポート チャネルがサポートされています。

- FCoE とポート チャネルによって FEX のペアに接続されているデュアルホーム接続サーバ

- アクティブ/スタンバイ NIC チーミングによって FEX のペアに接続されているデュアルホーム接続サーバ

拡張 vPC は次のトポロジをサポートしていません。

- 1 つのスイッチに接続する FEX のペアに接続されているデュアルホーム接続サーバ

  このトポロジは 1 つのスイッチに障害が発生した場合に機能するシステムになりますが、これは通常の動作で推奨されません。

- ポート チャネルによって 2 つを超える FEX に接続されているマルチホーム接続サーバ

  このトポロジによって、複雑性が増し、利点がほとんどなくなります。

拡張 vPC のスケーラビリティ

拡張 vPC のスケーラビリティは、デュアルホーム接続 FEX トポロジのスケーラビリティと似ています。

各 Cisco Nexus 5500 プラットフォーム スイッチは、最大 24 台の FEX（レイヤ 3 設定なし）または 8 台の FEX（レイヤ 3 設定あり）をサポートしています。 デュアルホーム接続 FEX トポロジでは、拡張 vPC の場合のように各 FEX は 2 つのスイッチによって管理されるため、ペアも同時に 24 台または 8 台の FEX をサポートします。

拡張 vPC の失敗応答

拡張 vPC トポロジにより、次のシナリオで説明しているシステム コンポーネントおよびリンクの障害の高レベルの復元力が実現します。

- ポート チャネルの 1 つ以上のメンバ リンクの障害

  ポート チャネルの 1 つのメンバ リンクに障害が発生した場合、トラフィック フローはポート チャネルの残りのメンバ リンクに移動されます。 ポート チャネルのすべてのメンバ リンクに障害が発生した場合、トラフィック フローは vPC の残りのポート チャネルにリダイレクトされます。

- 1 つの FEX の障害

  1 つの FEX に障害が発生した場合、すべてのデュアルホーム接続ホストからのトラフィック フローは残りの FEX に移動されます。

- 1 つのスイッチの障害

  1 つのスイッチに障害が発生した場合、すべてのデュアルホーム接続 FEX からのトラフィック フローは残りのスイッチに移動されます。 ホストからのトラフィックは影響を受けません。

- 1 つの FEX からの両方のアップリンクの障害

1 つの FEX からの両方のアップリンクに障害が発生した場合、FEX はそのホスト ポートをシャットダウンし、すべてのデュアルホーム接続ホストからのトラフィック フローは他の FEX に移動されます。

- vPC ピア リンクの障害

  vPC セカンダリ スイッチでピア リンクの障害が検出される場合、ピアキープアライブ リンクを介してプライマリ スイッチのステータスを確認します。 プライマリ スイッチが応答しない場合には、セカンダリ スイッチはすべてのトラフィック フローを元どおりに保持します。 プライマリ スイッチがアクティブな場合には、セカンダリ スイッチはその FEX へのインターフェイスをシャットダウンし、すべてのデュアルホーム接続FEXからのトラフィックフローはプライマリ スイッチに移動されます。 いずれの場合でも、ホストからのイーサネット トラフィックは影響を受けません。

  セカンダリ スイッチがFCoEトラフィックを伝送してそのFEXへのインターフェイスをシャットダウンする場合、FEX ホスト ポートにバインドされるすべての仮想ファイバ チャネル（vFC）インターフェイスもシャットダウンします。 この場合、ホストでは、マルチパスを使用して SAN トラフィックを残りの vFC インターフェイスに移動する必要があります。

- vPC ピアキープアライブ リンクの障害

  vPC ピアキープアライブ リンクの障害自体は、トラフィック フローに影響しません。

拡張 vPC のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	この機能には、ライセンスは必要ありません。 ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 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。

拡張 vPC の設定

拡張 vPC 設定手順の概要

拡張 vPC 設定は、2 つの標準 vPC 設定（ホストから 2 つのファブリック エクステンダへのデュアルホーム接続とファブリック エクステンダから 2 つのスイッチへのデュアルホーム接続）の組み合わせで構成されています。 ここでは、必要な設定作業について説明しますが、この 2 つの標準設定の詳細な手順については、このマニュアルの「仮想ポート チャネルの設定」に記述されています。

拡張 vPC を設定するには、次のステップを実行します。 特に明記されていない限り、各ステップの手順は仮想ポート チャネルの設定, （125 ページ）に記載されています。

（注） 両方のスイッチで設定を繰り返す必要がある手順では、設定の同期（config-sync）機能を使用すると、1つのスイッチを設定し、その設定が自動的にピア スイッチに同期されるようにすることができます。 設定の同期については、『*Cisco Nexus 5000 Series NX-OS Operations Guide*』を参照してください。

ステップ 1 各スイッチで vPC 機能と LACP 機能をイネーブルにします。

ステップ 2 各スイッチで必要な VLAN を作成します。

ステップ 3 vPC ドメイン ID を割り当てて、各スイッチで vPC ピアキープアライブ リンクを設定します。

ステップ 4 各スイッチで vPC ピア リンクを設定します。

ステップ 5 最初の FEX から各スイッチへのポート チャネルを設定します。

ステップ 6 2 番めの FEX から各スイッチへのポート チャネルを設定します。

ステップ 7 拡張 vPC が FCoE トラフィックに対応する必要がある場合、最初の FEX を 1 つのスイッチにアソシエートし、2 番めの FEX をもう一方のスイッチにアソシエートします。
『*Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide*』の「拡張 vPC での FCoE の設定」を参照してください。

ステップ 8 各 FEX でホスト ポート チャネルを設定します。

拡張 vPC の確認

拡張 vPC 設定の確認

vPC を使用し始める前に、同じ vPC ドメインの 2 つのピア スイッチでは、両方のスイッチで vPC トポロジの設定に互換性があるかについて確認するため、設定情報がやり取りされます。 設定不一致の場合の影響の重大度によって、一部の設定パラメータはタイプ 1 整合性検査パラメータと見なされ、一部はタイプ 2 と見なされます。

タイプ 1 パラメータで不一致が見つかると、両方のピア スイッチで vPC ポート上の VLAN が停止されます。 タイプ 2 パラメータで不一致が見つかると、警告の Syslog メッセージが生成されますが、vPC はアップ状態で実行中のままです。

（注） 拡張 vPC では、グレースフル整合性検査はサポートされていません。

拡張vPCのグローバル コンフィギュレーション パラメータに対する整合性検査は、デュアルホーム接続 FEX トポロジに対するものと同じであり、デュアルホーム接続 FEX のマニュアルに記載されています。 グローバル整合性検査に加え、拡張 vPC では、ここで説明されている作業によるインターフェイス レベルの検査が必要です。

次のコマンドを使用して、拡張 vPC の設定と整合性を確認します。

コマンド	目的
switch# **show feature**	vPC がイネーブルになっているかどうかを表示します。
switch# **show running-config vpc**	vPC の実行コンフィギュレーションの情報を表示します。
switch# **show vpc brief**	vPC に関する簡単な情報を表示します。
switch(config)# **show vpc consistency-parameters global**	すべての vPC インターフェイス全体で一貫している必要がある vPC グローバル パラメータのステータスを表示します。
switch(config)# **show vpc consistency-parameters interface port-channel** *channel-number*	vPC デバイス全体で一貫している必要がある特定のポート チャネルのステータスを表示します。

これらのコマンドの出力フィールドの詳細については、『*Cisco Nexus 5000 Series Command Reference*』を参照してください。

ポート チャネル番号の整合性の確認

拡張vPCの両方のスイッチでは、FEXへのデュアルホーム接続の同じポート チャネル番号を使用する必要があります。 異なるポート チャネル番号を使用すると、両方のスイッチでポート チャネルとそのメンバ ポートが停止されます。

この手順では、ポート チャネル番号設定の整合性を確認します。

手順の概要

1. **show running-config interface** *type/slot*[, *type/slot*[, ...]]
2. **show interface** *type/slot*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show running-config interface** *type/slot*[, *type/slot*[, ...]] 例： `switch-1# show running-config interface Ethernet110/1/1, Ethernet111/1/1`	ポート チャネル メンバ ポートの指定されたリストの設定を表示します。 両方のピア スイッチでこのコマンドを実行し、報告された **channel-group** 番号を比較して、スイッチ間でそれらの番号が一致していることを確認します。
ステップ 2	**show interface** *type/slot* 例： `switch-1# show interface Ethernet110/1/1`	指定されたポート チャネル メンバ ポートのステータスと設定を表示します。 両方のピア スイッチでこのコマンドを実行し、ポートのステータスを確認します。

次の例は、2つのスイッチ間でポート チャネル番号設定の整合性を確認する方法を示しています。次の例では、ポート チャネル番号設定が不整合であるため、メンバ ポートは停止されます。

```
switch-1# show running-config interface Ethernet110/1/1, Ethernet111/1/1

!Command: show running-config interface Ethernet110/1/1, Ethernet111/1/1
!Time: Sun Aug 28 03:38:23 2011

version 5.1(3)N1(1)

interface Ethernet110/1/1
channel-group 102

interface Ethernet111/1/1
channel-group 102

switch-2# show running-config interface Ethernet110/1/1, Ethernet111/1/1

!Command: show running-config interface Ethernet110/1/1, Ethernet111/1/1
!Time: Sun Aug 28 03:38:23 2011

version 5.1(3)N1(1)

interface Ethernet110/1/1
channel-group 101

interface Ethernet111/1/1
channel-group 101

switch-1# show interface Ethernet110/1/1
Ethernet110/1/1 is down (suspended by vpc)
  Hardware: 100/1000 Ethernet, address: 7081.0500.2402 (bia 7081.0500.2402)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec
  [...]

switch-2# show interface Ethernet110/1/1
Ethernet110/1/1 is down (suspended by vpc)
  Hardware: 100/1000 Ethernet, address: 7081.0500.2402 (bia 7081.0500.2402)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec
  [...]
```

共通のポート チャネル番号の確認

2 つのスイッチ間に共通のポート チャネル メンバが少なくとも 1 つあれば、FEX からスイッチ ペアへのポート チャネルはアップし、動作します。 1 つのスイッチでのみポート チャネルが割り当てられている FEX インターフェイスは停止されます。

手順の概要

1. **show port-channel summary**
2. （任意） **show interface** *type/slot*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show port-channel summary** 例： `switch-1# show port-channel summary`	ポート チャネル インターフェイスの概要を表示します。
ステップ 2	**show interface** *type/slot* 例： `switch-1# show interface ethernet 111/1/3`	（任意） 指定されたインターフェイスのステータスと設定を表示します。

次の例は、vPC の共通のメンバ ポートを確認する方法を示しています。 次の例では、vPC は両方のスイッチに共通していない 1 つのチャネル メンバを使用して設定されています。 そのメンバ ポートはシャットダウンとして示され、詳細な検査でメンバが vPC によって停止されていることが示されます。 このセッション部分では、各スイッチでポート チャネルが設定され、最初のスイッチに追加ポートがあります。

```
switch-1(config)# interface ethernet 110/1/3, ethernet 111/1/3
switch-1(config-if)# channel-group 101
switch-1(config-if)# interface port-channel 101
switch-1(config-if)# switchport access vlan 20

switch-2(config)# interface ethernet 110/1/3
switch-2(config-if)# channel-group 101
switch-2(config-if)# interface port-channel 101
switch-2(config-if)# switchport access vlan 20
```

このセッション部分では、追加ポートはダウン状態であると示され、ポート詳細の表示にポートが vPC によって停止されていることが示されます。

```
switch-1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
```

```
Group Port-       Type     Protocol  Member Ports
      Channel
------------------------------------------------------------------------------
1     Po1(SU)     Eth      LACP      Eth1/1(P)    Eth1/2(P)
[...]
101   Po101(SU)   Eth      NONE      Eth110/1/3(P)  Eth111/1/3(D)

switch-1# show interface ethernet 111/1/3
Ethernet111/1/3 is down (suspended by vpc)
  Hardware: 100/1000 Ethernet, address: 7081.0500.2582 (bia 7081.0500.2582)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec
  reliability 255/255, txload 1/255, rxload 1/255
```

拡張 vPC のインターフェイス レベルの整合性の確認

vPC の場合、ポート チャネル インターフェイス設定でポート モードおよび共有 VLAN の整合性をとるようにする必要があります。

この手順では、設定が vPC インターフェイスで一貫していることを確認します。

手順の概要

1. **show vpc consistency-parameters port-channel** *channel-number*

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**show vpc consistency-parameters port-channel** *channel-number*
	
	例：
	`switch# show vpc consistency-parameters interface port-channel 101`
	`switch(config)#`
		指定したポート チャネルの場合、vPC デバイス全体で一貫している必要があるステータス情報を表示します。

次の例は、vPC の 2 つのピア間でのインターフェイス設定も比較を表示する方法を示しています。この場合、VLAN 10 が両方のピアで許可されていますが、ポート モードが一致しないため、VLAN は停止されます。

```
NX-5000-1# show vpc consistency-parameters interface port-channel 101

    Legend:
        Type 1 : vPC will be suspended in case of mismatch

Name                        Type  Local Value            Peer Value
-------------               ----  ---------------------- -----------------------
mode                        1     on                     on
Speed                       1     1000 Mb/s              1000 Mb/s
Duplex                      1     full                   full
Port Mode                   1     access                 trunk
MTU                         1     1500                   1500
Admin port mode             1
Shut Lan                    1     No                     No
vPC+ Switch-id              1     3000                   3000
```

```
Allowed VLANs               -     10                    1-57,61-3967,4048-4093
Local suspended VLANs       -     10                    -
```

拡張 vPC の設定例

次の例は、この章の拡張 vPC 図のトポロジを使用した完全な設定手順を示しています。 トポロジ図では、各ポート チャネル リンクの横にある番号ペアは、インターフェイス ポート番号を表します。 たとえば、番号「3、4」というラベルが付いたスイッチ リンクは、スイッチ上のインターフェイス eth1/3 および eth1/4 を表します。

（注） 両方のスイッチで設定を繰り返す必要がある手順では、設定の同期（config-sync）機能を使用すると、1 つのスイッチを設定し、その設定が自動的にピア スイッチに同期されるようにすることができます。 設定の同期については、『*Cisco Nexus 5000 Series NX-OS Operations Guide*』を参照してください。

はじめる前に

Cisco Nexus 2000 シリーズ ファブリック エクステンダ FEX101 および FEX102 が接続され、オンラインであることを確認してください。

手順の概要

1. 各スイッチで vPC 機能と LACP 機能をイネーブルにします。
2. 各スイッチで必要な VLAN を作成します。
3. vPC ドメイン ID を割り当てて、各スイッチで vPC ピアキープアライブ リンクを設定します。
4. 各スイッチで vPC ピア リンクを設定します。
5. 最初の FEX から各スイッチへのポート チャネルを設定します。
6. 2 番めの FEX から各スイッチへのポート チャネルを設定します。
7. 各 FEX でホスト ポート チャネルを設定します。

手順の詳細

ステップ 1 各スイッチで vPC 機能と LACP 機能をイネーブルにします。

例：

```
NX-5000-1(config)# feature vpc
NX-5000-1(config)# feature lacp

NX-5000-2(config)# feature vpc
NX-5000-2(config)# feature lacp
```

ステップ 2 各スイッチで必要な VLAN を作成します。

例：
```
NX-5000-1(config)# vlan 10-20

NX-5000-2(config)# vlan 10-20
```

ステップ 3 vPC ドメイン ID を割り当てて、各スイッチで vPC ピアキープアライブ リンクを設定します。

例：
```
NX-5000-1(config)# vpc domain 123
NX-5000-1(config-vpc)# peer-keepalive destination 172.25.182.100

NX-5000-2(config)# vpc domain 123
NX-5000-2(config-vpc)# peer-keepalive destination 172.25.182.99
```

（注） 各スイッチを設定する際に、ピア スイッチの IP アドレスをピアキープアライブの宛先として使用します。

ステップ 4 各スイッチで vPC ピア リンクを設定します。

例：
```
NX-5000-1(config)# interface eth1/1-2
NX-5000-1(config-if)# channel-group 1 mode active
NX-5000-1(config-if)# interface Po1
NX-5000-1(config-if)# switchport mode trunk
NX-5000-1(config-if)# switchport trunk allowed vlan 1, 10-20
NX-5000-1(config-if)# vpc peer-link

NX-5000-2(config)# interface eth1/1-2
NX-5000-2(config-if)# channel-group 1 mode active
NX-5000-2(config-if)# interface Po1
NX-5000-2(config-if)# switchport mode trunk
NX-5000-2(config-if)# switchport trunk allowed vlan 1, 10-20
NX-5000-2(config-if)# vpc peer-link
```

ステップ 5 最初の FEX から各スイッチへのポート チャネルを設定します。

例：
```
NX-5000-1(config)# fex 101
NX-5000-1(config-fex)# interface eth1/3-4
NX-5000-1(config-if)# channel-group 101
NX-5000-1(config-if)# interface po101
NX-5000-1(config-if)# switchport mode fex-fabric
NX-5000-1(config-if)# vpc 101
NX-5000-1(config-if)# fex associate 101

NX-5000-2(config)# fex 101
NX-5000-2(config-fex)# interface eth1/3-4
NX-5000-2(config-if)# channel-group 101
NX-5000-2(config-if)# interface po101
NX-5000-2(config-if)# switchport mode fex-fabric
NX-5000-2(config-if)# vpc 101
NX-5000-2(config-if)# fex associate 101
```

ステップ 6 2 番めの FEX から各スイッチへのポート チャネルを設定します。

例：
```
NX-5000-1(config)# fex 102
NX-5000-1(config-fex)# interface eth1/5-6
```

```
NX-5000-1(config-if)# channel-group 102
NX-5000-1(config-if)# interface po102
NX-5000-1(config-if)# switchport mode fex-fabric
NX-5000-1(config-if)# vpc 102
NX-5000-1(config-if)# fex associate 102

NX-5000-2(config)# fex 102
NX-5000-2(config-fex)# interface eth1/5-6
NX-5000-2(config-if)# channel-group 102
NX-5000-2(config-if)# interface po102
NX-5000-2(config-if)# switchport mode fex-fabric
NX-5000-2(config-if)# vpc 102
NX-5000-2(config-if)# fex associate 102
```

ステップ 7 各 FEX でホスト ポート チャネルを設定します。

例：

```
NX-5000-1(config)# interface eth101/1/1, eth101/1/2
NX-5000-1(config-if)# channel-group 2 mode active
NX-5000-1(config-if)# interface eth102/1/1, eth102/1/2
NX-5000-1(config-if)# channel-group 2 mode active
NX-5000-1(config-if)# int po2
NX-5000-1(config-if)# switchport access vlan 10

NX-5000-2(config)# interface eth101/1/1, eth101/1/2
NX-5000-2(config-if)# channel-group 2 mode active
NX-5000-2(config-if)# interface eth102/1/1, eth102/1/2
NX-5000-2(config-if)# channel-group 2 mode active
NX-5000-2(config-if)# int po2
NX-5000-2(config-if)# switchport access vlan 10
```

第 11 章

Rapid PVST+ の設定

この章の内容は、次のとおりです。

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 が稼働するデバイスと相互運用されます。

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

（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 *14*：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 の一意の識別情報として機能します。

表 *10*：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

各 VLAN では、ブリッジ ID の数値が最も小さいスイッチが、ルート ブリッジとして選択されます。 すべてのスイッチがデフォルトのプライオリティ（32768）で設定されている場合、その VLAN で最小の MAC アドレスを持つスイッチが、ルート ブリッジになります。 ブリッジ プライオリティ値はブリッジ ID の最上位ビットを占めます。

ブリッジのプライオリティの値を変更すると、スイッチがルート ブリッジとして選定される可能性を変更することになります。 小さい値を設定するほどその可能性が大きくなり、大きい値を設定するほどその可能性は小さくなります。

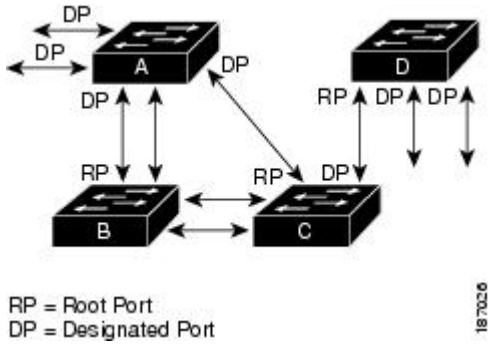
STP ルートブリッジは論理的に、ネットワークで各スパニングツリー トポロジの中心です。 ネットワークの任意の箇所からルート ブリッジに到達するために必要ではないすべてのパスは、STP ブロッキング モードになります。

BPDU には、送信側ブリッジおよびそのポートについて、ブリッジおよびMAC アドレス、ブリッジ プライオリティ、ポート プライオリティ、パス コストなどの情報が含まれます。 STP では、この情報を使用して、STP インスタンス用のルート ブリッジを選定し、ルート ブリッジに導くルート ポートを選択し、各セグメントの指定ポートを特定します。

スパニングツリー トポロジの作成

次の図では、スイッチ A がルートブリッジに選定されます。これは、すべてのスイッチでブリッジ プライオリティがデフォルト（32768）に設定されており、スイッチ A の MAC アドレスが最小であるためです。 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 *15*：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収束が行われます。 Rapid PVST+ によりスパニングツリーの再設定を 1 秒未満に発生させることができます（802.1D STP のデフォルト設定では 50 秒）。

（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 収束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。 エッジ ポート、新しいルート ポート、ポイントツーポイント リンクで接続したポートに、高速コンバージェンスが次のように提供されます。

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

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

（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。

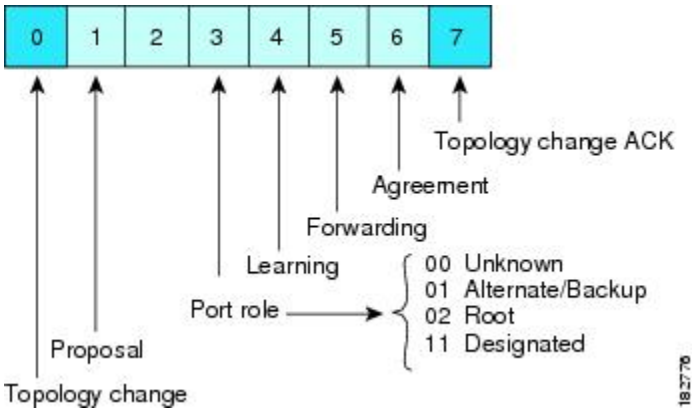
（注） スイッチが、レガシー 802.1D STP を実行しているスイッチと相互に動作しているときにのみ、TCA フラグが使用されます。

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 フラグの使用法を示します。

図 *16*： *BPDU* の *Rapid PVST+* フラグ バイト

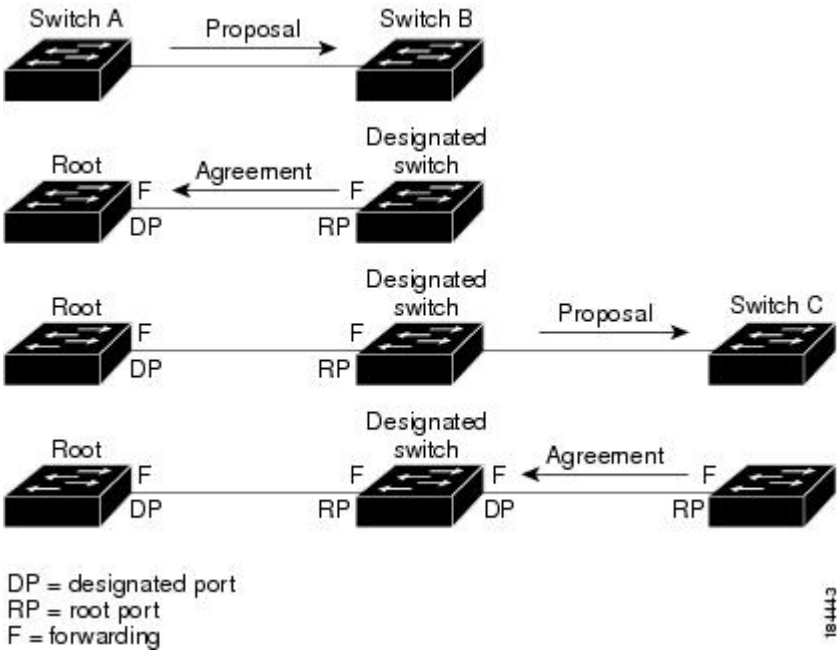


もう一つの重要な変更点は、Rapid PVST+ BPDU がタイプ 2、バージョン 2 であることで、これにより、スイッチでは、接続されているレガシー（802.1D）ブリッジを検出できるようになります。802.1D の BPDU は、バージョン 0 です。

提案と合意のハンドシェイク

次の図のように、スイッチ A は、ポイントツーポイント リンクを介してスイッチ B に接続され、すべてのポートがブロッキング ステートになります。 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 *17*：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 ポートを使って合意メッセージ（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のたびに、この提案と合意のハンドシェイクが、ルートからスパニングツリーの末端に向かって進みます。

スイッチは、ポート デュプレックス モードからリンク タイプを認識します。全二重ポートはポイントツーポイント接続であると見なされ、半二重ポートは共有接続であると見なされます。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するプロトコル タイマーを示します。

表 *11*： *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

ポートのロール

Rapid PVST+ では、ポートのロールを割り当て、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。

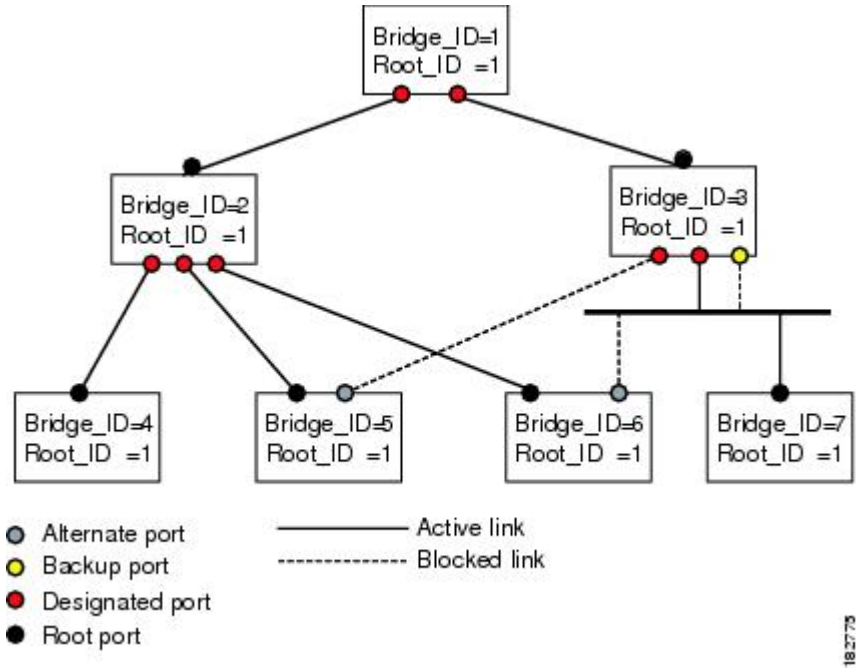
- ルート ポート：スイッチによりパケットがルート ブリッジに転送されるときに、最適のパス（最小コスト）を用意します。

- 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何もロールが与えられていません。

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

ルート ポートまたは指定ポートのロールを持つポートは、アクティブなトポロジに含まれます。代替ポートまたはバックアップ ポートのロールを持つポートは、アクティブなトポロジから除外されます（次の図を参照）。

図 *18*： ポートのロールをデモンストレーションするトポロジのサンプル



ポート ステート

Rapid PVST+ ポート ステートの概要

プロトコル情報がスイッチド LAN を通過するとき、伝播遅延が生じることがあります。 その結果、スイッチドネットワークのさまざまな時点および場所でトポロジー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ー情報がスイッチドLAN経由で伝播されるまで待機し、それからフレーム転送を開始する必要があります。

Rapid PVST+ または MST を使用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 モジュールから送られた BPDU を受信し、処理して送信します。
- ネットワーク管理メッセージを受信して応答します。

ラーニング ステート

ラーニング ステートにある LAN ポートは、フレームの MAC アドレスをラーニングすることによって、フレーム転送の準備をします。 LAN ポートは、ブロッキング ステートからラーニング ステートになります。

ラーニング ステートの LAN ポートでは、次の処理が実行されます。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- エンド ステーションの場所を、そのアドレス データベースに取り入れます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから送られた BPDU を受信し、処理して送信します。
- ネットワーク管理メッセージを受信して応答します。

フォワーディング ステート

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

フォワーディング ステートの LAN ポートでは、次の処理が実行されます。

- 接続セグメントから受信したフレームを転送します。
- 転送用に他のポートからスイッチングされたフレームを転送します。
- エンド ステーションの場所情報を、そのアドレス データベースに取り入れます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから受信した BPDU を処理します。
- ネットワーク管理メッセージを受信して応答します。

ディセーブル ステート

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

ディセーブルの LAN ポートでは、次の処理が実行されます。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- エンド ステーションの場所は、そのアドレス データベースには取り入れません （ラーニングは行われないため、アドレス データベースは更新されません）。
- ネイバーから BPDU を受信しません。
- システム モジュールから送信用の BPDU を受信しません。

ポート ステートの概要

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

表 *12*：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。

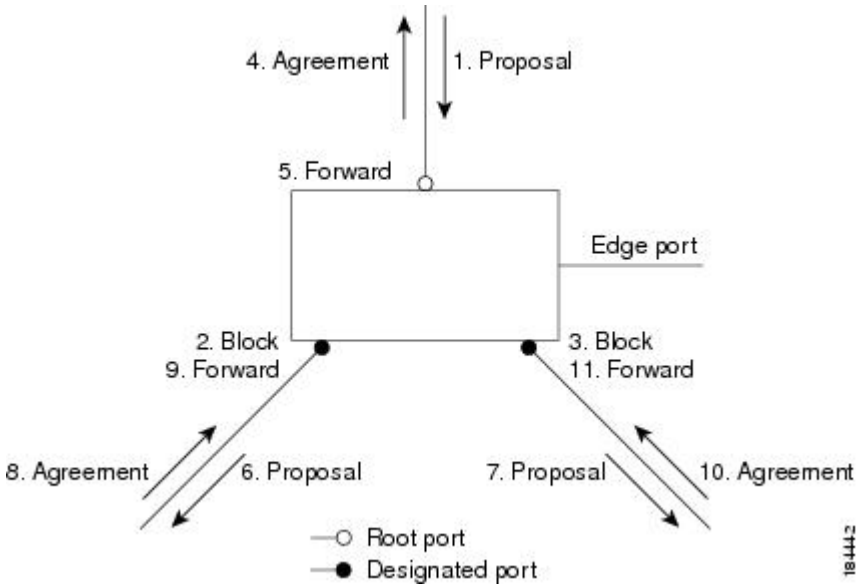
他のすべてのポートが同期化されると、スイッチはルート ポートで受信した優位のルート情報に同期化されます。 次のいずれかが当てはまる場合、スイッチ上の個々のポートで同期がとられます。

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

指定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、合意メッセージが送信されます。 ポイントツーポイント リンクで接続されているスイッチが、そのポートのロールについての合意に存在する場合、Rapid PVST+ により、ポート ステートがただちにフォワーディング ステートに移行します。 この一連のイベントを次の図に示します。

図 *19*： 高速コンバージェンス中のイベントのシーケンス



優位 BPDU 情報の処理

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

上位 BPDU がポートで受信されると、Rapid PVST+ は再設定を起動します。 そのポートが新しいルート ポートとして提案、選択されている場合、Rapid PVST+ は残りすべてのポートを同期させます。

受信した BPDU が提案フラグの設定された Rapid PVST+ BPDU の場合、スイッチは残りすべてのポートを同期させたあと、合意メッセージを送信します。前のポートがブロッキング ステートになるとすぐに、新しいルート ポートがフォワーディング ステートに移行します。

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

下位 BPDU 情報の処理

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

指定ポートは、下位 BPDU を受信すると、独自の情報ですぐに応答します。

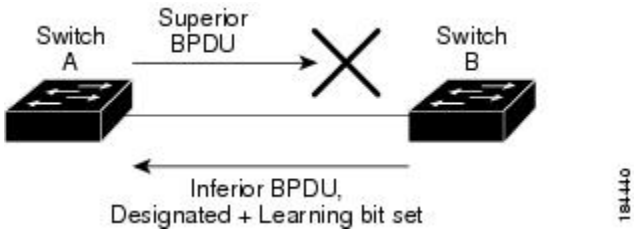
スパニングツリーの異議メカニズム

ソフトウェアは、受信したBPDUでポートのロールおよびステートの一貫性をチェックし、ブリッジング ループの原因となることがある単方向リンク障害を検出します。

指定ポートは、矛盾を検出すると、そのロールを維持しますが、廃棄ステートに戻ります。一貫性がない場合は、接続を中断した方がブリッジング 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の一般的な原因となる単方向リンク障害を示します。スイッチ A はルート ブリッジで、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 *20*： 単一方向リンクの失敗の検出



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 *13*： 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

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
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。

ポートのプライオリティ

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、提案フラグがオンに設定された 802.1w BPDU バージョン 2 の場合、スイッチは残りすべてのポートを同期させたあと、合意メッセージを送信します。 受信した BPDU が 802.1D BPDU バージョン 0 の場合は、スイッチは提案フラグを設定せずに、ポートの転送遅延タイマーを開始します。 新しいルート ポートでは、フォワーディング ステートに移行するために、2 倍の転送遅延時間が必要となります。

スイッチは、次のように、レガシー 802.1D スイッチと相互動作します。

- 通知：802.1D BPDU とは異なり 802.1w は、TCN BPDU を使用しません。 ただし、802.1D スイッチとの相互運用のため、Cisco NX-OS では、TCN BPDU を処理し、生成します。
- 受信応答：802.1w スイッチでは、802.1D スイッチから指定ポート上に TCN メッセージを受信すると、TCA ビットを設定し、802.1D コンフィギュレーション BPDU で応答します。 ただし、802.1D スイッチに接続されているルート ポートで TC While タイマー（802.1D の TC タイマーと同じ）がアクティブの場合、TCA がセットされたコンフィギュレーション BPDU を受信すると、TC While タイマーはリセットされます。

動作のこの方式は、802.1D スイッチでのみ必要です。 802.1w BPDU では、TCA ビットは設定されません。

- プロトコル移行：802.1D スイッチとの下位互換性のために、802.1w は、802.1D コンフィギュレーション BPDU と TCN BPDU をポートごとに選択的に送信します。

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

ポート移行遅延タイマーの期限切れ後にスイッチで 802.1D BPDU を受信した場合は、802.1D スイッチに接続していると見なして、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 マルチ スパニングツリー（MST）規格とシームレスに相互運用されます。 ユーザによる設定は不要です。

Rapid PVST+ の設定

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

Rapid PVST+ は VLAN ごとにイネーブルにします。 STP のインスタンスが VLAN ごとに維持されます（STP をディセーブルにした VLAN を除く）。 デフォルトで Rapid PVST+ は、デフォルト VLAN と、作成した各 VLAN でイネーブルになります。

Rapid PVST+ のイネーブル化

スイッチ上で Rapid PVST+ をイネーブルにすると、指定されている VLAN で Rapid PVST+ をイネーブルにする必要があります。

Rapid PVST+ はデフォルトの STP モードです。 MST と Rapid PVST+ は同時には実行できません。

（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。

手順の概要

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

手順の詳細

	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。

手順の概要

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

手順の詳細

	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。

	コマンドまたはアクション	目的
		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場合は、VLAN でスパニングツリーをディセーブルにしないでください。 VLAN の一部のスイッチおよびブリッジでスパニングツリーをディセーブルにして、その他のスイッチおよびブリッジでイネーブルにしておくことはできません。 スパニングツリーをイネーブルにしたスイッチとブリッジに、ネットワークの物理トポロジに関する不完全な情報が含まれることになるので、この処理によって予想外の結果となることがあります。 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 で現在ルートになっているブリッジのブリッジ プライオリティがスイッチによって確認されます。 スイッチは指定した VLAN のブリッジプライオリティを24576に設定します（このスイッチがそのVLANのルートになる値）。指定した VLAN のいずれかのルート ブリッジに 24576 より小さいブリッジ プライオリティが設定されている場合は、スイッチはその VLAN のブリッジ プライオリティを、最小のブリッジ プライオリティより 4096 だけ小さい値に設定します。

（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。

手順の概要

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

手順の詳細

	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。

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

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

セカンダリ ルート ブリッジの設定

ソフトウェア スイッチをセカンダリ ルートとして設定しているときに、STP ブリッジのプライオリティをデフォルト値（32768）から変更しておくと、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 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。

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。

手順の概要

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

手順の詳細

	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。

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

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

Rapid PVST+ のポート プライオリティの設定

Rapid PVST+ に最初に選択させる 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。

手順の概要

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

手順の詳細

	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 の範囲です。 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。

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

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

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

Rapid PVST+ 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。

手順の概要

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

手順の詳細

	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。

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

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

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

VLAN の Rapid PVST+ のブリッジ プライオリティの設定

VLAN の Rapid PVST+ のブリッジ プライオリティを設定できます。

（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。

手順の概要

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

手順の詳細

	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。

次の例は、VLAN のブリッジ プライオリティを設定する方法を示します。

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

VLAN の Rapid PVST+ の hello タイムの設定

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

（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。

手順の概要

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

手順の詳細

	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 タイムの値には 1 ～ 10 秒を指定できます。 デフォルトは 2 秒です。

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

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

VLAN の Rapid PVST+ の転送遅延時間の設定

Rapid PVST+ の使用時は、VLAN ごとに転送遅延時間を設定できます。

手順の概要

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

手順の詳細

	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。

次の例は、VLAN の転送遅延時間を設定する方法を示しています。

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

VLAN の Rapid PVST+ の最大経過時間の設定

Rapid PVST+ の使用時は、VLAN ごとに最大経過時間を設定できます。

手順の概要

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

手順の詳細

	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。

次の例は、VLAN の最大経過時間を設定する方法を示しています。

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

リンク タイプの設定

Rapid の接続性（802.1w 規格）は、ポイントツーポイントのリンク上でのみ確立されます。 リンク タイプは、デフォルトでは、インターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続であると見なされ、半二重ポートは共有接続であると見なされます。

リモート スイッチの 1 つのポートに、ポイントツーポイントで物理的に接続されている半二重リンクがある場合、リンク タイプのデフォルト設定を上書きし、高速移行をイネーブルにできます。

リンクを共有に設定すると、STP は 802.1D に戻ります。

手順の概要

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

手順の詳細

	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+ を再起動する方法を示しています。

```
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)
veth1/1          Desg FWD 2         128.129  Edge P2p
```

第 12 章

マルチ スパニングツリーの設定

この章の内容は、次のとおりです。

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収束が可能なため、802.1D 転送遅延がなくなり、ルート ブリッジ ポートと指定ポートが迅速にフォワーディング ステートに変わります

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 で定義されている Rapid Spanning Tree Protocol（RSTP）と、IEEE 802.1D に組み込まれた RSTP
- 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 MSTI に参加できるようにするには、同一の MST 設定情報でスイッチの設定に整合性を持たせる必要があります。

同じ MST 設定の相互接続スイッチの集まりが MST 領域です。 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 領域が制御されます。 この設定には、領域の名前、バージョン番号、MST VLAN とインスタンスの割り当てマップが含まれます。

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

各領域は、最大 65 の MST インスタンス（MSTI）までサポートします。 インスタンスは、1 ～ 4094 の範囲の任意の番号によって識別されます。 インスタンス 0 は、特別なインスタンスである IST 用に予約されています。 VLAN は、一度に 1 つの MST インスタンスに対してのみ割り当てることができます。

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

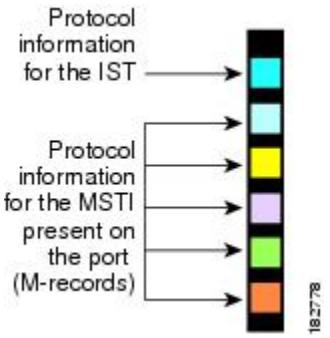
（注） ネットワークを、非常に多数の領域に分けることは推奨しません。

MST BPDU

1 つの領域に含まれる MST BPDU は 1 つだけで、その BPDU により、領域内の各 MSTI について M レコードが保持されます（次の図を参照）。 IST だけが MST 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 *21*： *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 領域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 領域で実行されるスパニングツリーです。

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

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

同じ領域内のすべての 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、領域に対してローカルです。たとえば、領域 A と領域 B が相互接続されている場合でも、領域 A にある MSTI 9 は、領域 B にある MSTI 9 には依存しません。

- CST は、MST 領域と、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 領域、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 領域にある IST の集まりです。 CIST は、MST 領域内部の IST や、MST 領域外部の CST と同じです。

MST 領域で計算されるスパニングツリーは、スイッチ ドメイン全体を含んだ CST 内のサブツリーとして認識されます。 CIST は、802.1w、802.1s、802.1D の各規格をサポートするスイッチで実行されているスパニングツリー アルゴリズムによって形成されています。 MST リージョン内の CIST は、リージョン外の CST と同じです。

MST 領域内でのスパニングツリーの動作

IST は、領域にあるすべての 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。 ネットワークに領域が 1 つしかない場合、CIST リージョナル ルートは CIST ルートにもなります。 CIST ルートが領域外にある場合、領域の境界にある MST スイッチの 1 つが、CIST リージョナル ルートとして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、同じ領域のネイバーから上位の IST 情報を受信すると、元のサブ領域を脱退して、真の CIST リージョナル ルートが含まれる新しいサブ領域に加入します。 このようにして、真の CIST リージョナル ルートが含まれているサブ領域以外のサブ領域はすべて縮小します。

MST 領域内のすべてのスイッチが同じ CIST リージョナル ルートを承認する必要があります。 領域内にある任意の 2 つのスイッチは、共通 CIST リージョナル ルートに収束する場合、MSTI に対するポート ロールのみを同期します。

MST 領域間のスパニングツリー動作

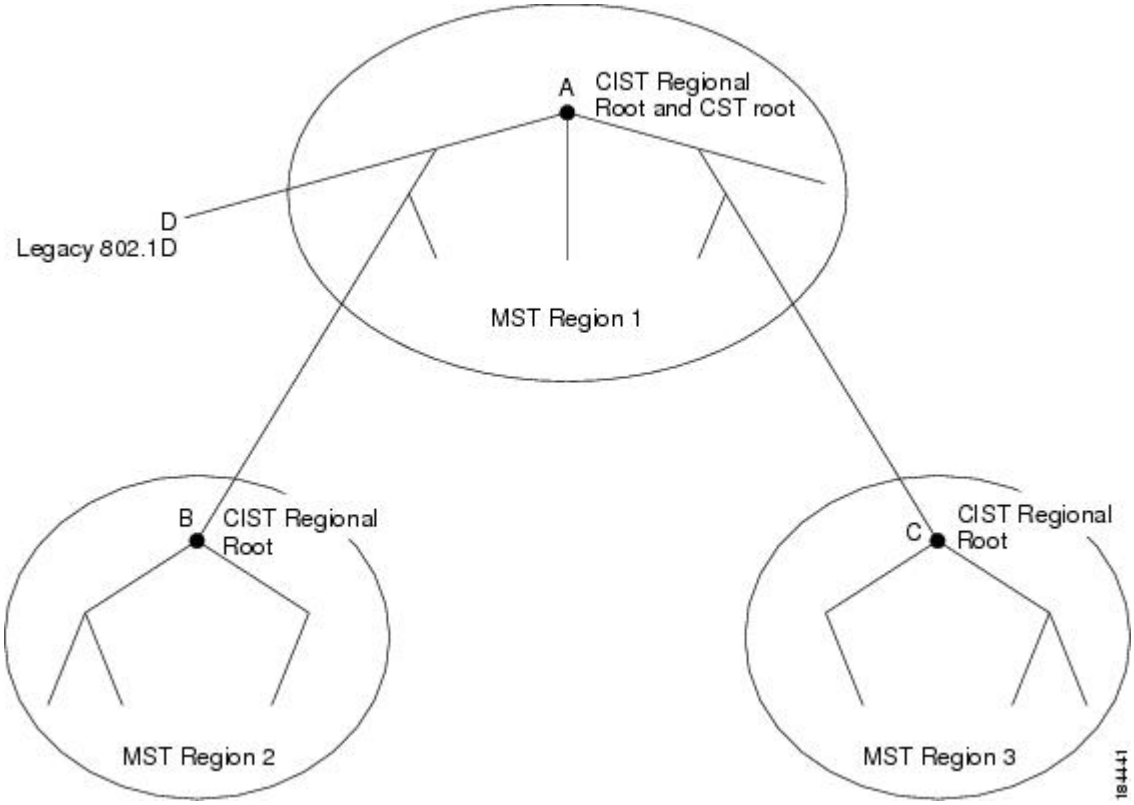
ネットワーク内に複数の領域、または 802.1 w や 802.1D STP インスタンスがある場合、MST はネットワーク内のすべての MST 領域、すべての 802.1w と 802.1D STP スイッチを含む CST を確立して、維持します。 MSTI は、領域の境界で IST と結合して CST になります。

IST は、領域内のすべての MST 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 領域と 802.1D（D）があるネットワークを示します。 リージョン 1 の CIST リージョナル ルート（A）は、CIST ルートでもあります。 リージョン 2 の CIST リージョナル

ルート（B）、およびリージョン 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 *22*：***MST*** 領域、***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、修飾子またはリージョン修飾子は不要です。 MST 用語を次に示します。

- CIST ルートは CIST のルート ブリッジで、ネットワーク全体にまたがる一意のインスタンスです。
- CIST 外部ルート パス コストは、CIST ルートまでのコストです。 このコストは MST 領域内で変化しません。 MST 領域は、CIST に対する唯一のスイッチのように見えます。 CIST 外部ルート パス コストは、これらの仮想スイッチとリージョンに属していないスイッチ間を計算して出したルート パス コストです。
- CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。 または、CIST リージョナル ルートがそのリージョンで CIST ルートに最も近いスイッチになります。 CIST リージョナル ルートは、IST のルート ブリッジとして動作します。
- CIST 内部ルート パス コストは、領域内の CIST リージョナル ルートまでのコストです。 このコストは、IST つまりインスタンス 0 だけに関連します。

ホップ カウント

MST 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と、領域内の最大ホップ数を設定し、IST およびその領域のすべての MSTI に適用できます。

ホップ カウントは、メッセージ エージ情報と同じ結果になります（再設定を開始）。 インスタンスのルート ブリッジは、コストが 0 でホップ カウントが最大値に設定された BPDU（M レコード）を常に送信します。 スイッチがこの BPDU を受信すると、受信 BPDU の残存ホップ カウントから 1 だけ差し引いた値を残存ホップ カウントとする BPDU を生成し、これを伝播します。 このホップ カウントが 0 になると、スイッチはその BPDU を廃棄し、ポート用に維持されていた情報を期限切れにします。

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

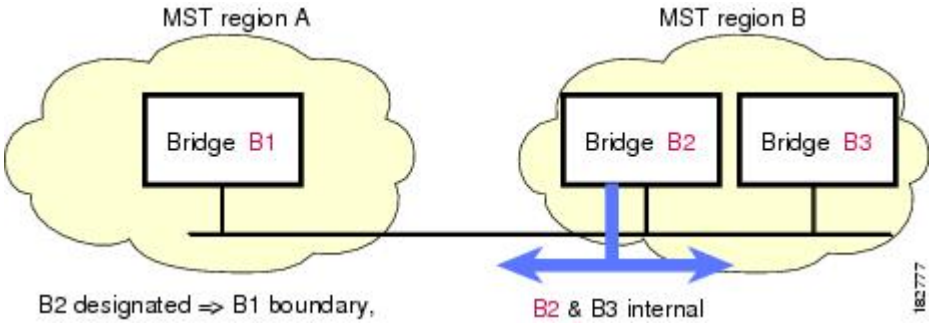
スイッチがスパニングツリー設定メッセージを受信せずに再設定を試行するまで待機する秒数として最大エージング タイムを設定します。

境界ポート

境界ポートは、ある領域を別の領域に接続するポートです。 指定ポートは、STP ブリッジを検出するか、設定が異なる MST ブリッジまたは Rapid PVST+ ブリッジから合意提案を受信すると、境界にあることを認識します。 この定義により、領域の内部にある 2 つのポートが、異なる領域に

属すポートとセグメントを共有できるため、ポートで内部メッセージと外部メッセージの両方を受信できる可能性があります（次の図を参照）。

図 *23*： *MST* 境界ポート



境界では、MST ポートのロールは問題ではなく、そのステートは強制的に IST ポート ステートと同じに設定されます。 境界フラグがポートに対してオンに設定されている場合、MST ポートのロールの選択処理では、ポートのロールが境界に割り当てられ、同じステートが IST ポートのステートとして割り当てられます。 境界にある IST ポートでは、バックアップ ポートのロール以外のすべてのポートのロールを引き継ぐことができます。

スパニングツリーの異議メカニズム

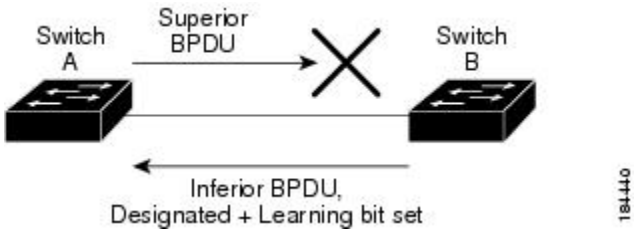
現在、この機能は、IEEE MST 規格にはありませんが、規格準拠の実装に含まれています。 ソフトウェアは、受信した BPDU でポートのロールおよびステートの一貫性をチェックし、ブリッジング ループの原因となることがある単方向リンク障害を検出します。

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 *24*：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、異なる領域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、ポートが領域の境界にあることを検出できます。

ただし、スイッチは、802.1D BPDU を受信しなくなった場合でも、自動的には 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、保留中の領域設定が作成されます。
  - 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。
  - 変更をコミットすることなく MST コンフィギュレーション モードを終了するには、**abort** コマンドを入力します。
  - 行った変更内容をすべてコミットして MST コンフィギュレーション モードを終了するには、**exit** コマンドを入力します。

MST のイネーブル化

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。また、vPC ピア スイッチで 2 つのスパニングツリー モードが異なる場合には不整合となるため、この操作は中断されます。

手順の概要

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

手順の詳細

	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 領域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** コマンドと **abort** コマンドとの違いに注意してください。

手順の概要

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

手順の詳細

	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**	システム上で、MST コンフィギュレーション モードを開始します。次の MST コンフィギュレーション パラメータを割り当てるには、MST コンフィギュレーション モードを開始しておく必要があります。 • 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

	コマンドまたはアクション	目的
		• 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**	• 最初のフォームでは、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 番目のフォームでは、変更をコミットすることなく MST コンフィギュレーション モードを終了します。
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。 • 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

領域名は、ブリッジ上に設定します。 同じ MST 領域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。

手順の概要

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

手順の詳細

	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。

	コマンドまたはアクション	目的
ステップ 3	switch(config-mst)# **name** *name*	MST 領域の名前を指定します。 *name* ストリングには最大 32 文字まで使用でき、大文字と小文字が区別されます。 デフォルトは空の文字列です。

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 領域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。

手順の概要

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

手順の詳細

	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 領域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 領域内に存在させるには、同じ VLAN からインスタンスへのマッピング、同じ構成リビジョン番号、および同じ MST の名前が設定されている必要があります。

領域には、同じ MST 設定の 1 つのメンバまたは複数のメンバを存在させることができます。各メンバでは、IEEE 802.1w RSTP BPDU を処理できる必要があります。 ネットワーク内の MST 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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **spanning-tree mst configuration**
3. switch(config-mst)# **instance** *instance-id* **vlan** *vlan-range*
4. switch(config-mst)# **name** *name*
5. switch(config-mst)# **revision** *version*

手順の詳細

	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。 VLAN を MSTI にマップする場合、マッピングは増加され、コマンドに指定した VLAN は、以前マッピングした VLAN に追加されるか、そこから削除されます。 VLAN 範囲を指定する場合は、ハイフンを使用します。たとえば、**instance 1 vlan 1-63** とコマンドを入力すると、MST インスタンス 1 に VLAN 1 ～ 63 がマッピングされます。 複数の VLAN を指定する場合はカンマで区切ります。たとえば、**instance 1 vlan 10, 20, 30** と指定すると、MST インスタンス 1 に VLAN 10、20、および 30 がマッピングされます。

	コマンドまたはアクション	目的
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 文字まで使用でき、大文字と小文字が区別されます。
ステップ 5	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 領域設定に戻すには、**no spanning-tree mst configuration** コンフィギュレーション コマンドを入力します。
- VLAN インスタンス マッピングをデフォルトの設定に戻すには、**no instance** *instance-id* **vlan** *vlan-range* MST コンフィギュレーション コマンドを使用します。
- デフォルトの名前に戻すには、**no name** MST コンフィギュレーション コマンドを入力します。
- デフォルトのリビジョン番号に戻すには、**no revision** MST コンフィギュレーション コマンドを入力します。
- Rapid PVST+ を再度イネーブルにするには、**no spanning-tree mode** または **spanning-tree mode rapid-pvst** のグローバル コンフィギュレーション コマンドを入力します。

次の例は、MST コンフィギュレーション モードを開始し、VLAN 10 ～ 20 を MSTI 1 にマッピングし、領域に region1 という名前を付けて、設定リビジョンを 1 に設定し、保留中の設定を表示し、変更を適用してグローバル コンフィギュレーション モードに戻る方法を示しています。

```
switch(config)# spanning-tree mst configuration
switch(config-mst)# instance 1 vlan 10-20
switch(config-mst)# name region1
switch(config-mst)# revision 1
switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instances configured 2
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------
```

VLAN から MST インスタンスへのマッピングとマッピング解除

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 領域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。

手順の概要

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

手順の詳細

	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 領域での IST 用に予約されています。 • *vlan-range* の範囲は 1 ～ 4094 です。 VLAN を MSTI にマッピングすると、マッピングは差分で実行され、コマンドで指定された VLAN が、以前マッピングされた VLAN に追加または VLAN から削除されます。
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 のセカンダリ VLAN をプライマリ VLAN と同じ 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。

手順の概要

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

手順の詳細

	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 のすべてのセカンダリ VLAN を、それぞれ関連するプライマリ VLAN と同じ MSTI に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。

手順の概要

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

手順の詳細

	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。 デフォルト値は 7 です。 このキーワードは、MSTI インスタンス 0 の場合にのみ使用できます。 • hello-time *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。
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。

手順の概要

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

手順の詳細

	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。 デフォルト値は 7 です。 このキーワードは、MSTI インスタンス 0 の場合にのみ使用できます。 • hello-time *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。
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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** {{*type slot*/*port*} | {**port-channel** *number*}}
3. switch(config-if)# **spanning-tree mst** *instance-id* **port-priority** *priority*

手順の詳細

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

（注） MST では、ロング パス コスト計算方式が使用されます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** {{*type slot*/*port*} | {**port-channel** *number*}}
3. switch(config-if)# **spanning-tree mst** *instance-id* **cost** [*cost* | **auto**]

手順の詳細

	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。 ループが発生した場合、MST はパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。 パス コストが小さいほど、送信速度が速いことを示します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 有効な範囲は 1 ～ 4094 です。 • *cost* の範囲は 1 ～ 200000000 です。 デフォルト値は auto で、インターフェイスのメディア速度から取得されるものです。

	コマンドまたはアクション	目的

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。

手順の概要

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

手順の詳細

	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。 使用可能な値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。 システムでは、他のすべての値が拒否されます。

	コマンドまたはアクション	目的

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。

手順の概要

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

手順の詳細

	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時間です。 これらのメッセージは、スイッチがアクティブであることを意味します。 *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。

手順の概要

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

手順の詳細

	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）。

手順の概要

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

手順の詳細

	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。 領域内の最大ホップを設定し、それを、その領域にある IST とすべての MST インスタンスに適用できます。 ホップ カウントは、メッセージ エージ情報と同じ結果になります（再設定を開始）。

手順の概要

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

手順の詳細

	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、領域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。

手順の概要

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

手順の詳細

	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。

手順の概要

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

手順の詳細

	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。

手順の概要

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

手順の詳細

	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 または異なる領域にアソシエートされている MST BPDU を受信するときに、ポートが領域の境界にあることを検出できます。 ただし、STP プロトコルの移行では、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。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 13 章

STP 拡張機能の設定

この章の内容は、次のとおりです。

STP 拡張機能について

シスコでは、STP に、収束をより効率的に行うための拡張機能を追加しました。 場合によっては、同様の機能が IEEE 802.1w 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間にポートを「ネットワーク」として設定すると、そのポートで Bridge Assurance がイネーブルになります。

（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 *14*：*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/ディセーブル	ディセーブル
ディセーブル	イネーブル/ディセーブル	イネーブル/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/ディセーブル	イネーブル/ディセーブル	イネーブル 注意 BPDU は送信されませんが、受信した場合には、通常の STP の動作が開始されません。BPDU の使用に当たっては、十分注意してください。

ループ ガードの概要

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

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

STP ループは、冗長なトポロジにおいてブロッキング ポートが誤ってフォワーディング ステートに移行すると発生します。 こうした移行は通常、物理的に冗長なトポロジ内のポートの 1 つ（ブロッキング ポートとは限らない）が BPDU の受信を停止すると起こります。

ループ ガードは、デバイスがポイントツーポイント リンクによって接続されているスイッチド ネットワークだけで役立ちます。 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。こうした復旧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 収束が実行され、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復旧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。

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。

手順の概要

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

手順の詳細

	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

	コマンドまたはアクション	目的
		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。

インターフェイスがホストに接続されていること。

手順の概要

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

手順の詳細

	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。

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。

手順の概要

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

手順の詳細

	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。

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。

手順の概要

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

手順の詳細

	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。

手順の概要

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

手順の詳細

	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 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） インターフェイス上で 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。

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 このコマンドを使用するときには注意してください。誤って使用すると、ブリッジング ループが発生するおそれがあります。

（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。

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。

手順の概要

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

手順の詳細

	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。

手順の概要

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

手順の詳細

	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） インターフェイス上で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。

スパニングツリー標準ポートが存在し、少なくとも一部のネットワーク ポートが設定済みであること。

手順の概要

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

手順の詳細

	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。

ループ ガードが、スパニングツリーの標準またはネットワーク ポート上で設定されていること。

手順の概要

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

手順の詳細

	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 14 章

Flex Link の設定

この章の内容は、次のとおりです。

Flex Link について

Flex Link は、レイヤ 2 インターフェイス（スイッチ ポートまたはポート チャネル）のペアで、1 つのインターフェイスがもう一方のバックアップとして機能するように設定されています。 この機能は、Spanning Tree Protocol（STP; スパニングツリープロトコル）の代替ソリューションです。 STP をディセーブルにしても、基本的リンク冗長性を保つことができます。 Flex Link は、通常、お客様がスイッチで STP を実行しない場合のサービス プロバイダーまたは企業ネットワークに設定されます。 スイッチが STP を実行中の場合は、STP がすでにリンク レベルの冗長性またはバックアップを提供しているため、Flex Link は不要です。

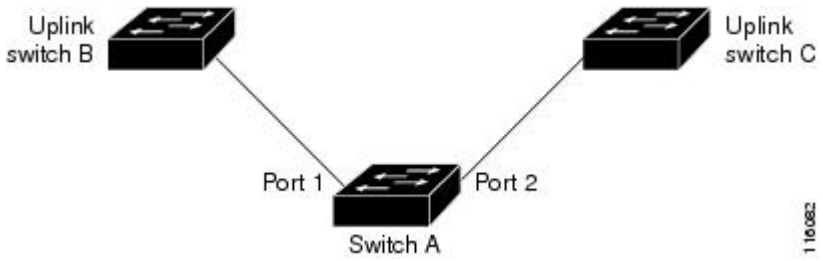
別のレイヤ 2 インターフェイスを Flex Link またはバックアップ リンクとして割り当てることで、1 つのレイヤ 2 インターフェイス（アクティブ リンク）に Flex Link を設定します。 Flex Link インターフェイスは、同じスイッチ上に設定できます。 リンクの 1 つがアップでトラフィックを転送しているときは、もう一方のリンクがスタンバイ モードで、このリンクがシャットダウンした場合にトラフィックの転送を開始できるように準備しています。 どの時点でも、1 つのインターフェイスのみがリンクアップ ステートでトラフィックを転送しています。 プライマリ リンクがシャットダウン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

フォルトでは、Flex Link は設定されておらず、バックアップ インターフェイスは定義されていません。 STP は Flex Link インターフェイスでディセーブルです。

Flex Link の設定例では、スイッチ A のポート 1 および 2 がアップリンク スイッチ B および C に接続されています。 これらのスイッチは Flex Link として設定されているので、どちらかのインターフェイスがトラフィックを転送し、もう一方のインターフェイスはスタンバイ モードになります。 ポート 1 がアクティブ リンクである場合、ポート 1 とスイッチ B との間でトラフィックの転送が開始され、ポート 2（バックアップ リンク）とスイッチ C との間のリンクでは、トラフィックは転送されません。 ポート 1 がダウンした場合はポート 2 がアップし、トラフィックをスイッチ C に転送し始めます。 ポート 1 は、再び動作を開始するとスタンバイ モードになり、トラフィックを転送しません。ポート 2 がトラフィック転送を続けます。

Flex Link はレイヤ 2 ポートおよびポート チャネルだけでサポートされ、VLAN やレイヤ 3 ポートではサポートされません。

図 *25*：*Flex Link* の設定例



プリエンプション

必要に応じて、プリエンプション メカニズムを設定し、優先してトラフィックの転送に使用するポートを指定できます。 たとえば、Flexlink ペアをプリエンプション モードで設定することにより、ピア ポートより帯域幅の大きいポートが動作を再開した後、ポートが 60 秒後に転送を開始し、ピア ポートがスタンバイとなります。 これを行うには、preemption mode bandwidth および delay コマンドを入力します。

プライマリ（転送）リンクがダウンすると、トラップによってネットワーク管理ステーションが通知を受けます。 スタンバイ リンクがダウンすると、トラップによってユーザが通知を受けます。

プリエンプションは、次の 3 つのモードで設定できます。

- forced：アクティブ インターフェイスが常にバックアップ インターフェイスより先に使用されます。
- bandwidth：より大きい帯域幅のインターフェイスが常にアクティブインターフェイスとして動作します。
- off：プリエンプションはありません。アップしている最初のインターフェイスが転送モードになります。

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

マルチキャスト

Flexlink インターフェイスが mrouter ポートとして学習されると、スタンバイ（非転送）インターフェイスがリンクアップしている場合には、そのインターフェイスも mrouter ポートとして学習されます。 この相互学習は、内部ソフトウェアのステートメンテナンス専用であり、マルチキャスト高速コンバージェンスがイネーブルでない限り、IGMP 動作とハードウェア転送に対して関連性はありません。 マルチキャスト高速コンバージェンスを設定すると、相互学習された mrouter ポートがただちにハードウェアに追加されます。 Flex Link では、IPv4 IGMP のマルチキャスト高速コンバージェンスをサポートしています。

注意事項

Flex Link の設定時には、次の注意事項に従ってください。

- 任意のアクティブ リンクに対して設定可能な Flex Link バックアップ リンクは 1 つだけで、アクティブ インターフェイスとは異なるインターフェイスでなければなりません。
- インターフェイスが所属できる Flex Link ペアは 1 つだけです。つまり、インターフェイスは 1 つのアクティブ リンクに対してだけ、バックアップ リンクになることができます。
- どちらのリンクも、EtherChannel に属するポートには設定できません。 ただし、2 つのポート チャネル（EtherChannel 論理インターフェイス）を Flex Link として設定でき、ポート チャネルおよび物理インターフェイスを Flex Link として設定して、ポート チャネルか物理インターフェイスのどちらかをアクティブ リンクにすることができます。
- STP は Flex Link ポートでディセーブルです。 ポート上にある VLAN が STP 用に設定されている場合でも、Flex Link ポートは STP に参加しません。 STP がイネーブルでない場合は、設定されているトポロジでループが発生しないようにしてください。
- Flex Link ポート、またはそのリンクの接続先ポートでは、STP 機能（PortFast、BPDU ガードなど）を設定しないでください。
- vPC はサポートされていません。 Flex Link は、設定の簡素化が求められ、アクティブ-アクティブ冗長の必要性がない vPC の代わりに使用されます。
- 次のタイプのインターフェイスで Flex Link を設定することはできません。
  - FEX ファブリック ポートと FEX ホスト ポート
  - FCoE（vFC インターフェイス）
  - VNTAG（vETH インターフェイス）
  - ポート セキュリティがイネーブルになっているインターフェイス

- レイヤ 3 インターフェイス
- SPAN 宛先
- ポート チャネル メンバ
- プライベート VLAN を使用して設定されているインターフェイス
- エンドノード モード
- FabricPath コア インターフェイス（レイヤ 2 マルチパス）

デフォルト設定

Flex Link には、次のパラメータのデフォルト設定があります。

パラメータ	定義
Flex Link	ディセーブル
プリエンプション モード	Off
プリエンプション遅延	35 秒

Flex Link の設定

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

手順の概要

1. **configure terminal**
2. **interface** *slot/port*
3. **switchport backup interface** {**ethernet** *slot/port* | **port-channel** *channel-no* } [**multicast fast-convergence** | **preemption** { **delay** *delay-time* | **mode** [**bandwidth** | **forced** | **off**] }]
4. （任意） **end**
5. （任意） **show interface** *interface-id* **switchport backup**
6. （任意） **copy running-config startup config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**interface** *slot/port*	イーサネット インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。 指定できるポート チャネルは 1 ～ 48 です。
ステップ 3	**switchport backup interface** {**ethernet** *slot/port* | **port-channel** *channel-no* } [**multicast fast-convergence** | **preemption** { **delay** *delay-time* | **mode** [**bandwidth** | **forced** | **off**] }]	物理レイヤ 2 インターフェイス（イーサネットまたはポート チャネル）を、Flex Link ペアの一部として設定します。 1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。 ethernet *slot/port*：バックアップ イーサネット インターフェイスを指定します。 スロット番号は 1 ～ 255、ポート番号は 1 ～ 128 です。 port-channel *channel-no*：ポート チャネル インターフェイスを指定します。 インターフェイス番号は 1 ～ 4096 です。 multicast：（任意）マルチキャスト パラメータを設定するように指定します。 fast-convergence：（任意）バックアップ インターフェイス上で高速コンバージェンスを設定します。 preemption：（任意）バックアップ インターフェイスのペアにプリエンプション方式を設定するように指定します。 delay *delay-time*：（任意）プリエンプション遅延を指定します。 指定できる範囲は 1 ～ 300 秒です。 デフォルト値は 35 秒です。 mode：（任意）プリエンプション モードを指定します。 bandwidth：（任意）より多くの帯域幅を使用できるインターフェイスが常にバックアップに優先することを指定します。 forced：（任意）常にバックアップをプリエンプトするインターフェイスを指定します。 off：（任意）バックアップからアクティブへの切り替えが発生しないことを指定します。
ステップ 4	**end**	（任意） 特権 EXEC モードに戻ります。
ステップ 5	**show interface** *interface-id* **switchport backup**	（任意） 設定を確認します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup config**	（任意） スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

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

```
switch(config)# feature flexlink
Switch(config)# interface ethernet1/1
Switch(config-if)# switchport backup interface ethernet2/1

switch(config)# interface po300
Switch(config-if)# switchport backup interface po301
switch# show ip igmp snooping mrouter
Type: S - Static, D - Dynamic, V - vPC Peer Link, I - Internal, C - Co-learned
Vlan  Router-port   Type      Uptime      Expires
4     Po300         D         00:00:12    00:04:50
4     Po301         DC        00:00:12    00:04:50
```

Flex Link プリエンプションの設定

Flex Link のペアにプリエンプション方式を設定できます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**interface** *slot/port*	イーサネットインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスは物理レイ

	コマンドまたはアクション	目的
		ヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。 指定できるポート チャネルは 1 ～ 48 です。
ステップ 3	**switchport backup interface ethernet** *slot/port*	物理レイヤ2インターフェイス（ポートチャネル）をインターフェイスがある Flex Link ペアの一部として設定します。 1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 4	**switchport backup interface ethernet** *slot/port* **preemption mode** [**bandwidth** | **forced** | **off**]	物理レイヤ 2 インターフェイス（イーサネットまたはポート チャネル）を、Flex Link ペアの一部として設定します。 1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。 Flex Link インターフェイス ペアのプリエンプション メカニズムとプリエンプション遅延を設定します。 次のプリエンプト モードを設定することができます。 • bandwidth：より大きい帯域幅のインターフェイスが常にアクティブ インターフェイスとして動作します。 • forced：アクティブ インターフェイスが常にバックアップ インターフェイスより先に使用されます。 • off：アクティブからバックアップへのプリエンプションは発生しません。
ステップ 5	**switchport backup interface ethernet** *slot/port* **preemption delay** *delay-time*	ポートが他のポートより先に使用されるまでの遅延時間を設定します。 デフォルトのプリエンプション遅延は 35 秒です。 （注） 遅延時間の設定は、forced モードおよび bandwidth モードでのみ有効です。
ステップ 6	**end**	（任意） 特権 EXEC モードに戻ります。
ステップ 7	**show interface** *interface-id* **switchport backup**	（任意） 設定を確認します。
ステップ 8	**copy running-config startup config**	（任意） スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

次に、バックアップ インターフェイスのペアに対してプリエンプト モードを bandwidth に設定し、設定を確認する例を示します。

```
Switch# configure terminal
Switch(conf)# interface ethernet0/1
```

```
Switch(conf-if)#switchport backup interface ethernet0/2 preemption mode forced
Switch(conf-if)#switchport backup interface ethernet0/2 preemption delay 50
Switch(conf-if)# end

Switch# show interface switchport backup detail
Active Interface Backup Interface State
------------------------------------------------------------------------------
Ethernet0/21 Ethernet0/2 Active Up/Backup Standby
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : 100000 Kbit (Gi0/1), 100000 Kbit (Gi0/2)
Mac Address Move Update Vlan : auto
```

Flex Link 設定の確認

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

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

設定例

次の例は、強制プリエンプションを使用してポート チャネル スイッチポート バックアップのペアを設定する方法を示しています。 アクティブな interface port-channel10 が優先転送インターフェイスです。

```
switch(config)# interface port-channel10
switch(config-if)# switchport backup interface port-channel20 preemption mode forced
switch(config-if)# switchport backup interface port-channel20 preemption delay 35
```

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

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

次の例は、Flex Linkインターフェイス（po300とpo301）のマルチキャスト高速コンバージェンスの例を示します。 po300 で一般クエリーを受信すると、mrouter ポートと po301 が相互学習されます。

```
switch(config)# interface po300
Switch(config-if)# switchport backup interface po301
switch# show ip igmp snooping mrouter
Type: S - Static, D - Dynamic, V - vPC Peer Link, I - Internal, C - Co-learned
Vlan  Router-port   Type      Uptime      Expires
4     Po300         D         00:00:12    00:04:50
4     Po301         DC        00:00:12    00:04:50
```

次の例は、po300 と po301 を mrouter ポート（po301 が相互学習される）として示します。これは、マルチキャスト高速コンバージェンスがディセーブルの場合、ハードウェア テーブルに追加されません。

```
switch# show ip igmp snooping groups vlan 4
Type: S - Static, D - Dynamic, R - Router port

Vlan  Group Address      Ver  Type  Port list
4     */*                -    R     Po300 Po301
   224.1.1.1          v2   D     Eth1/31

switch# show platform fwm info hw-stm | grep 0100.5e01.0101
1.4    0100.5e01.0101   midx 36  1:2849:0 0:0:1:0 1.0.0.0.0.24 (e:0)

switch# show platform fwm info oifl 36
oifl 36 vdc 1 oifl 36: vdc 1 gpinif 0, mcast idx 36(alt:0), oifl_type 2
oifl 36 vdc 1 oifl 36: oifl iods 8,44
oifl 36 vdc 1 oifl 36: max_iod 8192,  ref count 1000  num_oifs 2, seq_num 33
oifl 36 vdc 1 oifl 36: hw pgmd: 1 msg present: 0
oifl 36 vdc 1 oifl 36: l2_bum_ref_cnt 0,  l3_macg_ref_cnt 1000
oifl 36 vdc 1 oifl 36: if_indexs - Po300 Eth1/31
```

次の例は、マルチキャスト高速コンバージェンスがイネーブルの場合に、相互学習された po301 がハードウェアに追加されることを示しています。

```
switch(config)# interface po300
Switch(config-if)# switchport backup interface po301 multicast fast-convergence

switch# show platform fwm info hw-stm | grep 0100.5e01.0101
1.4    0100.5e01.0101   midx 38   1:2849:0 0:0:1:0 1.0.0.0.0.26 (e:0)

switch# show platform fwm info oifl 38
oifl 38 vdc 1 oifl 38: vdc 1 gpinif 0, mcast idx 38(alt:0), oifl_type 2
oifl 38 vdc 1 oifl 38: oifl iods 8-9,44
oifl 38 vdc 1 oifl 38: max_iod 8192,  ref count 1000  num_oifs 3, seq_num 35
oifl 38 vdc 1 oifl 38: hw pgmd: 1 msg present: 0
oifl 38 vdc 1 oifl 38: l2_bum_ref_cnt 0,  l3_macg_ref_cnt 1000
oifl 38 vdc 1 oifl 38: if_indexs - Po300 Po301 Eth1/31
```

次の例は、Flex Link の実行コンフィギュレーションを示しています。

```
switch# show running-config flexlink

!Command: show running-config flexlink
!Time: Thu Jan  1 03:21:12 2011

version 5.0(3)N2(1)
feature flexlink

logging level Flexlink 5

interface port-channel500
  switchport backup interface port-channel501 preemption delay 36
  switchport backup interface port-channel501 multicast fast-convergence

interface Ethernet2/2
  switchport backup interface port-channel507 preemption mode forced
```

次の例は、Flex Link インターフェイスの詳細を示します。 (scheduled) が表示されるため、強制プリエンプションが実行されようとしています。

```
switch# show interface switchport backup detail

Switch Backup Interface Pairs:

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

port-channel300         port-channel301         Active Down/Backup Up
        Preemption Mode  : forced
        Preemption Delay : 35 seconds (default) (scheduled)
        Multicast Fast Convergence  : Off
        Bandwidth : 20000000 Kbit (port-channel300), 10000000 Kbit (port-channel301)
```

第 15 章

LLDP の設定

この章の内容は、次のとおりです。

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、ポート記述、システム機能、システム記述、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、次の必要な管理 LLDP TLV をサポートします。

- Data Center Ethernet Parameter Exchange（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 を拡張したプロトコルです。 これは、ピア間のノード 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 パケットに応答するように設計されています。

DCBXP はデフォルトでイネーブルであり、提供された LLDP はイネーブルです。 LLDP がイネーブルである場合、[**no**] **lldp tlv-select dcbxp** コマンドを使用して DCBXP をイネーブルまたはディセーブルにすることができます。 LLDP の送信または受信がディセーブルになっているポートでは、DCBXP はディセーブルです。

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

スイッチで LLDP 機能がイネーブルになっていることを確認してください。

手順の概要

1. switch# **configure terminal**
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**}}
3. switch(config)# **no lldp** {**holdtime** | **reinit** | **timer**}
4. （任意）switch#**show lldp**

手順の詳細

	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を設定します（10 ～ 255 秒）。 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を設定します（1 ～ 10 秒）。 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を設定します（5 ～ 254 秒）。 デフォルト値は 30 秒です。 **tlv-select** オプションを使用して、Type Length Value（TLV）を指定します。 デフォルトでは、すべての TLV の送受信がイネーブルです。 **dcbxp** オプションを使用して、Data Center Ethernet Parameter Exchange（DCBXP）TLV メッセージを指定します。 **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。

	コマンドまたはアクション	目的
		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。 **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 をイネーブルにして管理アドレス TLV を送受信する例を示します。

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

インターフェイス LLDP 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。

手順の概要

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

手順の詳細

	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。
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
```

第 16 章

MAC アドレス テーブルの設定

この章の内容は、次のとおりです。

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 MAC アドレスを受信側の LAN ポートにアソシエートします。

スイッチは、受信したフレームの送信元 MAC アドレスを使用して、アドレス テーブルを動的に構築します。 そのアドレス テーブルにリストされていない受信側 MAC アドレスのフレームを受信すると、そのフレームを、同一 VLAN のフレームを受信したポート以外のすべての LAN ポートへフラッディングします。 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、複数のユニキャスト 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 MAC アドレスは手動で設定できます。 手動で設定したアドレスは、スタティック MAC アドレスとなります。

（注） スタティック MAC アドレスは、インターフェイス コンフィギュレーション モードでも VLAN コンフィギュレーション モードでも設定できます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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-)# **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。

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
```

mac-address-table static コマンドでは、スタティック MAC アドレスを仮想インターフェイスに割り当てることができます。

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。

（注） MAC 経過時間は、インターフェイス コンフィギュレーション モードでも VLAN コンフィギュレーション モードでも設定できます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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)# **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。 指定できる範囲は 0 ～ 1000000 秒です。デフォルトは 300 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 600 秒（10 分）に設定する例を示します。

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

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

MAC アドレス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 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 17 章

IGMP スヌーピングの設定

この章の内容は、次のとおりです。

IGMP スヌーピングの情報

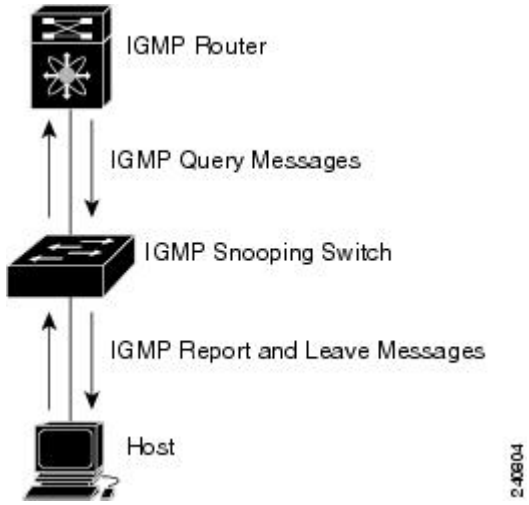
IGMP スヌーピング ソフトウェアは、VLAN 内の IGMP プロトコル メッセージを調べて、このトラフィックの受信に関連のあるホストまたはその他のデバイスに接続されているのはどのインターフェイスかを検出します。 IGMP スヌーピングは、インターフェイス情報を使用して、マルチアクセス LAN 環境での帯域幅消費を減らすことができ、これによって VLAN 全体のフラッディングを防ぎます。 IGMP スヌーピング機能は、どのポートがマルチキャスト対応ルータに接続されているかを追跡して、IGMP メンバーシップ レポートの転送管理を支援します。 トポロジの変更通知には、IGMP スヌーピング 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 *26*： *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、Optimized Multicast Flooding（OMF; 最適化されたマルチキャスト フラッディング）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 5000 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、次の表に示すオプションの IGMP スヌーピング パラメータを設定します。

表 *15*：*IGMP* スヌーピング パラメータ

パラメータ	説明
IGMP スヌーピング	VLAN ごとに IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。 （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。デフォルトではイネーブルになっています。

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。 デフォルトではディセーブルになっています。
最終メンバーのクエリー 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、最終メンバー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。 デフォルトではディセーブルになっています。
レポート抑制	マルチキャスト対応ルータに送信されるメンバーシップ レポート トラフィックを制限します。 レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。 デフォルトではイネーブルになっています。
マルチキャスト ルータ	マルチキャスト ルータへのスタティック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。 Virtual Port Channel（vPC）ピア リンクへのスタティックな接続を設定します。

パラメータ	説明
マルチキャスト ルータの vPC ピア リンク	Virtual Port Channel（vPC）ピア リンクへのスタティックな接続を設定します。 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 パケットが各レシーバ VLAN のピア リンクに送信されます。 vPC ピア リンク上のマルチキャスト トラフィックを孤立ポートがある各レシーバ VLAN に送信するには、**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と、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 およびレシーバ VLAN のピア リンクに送信されません。 また、IGMP スヌーピング mrouter vPC ピア リンクをピア VPC スイッチでグローバルにディセーブルにします。 （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 スイッチに接続されているデュアルホーム接続 FEX があるトポロジで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。

手順の概要

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

手順の詳細

	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。 デフォルトではイネーブルになっています。 （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。
ステップ 3	switch(config)# **vlan** *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。 デフォルトではイネーブルになっています。 （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。

	コマンドまたはアクション	目的
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、最終メンバーのクエリー 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。 デフォルトではディセーブルになっています。
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。 デフォルトではイネーブルになっています。
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**	Virtual Port Channel（vPC）ピア リンクへのスタティックな接続を設定します。 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 パケットが各レシーバ VLAN のピア リンクに送信されます。 vPC ピア リンク上のマルチキャスト トラフィックを孤立ポートがある各レシーバVLANに送信するには、**no ip igmp snooping mrouter vpc-peer-link** コマンドを使用します。 また、IGMP スヌーピング mrouter vPC ピア リンクをピア VPC スイッチでグローバルにディセーブルにします。
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 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 mrouter vpc-peer-link
switch(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface ethernet 1/10
switch(config-vlan)# end
```

次に、vPC ピア リンクへのスタティックな接続を設定する例と vPC ピア リンクへのスタティックな接続を削除する例を示します。

```
switch(config)# ip igmp snooping mrouter vpc-peer-link
switch(config)# no ip igmp snooping mrouter vpc-peer-link
Warning: IGMP Snooping mrouter vpc-peer-link should be globally disabled on peer VPC switch
 as well.
switch(config)#
```

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。
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 18 章

MVR の設定

この章の内容は、次のとおりです。

MVR について

MVR の概要

一般的なレイヤ 2 マルチ VLAN ネットワークでは、マルチキャスト グループへの加入者を複数の VLAN に設定できます。 それらの VLAN 間でデータ分離を維持するには、送信元 VLAN 上のマルチキャスト ストリームをルータに渡す必要があります。そこで、そのストリームがすべての加入者 VLAN で複製され、アップストリーム帯域幅が消費されます。

マルチキャスト VLAN レジストレーション（MVR）を使用すると、レイヤ 2 スイッチでマルチキャスト データを共通の割り当て済み VLAN の送信元から加入者 VLAN に転送し、ルータのバイパスによってアップストリーム帯域幅を節約できます。 スイッチは、MVR IP マルチキャスト ストリームのマルチキャストデータを、IGMP レポートまたはMVR のスタティック コンフィギュレーションのいずれかを使用して、ホストが加入した MVR ポートに対してだけ転送します。 スイッチは、MVR ホストから受信した IGMP レポートを送信元ポートに対してだけ転送します。他のトラフィックでは、VLAN 分離が保持されます。

MVR では、マルチキャスト ストリームを送信元から伝送するために、少なくとも 1 つの VLAN を共通 VLAN として指定する必要があります。 そのような複数のマルチキャスト VLAN（MVR

VLAN）をシステムで設定でき、さらにグローバルなデフォルトMVR VLANとインターフェイス固有のデフォルトMVR VLANを設定できます。 MVRを使用した各マルチキャストグループは、MVR VLANに割り当てられます。

MVRを使用すると、ポート上の加入者は、IGMP JoinおよびLeaveメッセージを送信することで、MVR VLAN上のマルチキャストストリームへの加入および脱退を行うことができます。 MVRグループからのIGMP Leaveメッセージは、Leaveメッセージを受信するVLANのIGMP設定に従って処理されます。 IGMP高速脱退がVLANでイネーブルになっている場合、ポートがただちに削除されます。それ以外の場合は、他のホストがポートに存在するかどうかを判断するために、IGMPクエリーがグループに送信されます。

MVR の他の機能との相互運用性

MVR と IGMP スヌーピング

MVRはIGMPスヌーピングの基本メカニズムで動作しますが、この2つの機能はそれぞれ単独で動作します。 それぞれ、もう一方の機能の動作に影響を与えずにイネーブルまたはディセーブルに設定できます。 IGMPスヌーピングがグローバルに、あるいはVLANでディセーブルになっている場合、およびMVRがVLANでイネーブルになっている場合、IGMPスヌーピングはVLANで内部的にイネーブルです。 非MVRレシーバポート上でMVRグループ用に受信したJoinまたはMVRレシーバポート上で非MVRグループ用に受信したJoinは、IGMPスヌーピングによって処理されます。

MVR と vPC

- IGMPスヌーピングと同様に、vPCピアスイッチで受信されたIGMP制御メッセージは、ピア間で交換され、MVRグループ情報を同期できます。
- MVR設定は、ピア間で一貫している必要があります。
- **no ip igmp snooping mrouter vpc-peer-link** 設定オプションがMVRに適用されます。 このコマンドを使用すると、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およびレシーバVLANのピアリンクに送信されません。

MVR のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	この機能には、ライセンスは必要ありません。 ライセンスパッケージに含まれていない機能はすべてCisco NX-OSシステムイメージにバンドルされており、追加費用は一切発生しません。 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。

MVR に関する注意事項と制約事項

MVR を設定する場合は、次の注意事項に従ってください。

- MVR は、個々のポート、ポート チャネル、仮想イーサネット（vEth）ポートなどのレイヤ 2 イーサネット ポートでのみサポートされます。
- MVR レシーバ ポートはアクセス ポートでなければなりません。トランク ポートにはできません。 MVR 送信元ポートは、アクセス ポートまたはトランク ポートのどちらかにする必要があります。
- プライオリティ タギングは、MVR レシーバ ポートではサポートされません。
- プライベート VLAN（PVLAN）を使用する場合、セカンダリ VLAN を MVR VLAN として設定できません。
- MVR VLAN の合計数は 250 未満にする必要があります。

デフォルトの MVR 設定

パラメータ	デフォルト
MVR	グローバルおよびインターフェイス単位でディセーブル
グローバル MVR VLAN	未設定
インターフェイスのデフォルト（ポート単位）	受信ポートでも送信元ポートでもない

MVR の設定

MVR グローバル パラメータの設定

手順の概要

1. **configure terminal**
2. [**no**] **mvr**
3. [**no**] **mvr-vlan** *vlan-id*
4. [**no**] **mvr-group** *addr*[/*mask*] [**count** *groups*] [**vlan** *vlan-id*]
5. （任意） **end**
6. （任意） **clear mvr counters** [**source-ports** | **receiver-ports**]
7. （任意） **show mvr**
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **mvr**
	
	例：
	`switch(config)# mvr`
	`switch(config-mvr)#`
		MVR をグローバルにイネーブルにします。 デフォルトではディセーブルになっています。
		MVR をディセーブルにするには、このコマンドの **no** 形式を使用します。

ステップ 3	[**no**] **mvr-vlan** *vlan-id* 例： `switch(config-mvr)# mvr-vlan 100`	グローバルなデフォルト MVR VLAN を指定します。 MVR VLAN は、後続のレシーバが加入するマルチキャスト メッセージの送信元です。 指定できる範囲は 1 ～ 4094 です。 MVR VLAN をクリアするには、コマンドの **no** 形式を使用します。
ステップ 4	[**no**] **mvr-group** *addr*[/*mask*] [**count** *groups*] [**vlan** *vlan-id*] 例： `switch(config-mvr)# mvr-group 230.1.1.1 count 4`	指定した IPv4 アドレスのマルチキャスト グループと（任意の）ネットマスクの長さをグローバルなデフォルト MVR VLAN に追加します。 このコマンドを繰り返して、追加グループを MVR VLAN に追加することができます。

	コマンドまたはアクション	目的
		IP アドレスは *a.b.c.d/m* 形式で入力します。*m* はネットマスクのビット数（1 ～ 31）です。 （任意）指定した IP ドレスから始まる連続マルチキャスト IP アドレスを使用して、MVR グループ数を指定できます。 **count** キーワードを使用して、その後に 1 ～ 64 の番号を指定します。 （任意）**vlan** キーワードを使用して、グループの MVR VLAN を明示的に指定することができます。このキーワードを使用しない場合、グループはデフォルト MVR VLAN に割り当てられます。 グループ設定をクリアするには、コマンドの **no** 形式を使用します。

ステップ 5	**end**
	例：
	`switch(config-mvr)# end`
	`switch#`
		（任意）
		特権 EXEC モードに戻ります。

ステップ 6	**clear mvr counters** [**source-ports** | **receiver-ports**] 例： `switch# clear mvr counters`	（任意） MVR IGMP パケット カウンタをクリアします。
ステップ 7	**show mvr** 例： `switch# show mvr`	（任意） グローバル MVR 設定を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、MVR をグローバルにイネーブルにし、グローバル パラメータを設定する方法を示しています。

```
switch# configure terminal
switch(config)# mvr
switch(config-mvr)# mvr-vlan 100
switch(config-mvr)# mvr-group 230.1.1.1 count 4
switch(config-mvr)# mvr-group 228.1.2.240/28 vlan 101
switch(config-mvr)# mvr-group 235.1.1.6 vlan 340
switch(config-mvr)# end
switch# show mvr
MVR Status           : enabled
Global MVR VLAN      : 100
Number of MVR VLANs  : 3
switch#
```

MVR インターフェイスの設定

手順の概要

1. **configure terminal**
2. **mvr**
3. **interface** {**ethernet** *type slot/port* | **port-channel** *channel-number* | **vethernet** *number*}
4. [**no**] **mvr-type** {**source** | **receiver**}
5. （任意） [**no**] **mvr-vlan** *vlan-id*
6. （任意） [**no**] **mvr-group** *addr*[*/mask*] [**vlan** *vlan-id*]
7. （任意） **end**
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`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	**mvr**
	
	例：
	`switch(config)# mvr`
	`switch(config-mvr)#`
		MVRをグローバルにイネーブルにします。デフォルトではディセーブルになっています。

ステップ 3	**interface** {**ethernet** *type slot/port* | **port-channel** *channel-number* | **vethernet** *number*}
	
	例：
	`switch(config-mvr)# interface ethernet 1/10`
	`switch(config-if)#`
		設定するレイヤ2ポートを指定して、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	[**no**] **mvr-type** {**source** | **receiver**} 例： `switch(config-if)# mvr-type receiver`	MVR ポートを、次のポート タイプのいずれかに設定します。 • **source**：マルチキャスト データを送受信するアップリンク ポートが MVR 送信元として設定されます。 そのポートは、自動的に MVR マルチキャスト グループのスタティック レシーバになります。 送信元ポートを MVR VLAN のメンバにする必要があります。 • **receiver**：MVR マルチキャスト グループに加入するホストに接続されているアクセス ポートが MVR レシーバとして設定され

	コマンドまたはアクション	目的
		ます。 レシーバ ポートでデータを受信するのは、IGMP Leave および Join メッセージを使用してそのポートがマルチキャスト グループのメンバになっている場合だけです。 MVR 特性を使用して非 MVR ポートを設定しようとすると、その設定はキャッシュされますが、そのポートがMVRポートがになるまで有効になりません。 デフォルトのポート モードは非 MVR です。
ステップ 5	[**no**] **mvr-vlan** *vlan-id* 例： `switch(config-if)# mvr-vlan 100`	（任意） インターフェイスで受信された Join 用にグローバルなデフォルト MVR VLAN を上書きするインタフェースのデフォルト MVR VLAN を指定します。 MVR VLAN は、後続のレシーバが加入するマルチキャスト メッセージの送信元です。 指定できる範囲は 1 ～ 4094 です。

ステップ 6	[**no**] **mvr-group** *addr*[*/mask*] [**vlan** *vlan-id*]
	
	例：
	`switch(config-if)# mvr-group 225.1.1.1 vlan 100`
	`switch(config-if)# mvr-group 226.1.1.1 vlan 200`
		（任意）
		指定した IPv4 アドレスのマルチキャスト グループと（任意）ネットワークマスクの長さをインターフェイス MVR VLAN に追加し、グローバル MVR グループ設定を上書きします。 このコマンドを繰り返して、追加グループを MVR VLAN に追加することができます。
		IP アドレスは *a.b.c.d/m* 形式で入力します。*m* はネットマスクのビット数（1 ～ 31）です。
		（任意）**vlan** キーワードを使用して、グループの MVR VLAN を明示的に指定することができます。このキーワードを使用しない場合、グループはインターフェイスのデフォルト MVR VLAN（指定した場合）またはグローバルなデフォルト MVR VLAN に割り当てられます。
		IPv4 アドレスとネットワークマスクをクリアするには、コマンドの **no** 形式を使用します。

ステップ 7	**end**
	
	例：
	`switch(config-if)# end`
	`switch#`
		（任意）
		特権 EXEC モードに戻ります。

ステップ 8	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、イーサネット ポートを MVR レシーバ ポートとして設定する方法を示しています。

```
switch# configure terminal
switch(config)# mvr
switch(config-mvr)# interface ethernet 1/10
switch(config-if)# mvr-type receiver
switch(config-if)# end
switch# copy running-config startup-config
switch#
```

MVR 設定の確認

MVR 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	説明
show mvr	MVR サブシステムの設定およびステータスを表示します。
show mvr groups	MVR グループの設定を表示します。
show mvr interface {**ethernet** *type slot/port* | **port-channel** *number*}	指定したインターフェイスの MVR 設定を表示します。
show mvr members [**count**]	すべての MVR メンバーの数と詳細を表示します。
show mvr members interface {**ethernet** *type slot/port* | **port-channel** *number*}	指定したインターフェイスの MVR メンバの詳細を表示します。
show mvr members vlan *vlan-id*	指定した VLAN の MVR メンバの詳細を表示します。
show mvr receiver-ports [**ethernet** *type slot/port* | **port-channel** *number*]	すべてのインターフェイスまたは指定したインターフェイスのすべての MVR レシーバ ポートを表示します。
show mvr source-ports [**ethernet** *type slot/port* | **port-channel** *number*]	すべてのインターフェイスまたは指定したインターフェイスのすべての MVR 送信元ポートを表示します。

例

次に、MVR パラメータを確認する例を示します。

```
switch# show mvr
MVR Status          : enabled
Global MVR VLAN     : 100
Number of MVR VLANs : 4
```

次に、MVR グループ設定を確認する例を示します。

```
switch# show mvr groups
* - Global default MVR VLAN.

Group start    Group end       Count  MVR-VLAN Interface
                               Mask
-------------  --------------- ------ -------- -----------
228.1.2.240    228.1.2.255     /28     101
230.1.1.1      230.1.1.4        4     *100
235.1.1.6      235.1.1.6        1      340
225.1.3.1      225.1.3.1        1     *100     Eth1/10
```

次に、MVR インターフェイス設定とステータスを確認する例を示します。

```
switch# show mvr interface
Port          VLAN Type      Status    MVR-VLAN
----          ---- ----      ------    --------
Po10          100  SOURCE    ACTIVE    100-101
Po201         201  RECEIVER  ACTIVE    100-101,340
Po202         202  RECEIVER  ACTIVE    100-101,340
Po203         203  RECEIVER  ACTIVE    100-101,340
Po204         204  RECEIVER  INACTIVE  100-101,340
Po205         205  RECEIVER  ACTIVE    100-101,340
Po206         206  RECEIVER  ACTIVE    100-101,340
Po207         207  RECEIVER  ACTIVE    100-101,340
Po208         208  RECEIVER  ACTIVE    2000-2001
Eth1/9        340  SOURCE    ACTIVE    340
Eth1/10       20   RECEIVER  ACTIVE    100-101,340
Eth2/2        20   RECEIVER  ACTIVE    100-101,340
Eth102/1/1    102  RECEIVER  ACTIVE    100-101,340
Eth102/1/2    102  RECEIVER  INACTIVE  100-101,340
Eth103/1/1    103  RECEIVER  ACTIVE    100-101,340
Eth103/1/2    103  RECEIVER  ACTIVE    100-101,340

Status INVALID indicates one of the following misconfiguration:
a) Interface is not a switchport.
b) MVR receiver is not in access, pvlan host or pvlan promiscuous mode.
c) MVR source is in fex-fabric mode.
```

次に、すべての MVR メンバを表示する例を示します。

```
switch# show mvr members
MVR-VLAN  Group Address  Status   Members
--------  -------------  -------  -------
100       230.1.1.1      ACTIVE   Po201 Po202 Po203 Po205 Po206
100       230.1.1.2      ACTIVE   Po205 Po206 Po207 Po208
340       235.1.1.6      ACTIVE   Eth102/1/1
101       225.1.3.1      ACTIVE   Eth1/10 Eth2/2
101       228.1.2.241    ACTIVE   Eth103/1/1 Eth103/1/2
```

次に、すべてのインターフェイスのすべての MVR レシーバ ポートを表示する例を示します。

```
switch# show mvr receiver-ports
Port          MVR-VLAN  Status   Joins         Leaves
                                 (v1,v2,v3)
------------  --------  -------- ------------  ------------
Po201         100       ACTIVE   8             2
Po202         100       ACTIVE   8             2
Po203         100       ACTIVE   8             2
Po204         100       INACTIVE 0             0
Po205         100       ACTIVE   10            6
Po206         100       ACTIVE   10            6
Po207         100       ACTIVE   5             0
Po208         100       ACTIVE   6             0
Eth1/10       101       ACTIVE   12            2
Eth2/2        101       ACTIVE   12            2
Eth102/1/1    340       ACTIVE   16            15
Eth102/1/2    340       INACTIVE 16            16
Eth103/1/1    101       ACTIVE   33            0
Eth103/1/2    101       ACTIVE   33            0
```

次に、すべてのインターフェイスのすべての MVR 送信元ポートを表示する例を示します。

```
switch# show mvr source-ports
Port          MVR-VLAN  Status
------------  --------  --------
Po10          100       ACTIVE
Eth1/9        340       ACTIVE
```

第 19 章

トラフィック ストーム制御の設定

この章の内容は、次のとおりです。

トラフィック ストーム制御の概要

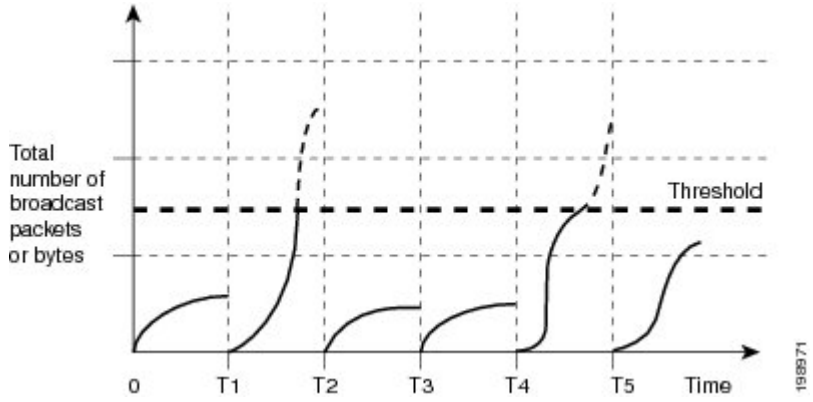
トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御機能を使用すると、物理インターフェイス上におけるブロードキャスト、マルチキャスト、または未知のユニキャスト トラフィック ストームによって、イーサネット インターフェイス経由の通信が妨害されるのを防ぐことができます。

トラフィック ストーム制御（トラフィック抑制ともいう）では、ブロードキャスト、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。

次の図に、指定したタイム インターバル期間中におけるイーサネット インターフェイス上のブロードキャスト トラフィック パターンを示します。 この例では、トラフィック ストーム制御が

T1 と T2 時間の間、および T4 と T5 時間の間で発生します。 これらのインターバル中に、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 *27*：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 5000 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と制約事項

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

- 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。

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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** {**ethernet** *slot*/*port* | **port-channel** *number*}
3. switch(config-if)# **storm-control** {**broadcast** | **multicast** | **unicast**} **level** *percentage*[.*fraction*]

手順の詳細

	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 ストーム設定

次の表に、トラフィック ストーム制御パラメータのデフォルト設定値を示します。

表 *16*：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

第 20 章

ファブリック エクステンダの設定

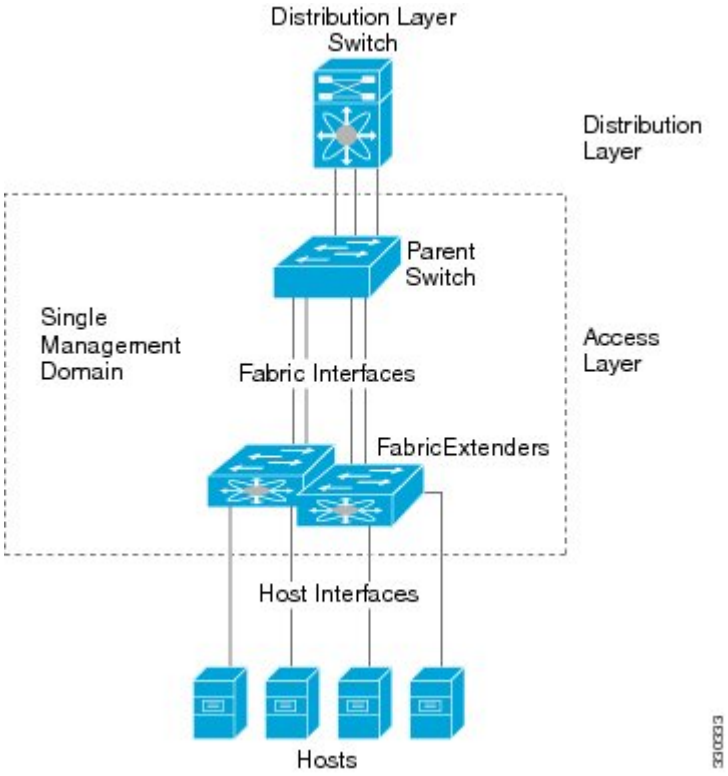
この章の内容は、次のとおりです。

Cisco Nexus 2000 シリーズ ファブリック エクステンダについて

FEX とも呼ばれる Cisco Nexus 2000 シリーズ ファブリック エクステンダは、高度にスケーラブルで柔軟なサーバ ネットワーキング ソリューションで、Cisco Nexus シリーズ デバイスと組み合わせることにより、サーバ集約のための高密度で低コストの接続を実現します。 ファブリック エクステンダは、ギガビット イーサネット、10 ギガビット イーサネット、ユニファイド ファブリック、ラック、ブレード サーバなどの環境全体で拡張性を高め、データセンターのアーキテクチャと運用を簡素化するように設計されています。

ファブリック エクステンダは、親スイッチの Cisco Nexus シリーズ デバイスに統合されることで、親デバイスから提供される設定情報を使用して、自動的にプロビジョニングおよび設定を行うことができます。 この統合により、次の図に示されている単一管理ドメインで、多くのサーバやホストが、セキュリティや QoS（Quality Of Service）設定パラメータを含め、親デバイスと同じフィーチャ セットを使用してサポートされます。 ファブリック エクステンダと親スイッチを統合することにより、スパニングツリー プロトコル（STP）を使用することなく、大規模なマルチパス、ループフリー、およびアクティブ-アクティブのデータセンター トポロジが構築できます。

図 *28*： 単一管理ドメイン



Cisco Nexus 2000 シリーズ ファブリック エクステンダは、すべてのトラフィックを親の Cisco Nexus シリーズ デバイスに 10 ギガビット イーサネット ファブリック アップリンクを介して転送します。このため、すべてのトラフィックが Cisco Nexus シリーズデバイスで確立されているポリシーにより検査されます。

ファブリックエクステンダに、ソフトウェアは同梱されません。 ソフトウェアは、親デバイスから自動的にダウンロードおよびアップグレードされます。

ファブリック エクステンダの用語

このマニュアルでは、次の用語を使用しています。

- ファブリック インターフェイス：ファブリック エクステンダから親スイッチへの接続専用の 10 ギガビット イーサネットのアップリンク ポートです。 ファブリック インターフェイスは他の目的には使用できません。 親スイッチに直接接続する必要があります。

（注） ファブリック インターフェイスに対応するインターフェイスが親スイッチにあります。 このインターフェイスを有効にするには、**switchport mode fex-fabric** コマンドを入力します。

- ポート チャネル ファブリック インターフェイス：ファブリック エクステンダから親スイッチへのポート チャネルのアップリンク接続です。 この接続は、単一論理チャネルにバンドルされているファブリック インターフェイスで構成されます。
- ホスト インターフェイス：サーバまたはホスト システムに接続するためのイーサネット ホスト インターフェイスです。

（注） ブリッジまたはスイッチをホストインターフェイスに接続しないでください。これらのインターフェイスは、エンド ホスト接続またはエンド サーバ接続を提供するように設計されています。

- ポート チャネル ホスト インターフェイス：サーバまたはホスト システムに接続するためのポート チャネル ホスト インターフェイスです。

ファブリック エクステンダの機能

Cisco Nexus 2000 シリーズ ファブリック エクステンダを使用すると、単一のスイッチ、および一貫性が維持された単一のスイッチ機能セットが、多くのホストおよびサーバ全体でサポートできます。 単一の管理エンティティ下で大規模なサーバドメインをサポートすることにより、ポリシーが効率的に適用されます。

親スイッチの一部の機能は、ファブリック エクステンダに拡張できません。

レイヤ 2 ホスト インターフェイス

ファブリック エクステンダは、ネットワーク ファブリックでコンピュータ ホストと他のエッジ デバイスの接続を提供します。 デバイスをファブリック エクステンダ ホスト インターフェイスに接続する際には、次の注意事項に従ってください。

- すべてのファブリック エクステンダ ホスト インターフェイスは、BPDU ガードがイネーブルになったスパニングツリー エッジ ポートとして実行され、スパニングツリー ネットワーク ポートとして設定することはできません。
- アクティブ/スタンバイ チーミング、802.3ad ポート チャネル、または他のホスト ベースのリンク冗長性メカニズムを利用しているサーバは、ファブリック エクステンダ ホスト インターフェイスに接続できます。
- スパニングツリーを実行しているデバイスがファブリック エクステンダ ホスト インターフェイスに接続されている場合に、BPDU を受信すると、そのホスト インターフェイスは errdisable ステートになります。
- Cisco Flexlink、vPC（BPDUFilter がイネーブルになっている）などのスパニングツリーに依存しない、リンク冗長性メカニズムを使用するエッジ スイッチは、ファブリック エクステンダ ホスト インターフェイスに接続できます。 スパニングツリーはループの排除に使用されないため、ファブリック エクステンダ ホスト インターフェイスの下でループのないトポロジを保証することに注意する必要があります。

Cisco Discovery Protocol（CDP）パケットを受け入れるようにホスト インターフェイスをイネーブルにできます。 このプロトコルは、リンクの両端でイネーブルになっている場合にだけ機能します。

（注） ファブリック エクステンダが仮想ポート チャネル（vPC）トポロジで設定されているときは、ファブリック インターフェイスで CDP がサポートされません。

入力パケット数および出力パケット数は、ホスト インターフェイスごとに提供されます。

BPDU ガードの詳細については、BPDU ガードの概要, （251 ページ）を参照してください。

ホスト ポート チャネル

Cisco Nexus 2248TP、Cisco Nexus 2232PP、および Cisco Nexus 2224PP では、ポート チャネル ホスト インターフェイス設定をサポートします。 ポート チャネルでは、最大 8 つのインターフェイスを組み合わせることができます。 ポート チャネルは LACP ありでもなしでも設定できます。

VLAN およびプライベート VLAN

ファブリック エクステンダでは、レイヤ 2 VLAN トランクおよび IEEE 802.1Q VLAN カプセル化がサポートされます。 ホスト インターフェイスは、次の制限の下で、プライベート VLAN のメンバになれます。

- ホスト インターフェイスは、独立ポートまたはコミュニティ ポートとしてだけ設定できます。
- ホスト インターフェイスは、無差別ポートとして設定できません。
- ホスト インターフェイスは、プライベート VLAN トランク ポートとして設定できません。

VLAN の詳細については、このマニュアルの「VLAN の設定」の章を参照してください。

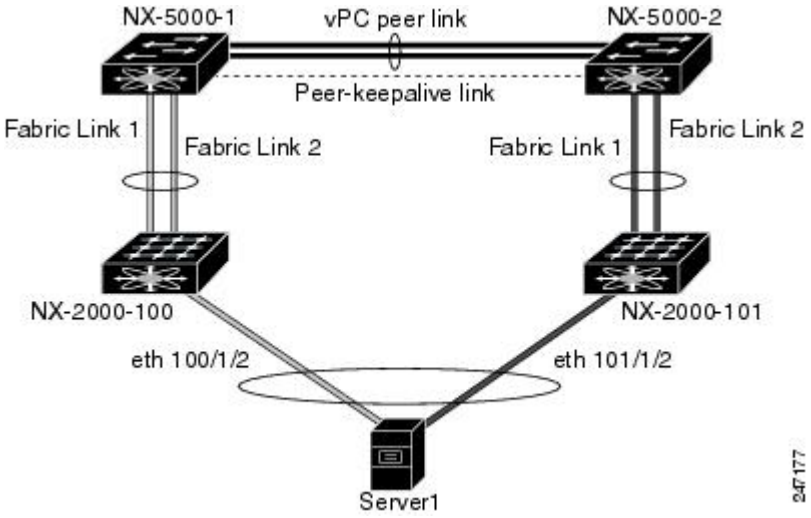
仮想ポート チャネル

仮想ポート チャネル（vPC）を使用して、Cisco Nexus 2000 シリーズ ファブリック エクステンダが親スイッチのペアに接続されているトポロジやファブリック エクステンダのペアが 1 つの親スイッチに接続されているトポロジを設定できます。 vPC では、マルチパス接続を提供できます。この接続を使用すると、ネットワーク上のノード間に冗長性を作成できます。

ファブリック エクステンダでは、次の vPC トポロジが可能です。

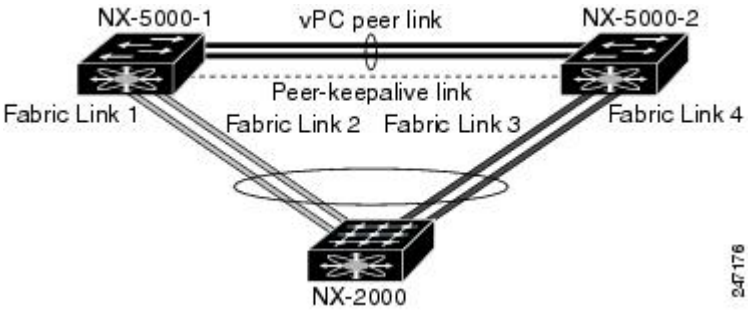
- 親スイッチは、ファブリック エクステンダにシングルホーム接続されます。その後、ファブリック エクステンダは、デュアル インターフェイスを持つサーバに接続されます（次の図を参照）。

図 *29*：シングルホーム接続 ファブリック エクステンダ *vPC* トポロジ



- ファブリック エクステンダは、2 つのアップストリームの親スイッチにデュアルホーム接続され、シングルホーム接続サーバのダウンストリームに接続されます（次の図を参照）。

図 *30*：デュアルホーム接続 ファブリック エクステンダ *vPC* トポロジ



この設定は、アクティブ-アクティブ トポロジとも呼ばれます。

Fibre Channel over Ethernet（FCoE）のサポート

Cisco Nexus 2232PP では、Fibre Channel over Ethernet（FCoE）をサポートしますが、次の制限事項があります。

- ファブリック エクステンダでサポートされるのは、FCoE Initialization Protocol（FIP）対応の統合ネットワーク アダプタ（CNA）だけです。
- ポート チャネルへのバインドは、ポート チャネルの 1 つのメンバのみに制限されます。

設定の詳細については、『*Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide*』（使用している Nexus ソフトウェア リリース版）を参照してください。 このマニュアルの入手可能なバージョンは、次の URL からダウンロードできます。http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

プロトコル オフロード

Cisco Nexus シリーズ デバイスのコントロール プレーンの負荷を低減するために、Cisco NX-OSにリンクレベルのプロトコル処理をファブリック エクステンダ CPU にオフロードする機能が導入されています。 次のプロトコルがサポートされています。

- リンク層検出プロトコル（LLDP）と Data Center Bridging Exchange（DCBX）
- Cisco Discovery Protocol（CDP）
- Link Aggregation Control Protocol（LACP）

Quality of Service

ファブリック エクステンダには、QoS（Quality Of Service）をサポートするために 2 つのユーザ キューが用意されています。1 つはすべての no-drop クラス用で、他の 1 つはすべての drop クラス用です。 親スイッチで設定されているクラスは、これら 2 つのキューのいずれかにマッピングされます。no-drop クラス用のトラフィックは 1 つのキューに、すべての drop クラス用のトラフィックは別のキューにマッピングされます。 出力ポリシーも、これら 2 つのクラスに制限されます。

Cisco Nexus シリーズ デバイスには、マッチング ブロードキャスト用の class-all-flood とマルチキャスト トラフィック用の class-ip-multicast の 2 つの定義済みのクラス マップが用意されています。これらのクラスは、ファブリック エクステンダでは無視されます。

ファブリック エクステンダでは、IEEE 802.1p サービス クラス（CoS）値を使用して、トラフィックを適切なクラスに関連付けます。 ポートごとの QoS 設定と CoS ベースの出力キューイングもサポートされています。

ホスト インターフェイスは、IEEE 802.3x リンク レベル フロー制御（LLC）を使用して実装されているポーズ フレームをサポートします。 すべてのホスト インターフェイスにおいて、デフォルトでフロー制御送信はイネーブル、フロー制御受信はディセーブルです。 自動ネゴシエーションは、ホスト インターフェイスでイネーブルです。 クラスごとのフロー制御は、QoS クラスに従って設定されます。

ホスト インターフェイスはジャンボ フレーム（最大 9216 バイト）をサポートしますが、ホスト インターフェイスごとの最大伝送単位（MTU）はサポートされていません。 代わりに、MTU は QoS クラスに従って設定されます。 MTU を変更するには、親スイッチでポリシーとクラス マップを設定します。 ファブリック エクステンダでは 2 つのユーザ キューしか用意されていないので、drop キューの MTU はすべての drop クラスの最大 MTU に、no-drop キューの MTU はすべての no-drop クラスの最大 MTU に設定されます。

LLC と QoS の詳細については、『*Cisco Nexus 5000 Series NX-OS Quality of Service Configuration Guide*』（使用している Nexus ソフトウェア リリース版）を参照してください。 このマニュアルの入手可能なバージョンは、次の URL からダウンロードできます。http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

アクセス コントロール リスト

ファブリック エクステンダでは、Cisco Nexus シリーズの親デバイスで利用可能なすべての入力アクセス コントロール リスト（ACL）がサポートされます。

ACL の詳細については、『*Cisco Nexus 5000 Series NX-OS Security Configuration Guide*』（使用している Nexus ソフトウェア リリース版）を参照してください。 このマニュアルの入手可能なバージョンは、次の URL からダウンロードできます。http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

IGMP スヌーピング

IGMP スヌーピングは、ファブリック エクステンダのすべてのホスト インターフェイスでサポートされています。

ファブリック エクステンダとその親スイッチは、宛先マルチキャスト MAC アドレスのみに基づいた 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。

（注） 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。 また、『*Cisco Nexus 5000 Series NX-OS Multicast Routing Configuration Guide*』（使用している Nexus ソフトウェア リリース版）を参照してください。このマニュアルの入手可能なバージョンは、次の URL からダウンロードできます。http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

スイッチド ポート アナライザ

ファブリックエクステンダのホストインターフェイスは、スイッチドポートアナライザ（SPAN）送信元ポートとして設定できます。 ファブリック エクステンダのポートは、SPAN 宛先として設定できません。 同じファブリック エクステンダ上のすべてのホスト インターフェイスでサポートされる SPAN セッションは 1 つだけです。 入力送信元（Rx）、出力送信元（Tx）、または両方のモニタリングがサポートされています。

（注） ファブリック エクステンダのホスト インターフェイスが属する VLAN のセットのすべての IP マルチキャスト トラフィックは、SPAN セッションでキャプチャされます。 IP マルチキャスト グループのメンバーシップでトラフィックは分離できません。

同じファブリック エクステンダのホスト インターフェイスに対して入力および出力モニタリングが設定されていると、同じパケットが 2 回表示されます。設定されている Rx とのインターフェイスのパケット入力として 1 回表示され、さらに、設定されている Tx とのインターフェイスのパケット出力として再度表示されます。

SPAN の詳細については、『*Cisco Nexus 5000 Series NX-OS System Management Configuration Guide*』（使用している Nexus ソフトウェア リリース版）を参照してください。 このマニュアルの入手可能なバージョンは、次の URL からダウンロードできます。http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

ファブリック インターフェイスの機能

FEX ファブリック インターフェイスは、スタティック ポート チャネルとプライオリティ フロー制御（PFC）をサポートします。 PFC を使用すると、（インターフェイス上のすべてのトラフィッ

クではなく）インターフェイス上の特定のトラフィック クラスにポーズ機能を適用できます。初期の検出および関連付けプロセスで、SFP+ 検証および Digital Optical Monitoring（DOM）が次のように実行されます。

- FEX で、アップリンク SFP+ トランシーバ上のローカル チェックが実行されます。セキュリティ チェックに失敗すると LED が点灯しますが、リンクは引き続きアップ可能です。
- バックアップ イメージで実行していると、FEX のローカル チェックはバイパスされます。
- ファブリック インターフェイスのアップ時に、親スイッチにより SFP 検証が再実行されます。SFP 検証に失敗すると、ファブリック インターフェイスはダウンしたままになります。

親スイッチの 1 つのインターフェイスが fex-fabric モードに設定されると、そのポートで設定されており、このモードに関連しない他のすべての機能は、非アクティブになります。インターフェイスが再設定されて fex-fabric モードが解除されると、以前の設定が再びアクティブになります。

（注） ファブリック インターフェイスでは、クラスごとのフロー制御モードがデフォルトでイネーブルです。ファブリック インターフェイスが親スイッチで設定されると、PFC モードがデフォルトでイネーブルです。この設定は変更できません。

PFC の詳細については、『*Cisco Nexus 5000 Series NX-OS Quality of Service Configuration Guide*』（使用している Nexus ソフトウェア リリース版）を参照してください。このマニュアルの入手可能なバージョンは、次の URL からダウンロードできます。http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

オーバーサブスクリプション

スイッチ環境におけるオーバーサブスクリプションとは、ポート使用を最適化するために、複数のデバイスを同じインターフェイスに接続することです。インターフェイスは最大速度で動作する接続をサポートします。ほとんどのインターフェイスは最大速度で動作しないため、ポートを共有することにより未使用の帯域幅を有効活用できます。Cisco Nexus 2000 シリーズ ファブリック エクステンダの場合、オーバーサブスクリプションは、アクティブなホスト インターフェイスへの利用可能なファブリック インターフェイスの機能で、イーサネット環境にコスト効果の高い拡張性と柔軟性をもたらします。

Cisco Nexus 2148T ファブリック エクステンダには、4 つの 10 ギガビット イーサネット ファブリック インターフェイスと 48 の 1000 Base-T（1 ギガビット）イーサネット ホスト インターフェイスが用意されています。このため、多くの種類の設定が可能です。たとえば次のように設定できます。

- オーバーサブスクリプションなし（4 つのファブリック インターフェイスに対して 40 のホスト インターフェイス）
- 1.2:1 のオーバーサブスクリプション（4 つのファブリック インターフェイスに対して 48 のホスト インターフェイス）

- 4.8:1 のオーバーサブスクリプション（1 つのファブリック インターフェイスに対して 48 のホスト インターフェイス）

Cisco Nexus 2248TP ファブリック エクステンダには、4 つの 10 ギガビット イーサネット ファブリック インターフェイスと 48 の 100/1000 Base-T（100 メガビット/1 ギガビット）イーサネット ホスト インターフェイスが用意されています。 そのホスト インターフェイスがギガビット イーサネット モードで動作している場合、同様の設定を Cisco Nexus 2148T に提供します。

Cisco Nexus 2248TP については、そのホスト インターフェイスが 100 Mb で動作している場合、オーバーサブスクリプションなしで簡単に動作できます。

Cisco Nexus 2232PP ファブリック エクステンダには、8 つの 10 ギガビット イーサネット ファブリック インターフェイスと 32 の 10 GBase-T イーサネット ホスト インターフェイスが用意されています。すべてのホストインターフェイスでは、使用可能なすべてのファブリック インターフェイスを使用します。（静的ピン接続はサポートされていません。ポートチャネルモードは、ファブリックインターフェイスでのみサポートされます）。すべてのホストインターフェイスでトラフィックをすべてのファブリック インターフェイスに送信する場合、Cisco Nexus 2232PP の最大オーバーサブスクリプション比率は 4:1 です。

Cisco Nexus 2232TM ファブリック エクステンダ には、8 つの 10 ギガビット イーサネット ファブリック インターフェイスと 32 の 10 GBase-T イーサネット ホスト インターフェイスが用意されています。 このため、4:1（1 つのファブリック インターフェイスに対して 4 つのホスト インターフェイス）以上のオーバーサブスクリプションを設定できます。

Cisco Nexus 2224PP ファブリック エクステンダには、2 つの 10 ギガビット イーサネット ファブリック インターフェイスと 24 の 100/1000 Base-T（100 メガビット/1 ギガビット）イーサネット ホスト インターフェイスが用意されています。 このため、1.2:1（2 つのファブリック インターフェイスに対して 24 のホスト インターフェイス）以上のオーバーサブスクリプションを設定できます。

管理モデル

Cisco Nexus 2000 シリーズ ファブリック エクステンダは、親スイッチにより、ゼロタッチ設定モデルを使用してファブリック インターフェイスを介して管理されます。スイッチは、ファブリック エクステンダのファブリック インターフェイスを検出することにより、ファブリック エクステンダを検出します。

ファブリック エクステンダが検出され、親スイッチに正常に関連付けられていると、次の操作が実行されます。

1. スイッチはソフトウェア イメージの互換性を確認し、必要に応じて、ファブリック エクステンダをアップグレードします。
2. スイッチとファブリック エクステンダは、相互にインバンド IP 接続を確立します。 スイッチは、ネットワークで使用されている可能性のある IP アドレスとの競合を避けるために、ファブリック エクステンダにループバック アドレスの範囲（127.15.1.0/24）で IP アドレスを割り当てます。

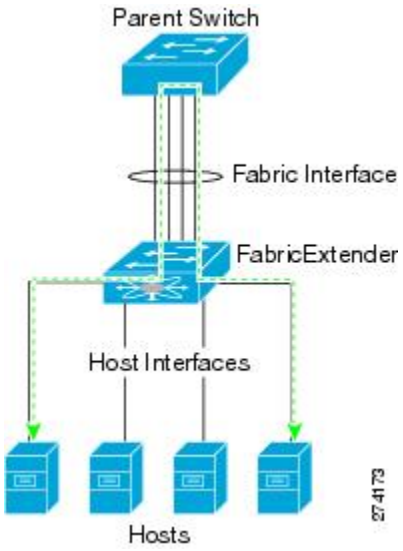
3 スイッチは、設定データを ファブリック エクステンダにプッシュします。 ファブリック エクステンダは、設定をローカルに保存しません。

4 ファブリック エクステンダは、更新された動作ステータスをスイッチに通知します。 ファブリックエクステンダのすべての情報は、スイッチの監視およびトラブルシューティングのためのコマンドを使用して表示されます。

フォワーディング モデル

Cisco Nexus 2000 シリーズ ファブリック エクステンダは、ローカル スイッチングを実行しません。すべてのトラフィックは、セントラルフォワーディングおよびポリシー適用を行う親スイッチに送信されます。このトラフィックには、次の図に示されているように、同じファブリック エクステンダに接続されている 2 つのシステム間でのホスト間通信も含まれます。

図 *31*： フォワーディング モデル



フォワーディング モデルにより、ファブリック エクステンダと Cisco Nexus シリーズ の親デバイス間の機能の一貫性が維持されます。

（注） ファブリックエクステンダは、エンドホスト接続をネットワーク ファブリックに提供します。このため、BPDU ガードがすべてのホスト インターフェイスでイネーブルになります。ブリッジまたはスイッチをホスト インターフェイスに接続すると、そのインターフェイスは BPDU が受信された時点で、エラーディセーブル状態になります。

ファブリック エクステンダのホスト インターフェイスで BPDU ガードはディセーブルにできません。

ファブリックエクステンダは、ネットワークからホストへの出力マルチキャストレプリケーションをサポートします。 ファブリック エクステンダに接続されているマルチキャスト アドレスに対して親スイッチから送信されるパケットは、ファブリック エクステンダの ASIC により複製され、対応するホストに送信されます。

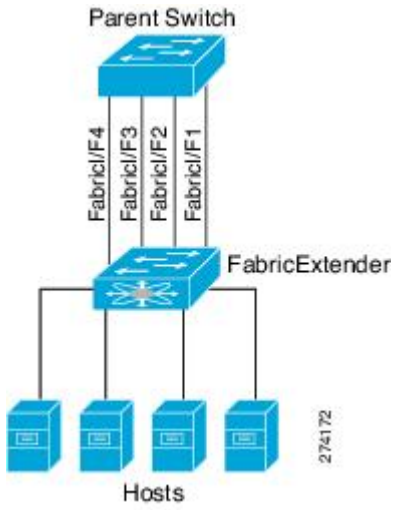
接続モデル

エンドホストから親スイッチへのトラフィックが Cisco Nexus 2000 シリーズ ファブリック エクステンダを通過する際に配信されるようにするために、2 つの方法（静的ピン接続ファブリック インターフェイス接続およびポート チャネル ファブリック インターフェイス接続）が用意されています。

静的ピン接続ファブリック インターフェイス接続

ホスト インターフェイスと親スイッチとの間の決定論的関係を提供するために、個々のファブリック インターフェイス接続を使用するようにファブリック エクステンダを設定できます。 この設定では、次の図で示されるように、10 ギガビット イーサネット ファブリック インターフェイスが接続されます。ファブリックエクステンダのモデルで利用可能な最大数までの範囲で、任意の数のファブリック インターフェイスを利用できます。

図 *32*： 静的ピン接続ファブリック インターフェイス接続



ファブリックエクステンダがアップすると、ホストインターフェイスは利用可能なファブリックインターフェイス間で均等に配布されます。 このため、各エンドホストから親スイッチへの接続に割り当てられている帯域幅はスイッチにより変更されません。常に指定された帯域幅が使用されます。

（注） ファブリック インターフェイスに障害が発生すると、関連付けられているすべてのホスト インターフェイスもダウンし、ファブリック インターフェイスが復旧するまでダウンしたままとなります。

ピン接続ファブリック インターフェイス接続を作成し、親スイッチがホストインターフェイスの配布を決定できるようにするために、**pinning max-links** コマンドを使用する必要があります。 ホストインターフェイスはmax-linksで指定した数で分割され、それに従って配布されます。 max-linksのデフォルト値は 1 です。

注意 **max-links** の値を変更すると、中断が発生します。ファブリック エクステンダのすべてのホスト インターフェイスはダウンし、親スイッチが静的ピン接続を再割り当てすると再びアップします。

ホストインターフェイスのピン接続順序は、最初、ファブリックインターフェイスが設定された順序で決定されます。親スイッチがリブートすると、設定されているファブリックインターフェイスは、ファブリックインターフェイスのポート番号の昇順でホストインターフェイスにピン接続されます。

リブート後にも決定論的で固定的な関連付けを維持するために、ピン接続を手動で再配布できます。

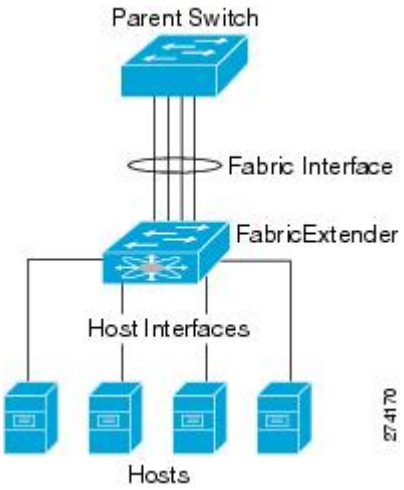
（注） ホスト インターフェイスの再配布は、常に、ファブリック インターフェイスのポート番号の昇順になります。

ポート チャネル ファブリック インターフェイス接続

ホスト インターフェイスと親スイッチとの間のロード バランシングを提供するために、ポート チャネル ファブリック インターフェイス接続を使用するようにファブリック エクステンダを設

定できます。この接続は、次の図に示されているように、10ギガビットイーサネットファブリック インターフェイスを単一の論理チャネルにバンドルします。

図 *33*：ポート チャネル ファブリック インターフェイス接続



親スイッチとの接続にポートチャネルファブリックインターフェイス接続を使用するようにファブリックエクステンダを設定すると、スイッチは、次のロードバランシング基準を使用してリンクを選択することで、ホストインターフェイスポートに接続されているホストからのトラフィックをロードバランシングします。

- レイヤ2フレームに対しては、スイッチは送信元および宛先のMACアドレスを使用します。
- レイヤ 3 フレームに対しては、スイッチは送信元および宛先の MAC アドレスと送信元および宛先の IP アドレスを使用します。

（注） ポート チャネルでファブリック インターフェイスに障害が発生しても、ホスト インターフェイスは影響を受けません。トラフィックは、ポート チャネル ファブリック インターフェイスの残りのリンク間で自動的に再配布されます。ファブリック ポート チャネルのすべてのリンクがダウンすると、FEX のすべてのホスト インターフェイスがダウン状態に設定されます。

ポート番号の表記法

ファブリック エクステンダで使用されるポート番号の表記法は、次のとおりです。

interface ethernet *chassis*/*slot*/*port*

ここで

- *chassis* は管理者により設定されます。ファブリック エクステンダは、個々のファブリック インターフェイスまたはポート チャネル ファブリック インターフェイスを介してCisco Nexus

シリーズ の親デバイスに直接接続されている必要があります。 シャーシ ID をスイッチの物理イーサネットインターフェイスまたはポートチャネルで設定して、それらのインターフェイスで検出されるファブリック エクステンダが識別されるようにします。

シャーシ ID の範囲は、100 ～ 199 です。

（注） シャーシIDが必要になるのは、ファブリックエクステンダのホストインターフェイスにアクセスする場合だけです。 100未満の値は、親スイッチのスロットであることを示します。 スイッチのインターフェイスで使用されるポート番号の表記法は、次のとおりです。

interface ethernet *slot*/*port*

- *slot* は、ファブリック エクステンダでのスロット番号を識別します。
- *port* は、特定のスロットおよびシャーシ ID でのポート番号を識別します。

ファブリック エクステンダ イメージ管理

Cisco Nexus 2000 シリーズ ファブリック エクステンダにソフトウェアは同梱されません。 ファブリック エクステンダのイメージは、親スイッチのシステム イメージにバンドルされています。 イメージは、親スイッチとファブリック エクステンダとの間の関連付け処理時に自動的に検証され、必要に応じてアップデートされます。

install all コマンドを入力すると、親 Cisco Nexus シリーズ スイッチのソフトウェアがアップグレードされ、接続されているファブリック エクステンダのソフトウェアもアップグレードされます。 ダウンタイムを最短にするために、インストールプロセスで新しいソフトウェアイメージがロードされている間、ファブリックエクステンダはオンラインに維持されます。 ソフトウェア イメージが正常にロードされると、親スイッチとファブリック エクステンダは自動的にリブートします。

このプロセスは、親スイッチとファブリック エクステンダとの間のバージョンの互換性を維持するために必要になります。

ファブリック エクステンダのハードウェア

Cisco Nexus 2000 シリーズ ファブリック エクステンダのアーキテクチャでは、さまざまな数および速度のホスト インターフェイスを備えたハードウェア構成を実現できます。

シャーシ

Cisco Nexus 2000 シリーズ ファブリック エクステンダは、ラック マウント用に設計された 1 RU シャーシです。 シャーシでは、冗長ファンおよび電源装置がサポートされます。

イーサネット インターフェイス

Cisco Nexus 2000 シリーズ ファブリック エクステンダには 4 つのモデルがあります。

- Cisco Nexus 2148T には、サーバまたはホストへのダウンリンク接続用に 48 個の 1000 Base-T イーサネット ホスト インターフェイスが搭載されています。また、親スイッチへのアップリンク接続用に SFP+ インターフェイス アダプタが付いた 10 ギガビット イーサネット ファブリック インターフェイスが 4 個搭載されています。
- Cisco Nexus 2224PP には、サーバまたはホストへのダウンリンク接続用に 24 個の 100 Base-T/1000 Base-T イーサネット ホスト インターフェイスが搭載されています。また、親スイッチへのアップリンク接続用に SFP+ インターフェイス アダプタが付いた 10 ギガビット イーサネット ファブリック インターフェイスが 2 個搭載されています。
- Cisco Nexus 2232PP には、親スイッチへのアップリンク接続用に SFP+ インターフェイス アダプタが付いた 32 個の 10 ギガビット イーサネット ホスト インターフェイス、および SFP+ インターフェイス アダプタを備えた 8 個の 10 ギガビット イーサネット ファブリック インターフェイスが搭載されています。
- Cisco Nexus 2248TP には、サーバまたはホストへのダウンリンク接続用に 48 個の 100 Base-T/1000 Base-T イーサネット ホスト インターフェイスが搭載されています。また、親スイッチへのアップリンク接続用に SFP+ インターフェイス アダプタが付いた 10 ギガビット イーサネット ファブリック インターフェイスが 4 個搭載されています。

  Cisco Nexus 2248TP-E は、次の機能を追加した Cisco Nexus 2248TP のすべての機能を備えています。

  - 大きいバーストを緩和するための大きなバッファ。
  - ポートごとの入力および出力 queue-limit のサポート。
  - カウンタのデバッグのサポート。
  - ファブリック エクステンダとスイッチ間の 3000 m のケーブル長での no-drop 動作の一時停止のサポート。
  - ユーザが設定できる共有バッファのサポート。

ファブリックエクステンダのファブリックインターフェイスとのアソシエーションについて

Cisco Nexus 2000 シリーズ ファブリック エクステンダは、物理イーサネットまたはポート チャネルを介して親デバイスに接続されます。 ファブリック エクステンダは、デフォルトでは、FEX-number を割り当てるか、接続するインターフェイスに関連付けるまで、親デバイスに接続できません。

（注） ファブリック エクステンダは、複数の異なる物理イーサネット インターフェイスまたは 1 つのポート チャネル インターフェイスを介してスイッチに接続できます。

（注） 親スイッチに接続されるファブリック エクステンダを設定して使用する前に、**feature fex** コマンドを使用してファブリック エクステンダの機能をイネーブルにする必要があります。

ファブリック エクステンダのイーサネット インターフェイスとのアソシエーション

はじめる前に

ファブリック エクステンダ機能がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. **switchport mode fex-fabric**
4. **fex associate** *FEX-number*
5. （任意） **show interface ethernet** *port*/*slot* **fex-intf**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**interface ethernet** *slot*/*port*
	
	例：
	`switch(config)# interface ethernet 1/40`
	`switch(config)#`
		設定するイーサネット インターフェイスを指定します。

ステップ 3	**switchport mode fex-fabric**
	
	例：
	`switch(config-if)# switchport mode fex-fabric`
	`switch(config-if)#`
		外部ファブリック エクステンダをサポートするように、インターフェイスを設定します。

	コマンドまたはアクション	目的

ステップ 4	**fex associate** *FEX-number*
	
	例：
	`switch(config-if)# fex associate 101`
	`switch#`
		インターフェイスに接続されているファブリック エクステンダ装置に、FEX-number をアソシエートします。 FEX-number の範囲は 100 ～ 199 です。

ステップ 5	**show interface ethernet** *port*/*slot* **fex-intf**
	
	例：
	`switch# show interface ethernet 1/40 fex-intf`
	`switch#`
		（任意）
		ファブリック エクステンダのイーサネット インターフェイスへのアソシエーションを表示します。

次に、ファブリック エクステンダをスイッチのイーサネット インターフェイスにアソシエートする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/40
switch(config-if)# switchport mode fex-fabric
switch(config-if)# fex associate 101
switch(config)#
```

次に、ファブリック エクステンダと親デバイスとのアソシエーションを表示する例を示します。

```
switch# show interface ethernet 1/40 fex-intf
Fabric           FEX
Interface        Interfaces
---------------------------------------------------
Eth1/40          Eth101/1/48   Eth101/1/47   Eth101/1/46   Eth101/1/45
                 Eth101/1/44   Eth101/1/43   Eth101/1/42   Eth101/1/41
                 Eth101/1/40   Eth101/1/39   Eth101/1/38   Eth101/1/37
                 Eth101/1/36   Eth101/1/35   Eth101/1/34   Eth101/1/33
                 Eth101/1/32   Eth101/1/31   Eth101/1/30   Eth101/1/29
                 Eth101/1/28   Eth101/1/27   Eth101/1/26   Eth101/1/25
                 Eth101/1/24   Eth101/1/23   Eth101/1/22   Eth101/1/21
                 Eth101/1/20   Eth101/1/19   Eth101/1/18   Eth101/1/17
                 Eth101/1/16   Eth101/1/15   Eth101/1/14   Eth101/1/13
                 Eth101/1/12   Eth101/1/11   Eth101/1/10   Eth101/1/9
                 Eth101/1/8    Eth101/1/7    Eth101/1/6    Eth101/1/5
                 Eth101/1/4    Eth101/1/3    Eth101/1/2    Eth101/1/1
```

ファブリック エクステンダのポート チャネルとのアソシエーション

はじめる前に

ファブリック エクステンダ フィーチャが、イネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface port-channel** *channel*
3. **switchport mode fex-fabric**
4. **fex associate** *FEX-number*
5. （任意） **show interface port-channel** *channel* **fex-intf**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *channel*
	
	例：
	`switch(config)# interface port-channel 4`
	`switch(config-if)#`
		設定するポート チャネルを指定します。

ステップ 3	**switchport mode fex-fabric** 例： `switch(config-if)# switchport mode fex-fabric`	外部ファブリック エクステンダをサポートするように、ポート チャネルを設定します。
ステップ 4	**fex associate** *FEX-number* 例： `switch(config-if)# fex associate 101`	インターフェイスに接続されているファブリック エクステンダ装置に、FEX-number をアソシエートします。 FEX-number の範囲は 100 ～ 199 です。
ステップ 5	**show interface port-channel** *channel* **fex-intf** 例： `switch# show interface port-channel 4 fex-intf`	（任意） ファブリック エクステンダのポート チャネル インターフェイスへのアソシエーションを表示します。

例

次に、ファブリック エクステンダを親デバイスのポートチャネルインターフェイスにアソシエートする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/28
switch(config-if)# no shutdown
switch(config-if)# channel-group 4
switch(config-if)# exit
switch(config)# interface ethernet 1/29
```

```
switch(config-if)# no shutdown
switch(config-if)# channel-group 4
switch(config-if)# exit
switch(config)# interface ethernet 1/30
switch(config-if)# no shutdown
switch(config-if)# channel-group 4
switch(config-if)# exit
switch(config)# interface ethernet 1/31
switch(config-if)# no shutdown
switch(config-if)# channel-group 4
switch(config-if)# exit
switch(config)# interface port-channel 4
switch(config-if)# switchport
switch(config-if)# switchport mode fex-fabric
switch(config-if)# fex associate 101
```

ヒント　シスコでは、物理インターフェイスからではなく、ポート チャネル インターフェイスのみから **fex associate** コマンドを発行することを推奨します。

物理ポートをポート チャネルに接続する前に、その物理ポートを FEX にアソシエートしようとすると、その物理ポートはエラーディセーブル ステートに移行し、Cisco Nexus 7000 スイッチはそのリンク上の FEX と通信しません。エラーディセーブル ステートをクリアし、そのリンクをアップ状態にするには、**shutdown** コマンドと **no shutdown** コマンドをイーサネット インターフェイス（ポート チャネル インターフェイスではなく）で発行する必要があります。これは、ケーブル接続の前に設定を実行する場合には当てはまりません。

（注）　物理インターフェイスをポート チャネルに追加する際には、ポート チャネルと物理インターフェイス上の設定が一致していなければなりません。

次に、ファブリック エクステンダと親デバイスとのアソシエーションを表示する例を示します。

```
switch# show interface port-channel 4 fex-intf
Fabric           FEX
Interface        Interfaces
---------------------------------------------------
Po4              Eth101/1/48   Eth101/1/47   Eth101/1/46   Eth101/1/45
                 Eth101/1/44   Eth101/1/43   Eth101/1/42   Eth101/1/41
                 Eth101/1/40   Eth101/1/39   Eth101/1/38   Eth101/1/37
                 Eth101/1/36   Eth101/1/35   Eth101/1/34   Eth101/1/33
                 Eth101/1/32   Eth101/1/31   Eth101/1/30   Eth101/1/29
                 Eth101/1/28   Eth101/1/27   Eth101/1/26   Eth101/1/25
                 Eth101/1/24   Eth101/1/23   Eth101/1/22   Eth101/1/21
                 Eth101/1/20   Eth101/1/19   Eth101/1/18   Eth101/1/17
                 Eth101/1/16   Eth101/1/15   Eth101/1/14   Eth101/1/13
                 Eth101/1/12   Eth101/1/11   Eth101/1/10   Eth101/1/9
                 Eth101/1/8    Eth101/1/7    Eth101/1/6    Eth101/1/5
                 Eth101/1/4    Eth101/1/3    Eth101/1/2    Eth101/1/1
```

インターフェイスからファブリックエクステンダのアソシエーションの解除

はじめる前に

ファブリック エクステンダ フィーチャが、イネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface** {**ethernet** *slot*/*port* | **port-channel** *channel*}
3. **no fex associate**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**interface** {**ethernet** *slot*/*port*	**port-channel** *channel*}
		
		例：
		`switch(config)# interface port-channel 4`
		`switch(config-if)#`
			設定するインターフェイスを指定します。 インターフェイスは、イーサネット インターフェイスまたはポート チャネルにすることができます。

ステップ 3	**no fex associate** 例： `switch(config-if)# no fex associate`	インターフェイスに接続されているファブリック エクステンダ装置の関連付けを解除します。

ファブリック エクステンダのグローバル機能の設定

はじめる前に

ファブリック エクステンダ機能がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **fex** *FEX-number*
3. （任意） **description** *desc*
4. （任意） **no description**
5. （任意） **type** *FEX-type*
6. （任意） **no type**
7. （任意） **pinning max-links** *uplinks*
8. （任意） **no pinning max-links**
9. （任意） **serial** *serial*
10. （任意） **no serial**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**fex** *FEX-number*
	
	例：
	`switch(config)# fex 101`
	`switch(config-fex)#`
		指定されたファブリック エクステンダの設定モードを開始します。
		FEX-number の範囲は 100 ～ 199 です。

ステップ 3	**description** *desc*
	
	例：
	`switch(config-fex)#`
	`description Rack7A-N2K`
		（任意）
		説明を指定します。 デフォルトは、文字列 FEX*xxxx* で、*xxxx* は FEX-number です。 FEX-number が 123 の場合、説明は FEX0123 です。

ステップ 4	**no description**
	
	例：
	`switch(config-fex)# no`
	`description`
		（任意）
		説明を削除します。

ステップ 5	**type** *FEX-type*
	
	例：
	`switch(config-fex)# type`
	`N2248T`
		（任意）
		ファブリック エクステンダのタイプを指定します。 FEX-type は次のいずれかです。
		• N2148T：48 個の 1000 Base-T イーサネット ホスト インターフェイスと 4 個の 10 ギガビット SFP+イーサネット ファブリック インターフェイス モジュール

	コマンドまたはアクション	目的
		• N2224TP：24 個の 100 Base-T/1000Base-T イーサネット ホスト インターフェイスと 2 個の 10 ギガビット SFP+ イーサネット ファブリック インターフェイス モジュール • N2232P：32 個の 10 ギガビット SFP+ イーサネット ホスト インターフェイスと 8 個の 10 ギガビット SFP+ イーサネット ファブリック インターフェイス モジュール • N2232TP：32 個の 10 ギガビット Base-T+ イーサネット ホスト インターフェイスと 8 個の 10 ギガビット SFP+ イーサネット ファブリック インターフェイス モジュール • N2232TT：32 個の 10 ギガビット Base-T+ イーサネット ホスト インターフェイスと 8 個の 10 ギガビット Base-T イーサネット ファブリック インターフェイス モジュール • N2248T および N2248TP-E：48 個の 100 ギガビット Base-T/1000Base-T+ イーサネット ホスト インターフェイスと 4 個の 10 ギガビット SFP+ イーサネット ファブリック インターフェイス モジュール Cisco Nexus シリーズの親デバイスは、バイナリ コンフィギュレーションにあるファブリック エクステンダのタイプを記憶します。 この機能が設定されると、ファブリック エクステンダがオンラインになるのは、そのタイプが設定済みの FEX-type と一致する場合だけです。
ステップ 6	**no type** 例： `switch(config-fex)# no type`	（任意） FEX-type を削除します。 この場合、ファブリック エクステンダがファブリック インターフェイスに接続されても、親スイッチのバイナリ コンフィギュレーションに以前保存された設定済みタイプと一致しないと、ファブリック エクステンダのすべてのインターフェイスのすべての設定が削除されます。
ステップ 7	**pinning max-links** *uplinks* 例： `switch(config-fex)# pinning max-links 2`	（任意） アップリンクの数を定義します。 デフォルトは 1 です。 指定できる範囲は 1 ～ 4 です。 このコマンドは、ファブリック エクステンダが 1 つまたは複数の静的にピン接続されたファブリック インターフェイスを使用して親スイッチに接続されている場合だけ、適用できます。 ポート チャネル接続は 1 つだけ可能です。 **注意** **pinning max-links** コマンドを使用してアップリンク数を変更すると、ファブリック エクステンダのすべてのホスト インターフェイス ポートが中断されます。

	コマンドまたはアクション	目的
ステップ 8	**no pinning max-links** 例： `switch(config-fex)# no pinning max-links`	（任意） アップリンクの数をデフォルトにリセットします。 **注意** **no pinning max-links** コマンドを使用してアップリンク数を変更すると、ファブリック エクステンダのすべてのホスト インターフェイス ポートが中断されます。
ステップ 9	**serial** *serial* 例： `switch(config-fex)# serial JAF1339BDSK`	（任意） シリアル番号文字列を定義します。このコマンドが設定され、ファブリック エクステンダが一致するシリアル番号文字列を報告する場合、スイッチでは、対応するシャーシ ID だけが関連付けることができます（**fex associate** コマンドを使用します）。 **注意** 指定したファブリック エクステンダのシリアル番号と一致しないシリアル番号を設定すると、ファブリック エクステンダは強制的にオフラインになります。
ステップ 10	**no serial** 例： `switch(config-fex)# no serial`	（任意） シリアル番号文字列を削除します。

ファブリック エクステンダのロケータ LED のイネーブル化

ファブリック エクステンダのロケータ ビーコン LED の点灯により、特定のファブリック エクステンダをラック内で見つけることができます。

手順の概要

1. **locator-led fex** *FEX-number*
2. （任意） **no locator-led fex** *FEX-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**locator-led fex** *FEX-number* 例： `switch# locator-led fex 101`	特定のファブリック エクステンダのロケータ ビーコン LED を点灯します。

	コマンドまたはアクション	目的
ステップ 2	**no locator-led fex** *FEX-number* 例： `switch# no locator-led fex 101`	（任意） 特定のファブリック エクステンダのロケータ ビーコン LED を消灯します。

リンクの再配布

静的にピン接続されたインターフェイスを使用してファブリック エクステンダをプロビジョニングすると、ファブリック エクステンダのダウンリンク ホスト インターフェイスは、最初に設定された順序でファブリック インターフェイスにピン接続されます。 ファブリック インターフェイスへのホスト インターフェイスの特別な関係がリブートしても維持されるようにするには、リンクを再びピン接続する必要があります。

この機能は、次の 2 つの状況で行うことができます。

- max-links 設定を変更する必要がある場合。
- ファブリック インターフェイスへのホスト インターフェイスのピン接続順序を維持する必要がある場合。

リンク数の変更

最初に親スイッチの特定のポート（たとえば、ポート33）を唯一のファブリックインターフェイスとして設定すると、48のすべてのホストインターフェイスがこのポートにピン接続されます。35 などの他のポートをプロビジョニングするには、**pinning max-links 2** コマンドを使用してホスト インターフェイスを再配布します。 これにより、すべてのホスト インターフェイスがダウンし、ホスト インターフェイス 1 ～ 24 はファブリック インターフェイス 33 に、ホスト インターフェイス 25 ～ 48 はファブリック インターフェイス 35 にピン接続されます。

ピン接続順序の維持

ホストインターフェイスのピン接続順序は、最初、ファブリックインターフェイスが設定された順序で決定されます。 この例では、4 つのファブリック インターフェイスが次の順序で設定されます。

```
switch# show interface ethernet 1/35 fex-intf
Fabric          FEX
Interface       Interfaces
---------------------------------------------------
 Eth1/35        Eth101/1/12   Eth101/1/11   Eth101/1/10   Eth101/1/9
                Eth101/1/8    Eth101/1/7    Eth101/1/6    Eth101/1/5
                Eth101/1/4    Eth101/1/3    Eth101/1/2    Eth101/1/1

switch# show interface ethernet 1/33 fex-intf
```

```
Fabric           FEX
Interface        Interfaces
---------------------------------------------------
 Eth1/33         Eth101/1/24   Eth101/1/23   Eth101/1/22   Eth101/1/21
                 Eth101/1/20   Eth101/1/19   Eth101/1/18   Eth101/1/17
                 Eth101/1/16   Eth101/1/15   Eth101/1/14   Eth101/1/13

switch# show interface ethernet 1/38 fex-intf
Fabric           FEX
Interface        Interfaces
---------------------------------------------------
 Eth1/38         Eth101/1/36   Eth101/1/35   Eth101/1/34   Eth101/1/33
                 Eth101/1/32   Eth101/1/31   Eth101/1/30   Eth101/1/29
                 Eth101/1/28   Eth101/1/27   Eth101/1/26   Eth101/1/25

switch# show interface ethernet 1/40 fex-intf
Fabric           FEX
Interface        Interfaces
---------------------------------------------------
 Eth1/40         Eth101/1/48   Eth101/1/47   Eth101/1/46   Eth101/1/45
                 Eth101/1/44   Eth101/1/43   Eth101/1/42   Eth101/1/41
                 Eth101/1/40   Eth101/1/39   Eth101/1/38   Eth101/1/37
```

ファブリック エクステンダを次回リブートすると、設定されたファブリック インターフェイスは、ファブリックインターフェイスのポート番号の昇順でホストインターフェイスにピン接続されます。 ファブリック エクステンダを再起動せずに同じ固定配布でホスト インターフェイスを設定するには、**fex pinning redistribute** コマンドを入力します。

ホスト インターフェイスの再配布

注意 このコマンドにより、ファブリック エクステンダのすべてのホスト インターフェイス ポートが中断されます。

手順の概要

1. **configure terminal**
2. **fex pinning redistribute** *FEX-number*

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**fex pinning redistribute** *FEX-number*
	
	例：
	`switch(config) # fex pinning redistribute 101`
	`switch(config) #`
		ホスト接続を再配布します。 *FEX-number* の範囲は 100 ～ 199 です。

ファブリック エクステンダ設定の確認

ファブリック エクステンダで定義されている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実行します。

コマンドまたはアクション	目的
show fex [*FEX-number*] [**detail**]	特定のファブリック エクステンダまたは接続されているすべての装置の情報を表示します。
show interface *type number* **fex-intf**	特定のスイッチインターフェイスにピン接続されているファブリック エクステンダのポートを表示します。
show interface fex-fabric	ファブリック エクステンダのアップリンクを検出しているスイッチインターフェイスを表示します。
show interface ethernet *number* **transceiver** [**fex-fabric**]	ファブリック エクステンダのアップリンクの SFP+ トランシーバおよび Diagnostic Optical Monitoring（DOM）の情報を表示します。
show feature-set	デバイスフィーチャ セットのステータスを表示します。

ファブリック エクステンダの設定例

次に、接続されているすべてのファブリック エクステンダ装置を表示する例を示します。

```
switch# show fex
  FEX         FEX           FEX                  FEX
Number    Description      State            Model            Serial
------------------------------------------------------------------------
100     FEX0100               Online     N2K-C2248TP-1GE   JAF1339BDSK
101     FEX0101               Online     N2K-C2232P-10GE   JAF1333ADDD
102     FEX0102               Online     N2K-C2232P-10GE   JAS12334ABC
```

次に、特定のファブリック エクステンダの詳細なステータスを表示する例を示します。

```
switch# show fex 100 detail
FEX: 100 Description: FEX0100   state: Online
  FEX version: 5.0(2)N1(1) [Switch version: 5.0(2)N1(1)]
  FEX Interim version: 5.0(2)N1(0.205)
  Switch Interim version: 5.0(2)N1(0.205)
  Extender Model: N2K-C2224TP-1GE,  Extender Serial: JAF1427BQLG
  Part No: 73-13373-01
  Card Id: 132, Mac Addr: 68:ef:bd:62:2a:42, Num Macs: 64
  Module Sw Gen: 21  [Switch Sw Gen: 21]
  post level: complete
 pinning-mode: static    Max-links: 1
```

```
  Fabric port for control traffic: Eth1/29
  Fabric interface state:
    Po100 - Interface Up. State: Active
    Eth1/29 - Interface Up. State: Active
    Eth1/30 - Interface Up. State: Active
  Fex Port         State  Fabric Port  Primary Fabric
       Eth100/1/1    Up       Po100       Po100
       Eth100/1/2    Up       Po100       Po100
       Eth100/1/3    Up       Po100       Po100
       Eth100/1/4    Up       Po100       Po100
       Eth100/1/5    Up       Po100       Po100
       Eth100/1/6    Up       Po100       Po100
       Eth100/1/7    Up       Po100       Po100
       Eth100/1/8    Up       Po100       Po100
       Eth100/1/9    Up       Po100       Po100
      Eth100/1/10    Up       Po100       Po100
      Eth100/1/11    Up       Po100       Po100
      Eth100/1/12    Up       Po100       Po100
      Eth100/1/13    Up       Po100       Po100
      Eth100/1/14    Up       Po100       Po100
      Eth100/1/15    Up       Po100       Po100
      Eth100/1/16    Up       Po100       Po100
      Eth100/1/17    Up       Po100       Po100
      Eth100/1/18    Up       Po100       Po100
      Eth100/1/19    Up       Po100       Po100
      Eth100/1/20    Up       Po100       Po100
      Eth100/1/21    Up       Po100       Po100
      Eth100/1/22    Up       Po100       Po100
      Eth100/1/23    Up       Po100       Po100
      Eth100/1/24    Up       Po100       Po100
      Eth100/1/25    Up       Po100       Po100
      Eth100/1/26    Up       Po100       Po100
      Eth100/1/27    Up       Po100       Po100
      Eth100/1/28    Up       Po100       Po100
      Eth100/1/29    Up       Po100       Po100
      Eth100/1/30    Up       Po100       Po100
      Eth100/1/31    Up       Po100       Po100
      Eth100/1/32    Up       Po100       Po100
      Eth100/1/33    Up       Po100       Po100
      Eth100/1/34    Up       Po100       Po100
      Eth100/1/35    Up       Po100       Po100
      Eth100/1/36    Up       Po100       Po100
      Eth100/1/37    Up       Po100       Po100
      Eth100/1/38    Up       Po100       Po100
      Eth100/1/39    Up       Po100       Po100
      Eth100/1/40  Down       Po100       Po100
      Eth100/1/41    Up       Po100       Po100
      Eth100/1/42    Up       Po100       Po100
      Eth100/1/43    Up       Po100       Po100
      Eth100/1/44    Up       Po100       Po100
      Eth100/1/45    Up       Po100       Po100
      Eth100/1/46    Up       Po100       Po100
      Eth100/1/47    Up       Po100       Po100
      Eth100/1/48    Up       Po100       Po100
Logs:
02/05/2010 20:12:17.764153: Module register received
02/05/2010 20:12:17.765408: Registration response sent
02/05/2010 20:12:17.845853: Module Online Sequence
02/05/2010 20:12:23.447218: Module Online
```

次に、特定のスイッチインターフェイスにピン接続されているファブリック エクステンダのインターフェイスを表示する例を示します。

```
switch# show interface port-channel 100 fex-intf
Fabric           FEX
Interface        Interfaces
---------------------------------------------------
 Po100           Eth100/1/48   Eth100/1/47   Eth100/1/46   Eth100/1/45
                 Eth100/1/44   Eth100/1/43   Eth100/1/42   Eth100/1/41
                 Eth100/1/40   Eth100/1/39   Eth100/1/38   Eth100/1/37
                 Eth100/1/36   Eth100/1/35   Eth100/1/34   Eth100/1/33
                 Eth100/1/32   Eth100/1/31   Eth100/1/30   Eth100/1/29
```

```
Eth100/1/28   Eth100/1/27   Eth100/1/26   Eth100/1/25
Eth100/1/24   Eth100/1/22   Eth100/1/20   Eth100/1/19
Eth100/1/18   Eth100/1/17   Eth100/1/16   Eth100/1/15
Eth100/1/14   Eth100/1/13   Eth100/1/12   Eth100/1/11
Eth100/1/10   Eth100/1/9    Eth100/1/8    Eth100/1/7
Eth100/1/6    Eth100/1/5    Eth100/1/4    Eth100/1/3
Eth100/1/2    Eth100/1/1
```

次に、ファブリックエクステンダのアップリンクに接続されているスイッチインターフェイスを表示する例を示します。

```
switch# show interface fex-fabric
     Fabric      Fabric       Fex                FEX
Fex  Port      Port State    Uplink    Model          Serial
--------------------------------------------------------------
100   Eth1/29        Active     3    N2K-C2248TP-1GE  JAF1339BDSK
100   Eth1/30        Active     4    N2K-C2248TP-1GE  JAF1339BDSK
102   Eth1/33        Active     1    N2K-C2232P-10GE  JAS12334ABC
102   Eth1/34        Active     2    N2K-C2232P-10GE  JAS12334ABC
102   Eth1/35        Active     3    N2K-C2232P-10GE  JAS12334ABC
102   Eth1/36        Active     4    N2K-C2232P-10GE  JAS12334ABC
101   Eth1/37        Active     5    N2K-C2232P-10GE  JAF1333ADDD
101   Eth1/38        Active     6    N2K-C2232P-10GE  JAF1333ADDD
101   Eth1/39        Active     7    N2K-C2232P-10GE  JAF1333ADDD
101   Eth1/40        Active     8    N2K-C2232P-10GE  JAF1333ADDD
```

次に、親スイッチ インターフェイスに接続されている SPF+ トランシーバのファブリック エクステンダのアップリンクの SFP+ トランシーバおよび Diagnostic Optical Monitoring（DOM）情報を表示する例を示します。

```
switch# show interface ethernet 1/40 transceiver
Ethernet1/40
    sfp is present
    name is CISCO-MOLEX INC
    part number is 74752-9026
    revision is A0
    serial number is MOC13321057
    nominal bitrate is 12000 MBits/sec
    Link length supported for copper is 3 m(s)
    cisco id is --
    cisco extended id number is 4
```

次に、ファブリック エクステンダのアップリンク ポートに接続されている SPF+ トランシーバのファブリック エクステンダのアップリンクの SFP+ トランシーバおよび DOM 情報を表示する例を示します。

```
switch# show interface ethernet 1/40 transceiver fex-fabric
Ethernet1/40
    sfp is present
    name is CISCO-MOLEX INC
    part number is 74752-9026
    revision is A0
    serial number is MOC13321057
    nominal bitrate is 12000 MBits/sec
    Link length supported for 50/125mm fiber is 0 m(s)
    Link length supported for 62.5/125mm fiber is 0 m(s)
    cisco id is --
    cisco extended id number is 4
```

シャーシ管理情報の確認

ファブリックエクステンダを管理するためにスイッチ スーパーバイザで使用される設定情報を表示するには、次のいずれかの作業を実行します。

コマンドまたはアクション	目的
show diagnostic result fex *FEX-number*	ファブリック エクステンダの診断テストの結果を表示します。
show environment fex {**all** | *FEX-number*} [**temperature** | **power** | **fan**]	環境センサーのステータスを表示します。
show inventory fex *FEX-number*	ファブリック エクステンダのコンポーネント情報を表示します。
show module fex [*FEX-number*]	ファブリック エクステンダのモジュール情報を表示します。
show sprom fex *FEX-number* {**all** | **backplane** | **powersupply** *ps-num*} | **all**	ファブリック エクステンダのシリアル PROM（SPROM）の内容を表示します。

シャーシ管理の設定例

次に、接続されているすべてのファブリック エクステンダ装置のモジュール情報を表示する例を示します。

```
switch# show module fex
FEX Mod Ports Card Type                          Model               Status.
--- --- ----- ---------------------------------- ------------------ -----------
100 1   48    Fabric Extender 48x1GE + 4x10G Mod N2K-C2248TP-1GE    present
101 1   32    Fabric Extender 32x10GE + 8x10G Mo N2K-C2232P-10GE    present
102 1   32    Fabric Extender 32x10GE + 8x10G Mo N2K-C2232P-10GE    present

FEX Mod Sw              Hw      World-Wide-Name(s) (WWN)
--- --- --------------  ------  -----------------------------------------------
100 1   4.2(1)N1(1)     0.103   --
101 1   4.2(1)N1(1)     1.0     --
102 1   4.2(1)N1(1)     1.0     --

FEX Mod  MAC-Address(es)                         Serial-Num
--- ---  --------------------------------------  ----------
100 1    000d.ece3.2800 to 000d.ece3.282f        JAF1339BDSK
101 1    000d.ecca.73c0 to 000d.ecca.73df        JAF1333ADDD
102 1    000d.ecd6.bec0 to 000d.ecd6.bedf        JAS12334ABC
```

次に、特定のファブリック エクステンダのモジュール情報を表示する例を示します。

```
switch# show module fex 100
FEX Mod Ports Card Type                          Model               Status.
--- --- ----- ---------------------------------- ------------------ -----------
100 1   48    Fabric Extender 48x1GE + 4x10G Mod N2K-C2248TP-1GE    present

FEX Mod Sw              Hw      World-Wide-Name(s) (WWN)
--- --- --------------  ------  -----------------------------------------------
100 1   4.2(1)N1(1)     0.103   --

FEX Mod  MAC-Address(es)                         Serial-Num
--- ---  --------------------------------------  ----------
100 1    000d.ece3.2800 to 000d.ece3.282f        JAF1339BDSK
```

次に、特定のファブリック エクステンダのコンポーネント情報を表示する例を示します。

```
switch# show inventory fex 101
NAME: "FEX 101 CHASSIS", DESCR: "N2K-C2248TP-1GE  CHASSIS"
```

```
PID: N2K-C2248TP-1GE   , VID: V00 , SN: SSI13380FSM

NAME: "FEX 101 Module 1", DESCR: "Fabric Extender Module: 48x1GE, 4x10GE Supervisor"
PID: N2K-C2248TP-1GE   , VID: V00 , SN: JAF1339BDSK

NAME: "FEX 101 Fan 1", DESCR: "Fabric Extender Fan module"
PID: N2K-C2248-FAN     , VID: N/A , SN: N/A

NAME: "FEX 101 Power Supply 2", DESCR: "Fabric Extender AC power supply"
PID: NXK-PAC-400W      , VID:  000, SN:      LIT13370QD6
```

次に、特定のファブリック エクステンダの診断テストの結果を表示する例を示します。

```
switch# show diagnostic result fex 101
FEX-101: 48x1GE/Supervisor  SerialNo   : JAF1339BDSK
Overall Diagnostic Result for FEX-101  : OK

Test results: (. = Pass, F = Fail, U = Untested)
TestPlatform:
0)             SPROM: ----------------> .
1)   Inband interface: ----------------> .
2)                Fan: ----------------> .
3)       Power Supply: ----------------> .
4) Temperature Sensor: ----------------> .

TestForwardingPorts:
Eth    1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Port ------------------------------------------------------------------------
       .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .

Eth   25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
Port ------------------------------------------------------------------------
       .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .

TestFabricPorts:
Fabric 1  2  3  4
Port ------------
       .  .  .  .
```

次に、特定のファブリック エクステンダの環境ステータスの結果を表示する例を示します。

```
switch# show environment fex 101


Temperature Fex 101:
----------------------------------------------------------------------
Module   Sensor     MajorThresh   MinorThres   CurTemp     Status
                    (Celsius)     (Celsius)    (Celsius)
----------------------------------------------------------------------
1        Outlet-1   60            50           33          ok
1        Outlet-2   60            50           38          ok
1        Inlet-1    50            40           35          ok
1        Die-1      100           90           44          ok


Fan Fex: 101:
-----------------------------------------------------
Fan             Model                Hw         Status
-----------------------------------------------------
Chassis         N2K-C2148-FAN        --         failure
PS-1            --                   --         absent
PS-2            NXK-PAC-400W         --         ok


Power Supply Fex 101:
--------------------------------------------------------------------------------
Voltage: 12 Volts
-------------------------------------------------------
PS  Model                Power       Power     Status
                         (Watts)     (Amp)
-------------------------------------------------------
```

```
1   --                          --         --     --
2   NXK-PAC-400W            4.32       0.36     ok


Mod Model                Power     Power       Power     Power       Status
                         Requested Requested   Allocated Allocated
                         (Watts)   (Amp)       (Watts)   (Amp)
--- -------------------  -------   ----------  --------- ----------  ----------
1    N2K-C2248TP-1GE     0.00      0.00        0.00      0.00        powered-up


Power Usage Summary:
--------------------
Power Supply redundancy mode:                 redundant

Total Power Capacity                                4.32 W

Power reserved for Supervisor(s)                    0.00 W
Power currently used by Modules                     0.00 W

                                                  -------------
Total Power Available                               4.32 W
                                                  -------------
```

次に、特定のファブリック エクステンダの SPROM を表示する例を示します。

```
switch# show sprom fex 101 all
DISPLAY FEX 101 SUP sprom contents
Common block:
 Block Signature : 0xabab
 Block Version   : 3
 Block Length    : 160
 Block Checksum  : 0x1a1e
 EEPROM Size     : 65535
 Block Count     : 3
 FRU Major Type  : 0x6002
 FRU Minor Type  : 0x0
 OEM String      : Cisco Systems, Inc.
 Product Number  : N2K-C2248TP-1GE
 Serial Number   : JAF1339BDSK
 Part Number     : 73-12748-01
 Part Revision   : 11
 Mfg Deviation   : 0
 H/W Version     : 0.103
 Mfg Bits        : 0
 Engineer Use    : 0
 snmpOID         : 9.12.3.1.9.78.3.0
 Power Consump   : 1666
 RMA Code        : 0-0-0-0
 CLEI Code       : XXXXXXXXXTBDV00
 VID             : V00
Supervisor Module specific block:
 Block Signature : 0x6002
 Block Version   : 2
 Block Length    : 103
 Block Checksum  : 0x2686
 Feature Bits    : 0x0
 HW Changes Bits : 0x0
 Card Index      : 11016
 MAC Addresses   : 00-00-00-00-00-00
 Number of MACs  : 0
 Number of EPLD  : 0
 Port Type-Num   : 1-48;2-4
 Sensor #1       : 60,50
 Sensor #2       : 60,50
 Sensor #3       : -128,-128
 Sensor #4       : -128,-128
 Sensor #5       : 50,40
 Sensor #6       : -128,-128
 Sensor #7       : -128,-128
 Sensor #8       : -128,-128
 Max Connector Power: 4000
 Cooling Requirement: 65
```

```
 Ambient Temperature: 40

DISPLAY FEX 101 backplane sprom contents:
Common block:
 Block Signature : 0xabab
 Block Version   : 3
 Block Length    : 160
 Block Checksum  : 0x1947
 EEPROM Size     : 65535
 Block Count     : 5
 FRU Major Type  : 0x6001
 FRU Minor Type  : 0x0
 OEM String      : Cisco Systems, Inc.
 Product Number  : N2K-C2248TP-1GE
 Serial Number   : SSI13380FSM
 Part Number     : 68-3601-01
 Part Revision   : 03
 Mfg Deviation   : 0
 H/W Version     : 1.0
 Mfg Bits        : 0
 Engineer Use    : 0
 snmpOID         : 9.12.3.1.3.914.0.0
 Power Consump   : 0
 RMA Code        : 0-0-0-0
 CLEI Code       : XXXXXXXXXTDBV00
 VID             : V00
Chassis specific block:
 Block Signature : 0x6001
 Block Version   : 3
 Block Length    : 39
 Block Checksum  : 0x2cf
 Feature Bits    : 0x0
 HW Changes Bits : 0x0
 Stackmib OID    : 0
 MAC Addresses   : 00-0d-ec-e3-28-00
 Number of MACs  : 64
 OEM Enterprise  : 0
 OEM MIB Offset  : 0
 MAX Connector Power: 0
WWN software-module specific block:
 Block Signature : 0x6005
 Block Version   : 1
 Block Length    : 0
 Block Checksum  : 0x66
wwn usage bits:
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
```

```
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
 00 00
License software-module specific block:
 Block Signature : 0x6006
 Block Version   : 1
 Block Length    : 16
 Block Checksum  : 0x86f
lic usage bits:
 ff ff ff ff ff ff ff ff

DISPLAY FEX 101 power-supply 2 sprom contents:
Common block:
 Block Signature : 0xabab
 Block Version   : 3
 Block Length    : 160
 Block Checksum  : 0x1673
 EEPROM Size     : 65535
 Block Count     : 2
 FRU Major Type  : 0xab01
 FRU Minor Type  : 0x0
 OEM String      : Cisco Systems Inc   NXK-PAC-400W
 Product Number  : NXK-PAC-400W
 Serial Number   :      LIT13370QD6
 Part Number     :          341
 Part Revision   : -037
 CLEI Code       : 5-01     01  000
 VID             :  000
 snmpOID         : 12336.12336.12336.12336.12336.12336.12374.12336
 H/W Version     : 43777.2
 Current         : 36
 RMA Code        : 200-32-32-32
Power supply specific block:
 Block Signature : 0x0
 Block Version   : 0
 Block Length    : 0
 Block Checksum  : 0x0
 Feature Bits    : 0x0
 Current 110v    : 36
 Current 220v    : 36
 Stackmib OID    : 0
```

Cisco Nexus N2248TP-E ファブリック エクステンダの設定

Cisco Nexus 2248TP-E ファブリック エクステンダは、次のものを設定するための追加コマンドを含む、Cisco Nexus 2248TP ファブリック エクステンダのすべての CLI コマンドをサポートします。

- 共有バッファ（FEX グローバル レベル）
- 入力方向の Queue-Limit（FEX グローバル レベルおよびインターフェイス レベル）
- 出力方向の Queue-Limit（FEX グローバル レベルおよびインターフェイス レベル）
- FEX とスイッチ間の 3000 m の距離での非ドロップ クラス（FEX グローバル レベル）

共有バッファの設定

共有バッファを設定する際の注意事項を次に示します。

- 共有バッファの設定は、FEX グローバル レベルで行われます。

- 使用可能バッファの合計サイズは 32MB であり、入力と出力の両方向で共有されます。
- 共有バッファのデフォルト サイズは、2539 2KB です。

  ただし、イーサネット ベースの pause no-drop クラスを設定した場合、共有バッファのサイズは 10800 KB に変更されます。 この変更は、pause no-drop クラスをサポートする専用バッファを拡大するために必要です。 pause no-drop クラスでは、共有プールからのバッファ スペースは使用されません。

（注） これらのコマンドを実行すると、すべてのポートでトラフィックの中断が発生する可能性があります。

手順の概要

1. **configure terminal**
2. **fex** *chassis_id*
3. **hardware N2248TP-E shared-buffer-size** *buffer-size*

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**fex** *chassis_id*
	
	例：
	`switch(config)# fex 100`
	`switch(config-fex)#`
		指定された FEX の設定モードを開始します。
		chassis_id 値の範囲は 100 ～ 199 です。

ステップ 3	**hardware N2248TP-E shared-buffer-size** *buffer-size* 例： `switch(config-fex)# hardware N2248TP-E shared-buffer-size 25000`	共有バッファ サイズ（KB）を指定します。 *buffer-size* 値の範囲は 10800 KB ～ 2539 KB です。 （注） **hardware N2248TP-E shared-buffer-size** コマンドでは、デフォルトの共有バッファ サイズ 25392 KB を指定します。

例：

```
switch# configure terminal
switch(config)# fex 100
switch(config-fex)# hardware N2248TP-E shared-buffer-size 25000
switch(config-fex)#
```

グローバル レベルでの Queue-Limit の設定

Queue-Limit を設定する際の注意事項を次に示します。

- tx キュー制限は、出力（n2h）方向で各キューに使用されるバッファ サイズを指定します。
- rx キュー制限は、入力（h2n）方向で各キューに使用されるバッファ サイズを指定します。
- FEX アップリンクで一時的な輻輳が発生した場合、入力キュー制限を調整できます。
- バースト吸収を改善するために、あるいは多対 1 のトラフィック パターンがある場合、出力キュー制限を調整できます。
- tx queue-limit をディセーブルにすると、出力ポートで共有バッファ全体を使用できます。

手順の概要

1. **configure terminal**
2. **fex** *chassis_id*
3. **hardware N2248TP-E queue-limit** *queue-limit* **tx|rx**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**fex** *chassis_id*
	
	例：
	`switch(config)# fex 100`
	`switch(config)#`
		指定された FEX の設定モードを開始します。
		chassis_id 値の範囲は 100 ～ 199 です。

ステップ 3	**hardware N2248TP-E queue-limit** *queue-limit* **tx|rx** 例： `switch(config-fex)# hardware N2248TP-E queue-limit 83000 tx`	FEX で出力（tx）また入力（rx）のキュー テール ドロップしきい値レベルを制御します。 • tx（出力）のデフォルトの queue-limit は 4 MB です。 （注） **hardware N2248TP-E queue-limit** コマンドでは、デフォルトの tx queue-limit を指定します。 • rx（入力）のデフォルトの queue-limit は 1 MB です。 （注） **hardware N2248TP-E queue-limit rx** コマンドでは、デフォルトの rx queue-limit を指定します。

例：

```
switch# configure terminal
switch(config)# fex 100
switch(config-fex)# hardware N2248TP-E queue-limit 83000 tx
switch(config-fex)#
```

ポート レベルでの Queue-Limit の設定

ポート レベルで queue-limit を設定することで、グローバル レベル設定を上書きできます。

また、ポート レベルで queue-limit をディセーブルにすることもできます。

手順の概要

1. **configure terminal**
2. **interface ethernet** *chassis_id / slot/port*
3. **hardware N2248TP-E queue-limit** *queue-limit* **tx|rx**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**interface ethernet** *chassis_id / slot/port* 例： `switch(config)# interface ethernet 100/1/1`	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	**hardware N2248TP-E queue-limit** *queue-limit* **tx|rx** 例： `switch(config-if)# hardware N2248TP-E queue-limit 83000 tx`	FEX で出力（tx）また入力（rx）のキュー テール ドロップしきい値レベルを制御します。 • tx（出力）のデフォルトの queue-limit は 4 MB です。 • rx（入力）のデフォルトの queue-limit は 1 MB です。

例：

```
switch# configure terminal
switch(config)# interface ethernet 100/1/1
switch(config-if)# hardware N2248TP-E queue-limit 83000 tx
switch(config-if)#
```

アップリンク距離の設定

Cisco Nexus N2248TP-E FEX は、FEX とスイッチ間で最大 3000 m まで pause no-drop クラスをサポートします。

FEX とスイッチ間のデフォルトのケーブル長は 300 m です。

（注） pause no-drop クラスを設定しない場合、アップリンク距離の設定は無効です。

手順の概要

1. **configure terminal**
2. **fex** *chassis_id*
3. **hardware N2248TP-E uplink-pause-no-drop distance** *distance-value*

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**fex** *chassis_id*
	
	例：
	`switch(config)# fex 100`
	`switch(config-fex)#`
		指定された FEX の設定モードを開始します。
		chassis_id 値の範囲は 100 ～ 199 です。

ステップ 3	**hardware N2248TP-E uplink-pause-no-drop distance** *distance-value* 例： `switch(config-fex)# hardware N2248TP-E uplink-pause-no-drop distance 3000`	FEX とスイッチ間の no-drop 距離を指定します。 最大距離は 3000 m です。 （注） **hardware N2248TP-E uplink-pause-no-drop distance** コマンドでは、デフォルトのケーブル長 300 m を指定します。

例：

```
switch# configure terminal
switch(config)# fex 100
switch(config-fex)# hardware N2248TP-E uplink-pause-no-drop distance 3000
switch(config-fex)#
```

第 21 章

VM-FEX の設定

この章の内容は、次のとおりです。

VM-FEX について

VM-FEX の概要

（先行標準）IEEE 802.1Qbh ポート エクステンダ テクノロジーに基づいて、Cisco Virtual Machine Fabric Extender（VM-FEX）はファブリックをスイッチ シャーシから仮想マシン（VM）にまで拡張します。 各 VM はネットワーク アダプタ vNIC に関連付けられ、次に親スイッチの仮想イーサネット（vEthernet または vEth）ポートに関連付けられます。 この専用仮想インターフェイスは、物理インターフェイスと同じ方法で管理、監視、およびスパニングすることができます。 ハイパーバイザーのローカル スイッチングは排除され、すべてのスイッチングは物理スイッチによって実行されます。

VM-FEX のコンポーネント

サーバ

VM-FEX は、ハイパーバイザとして VMware 仮想化環境 Cisco UCS C シリーズ ラックマウント サーバによってサポートされます。

サーバの設定は、Cisco Integrated Management Controller（CIMC）を使用して実行され、GUI と CLI インターフェイスの両方が提供されます。ハイパーバイザおよび仮想化サービスの設定は、VMware vSphere クライアントを使用して実行されます。

CIMC および VM-FEX 設定の詳細については、次のマニュアルを参照してください。

- 『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』
- 『*Cisco UCS Manager VM-FEX for VMware GUI Configuration Guide*』

仮想インターフェイス カード アダプタ

VM-FEX は、仮想化されたスタティック インターフェイスまたはダイナミック インターフェイスをサポートするデュアルポート 10 ギガビット イーサネット PCIe アダプタである、Cisco UCS P81E 仮想インターフェイス カード(VIC)によりサポートされています。これには、128 までの仮想ネットワーク インターフェイス カード（vNIC）が含まれます。

VIC とその vNIC の設定は、Cisco UCS C シリーズ サーバの CIMC インターフェイスを使用して実行されます。

FEX

サーバの物理ポートは、スイッチに、またはスイッチに接続されているファブリック エクステンダ（FEX）に直接接続することができます。 VM-FEX は、Cisco Nexus 2000 シリーズ ファブリック エクステンダによってサポートされます。

スイッチ

VM-FEX は、Cisco NX-OS Release 5.1(3)N1(1) 以降のリリースを稼働している Cisco Nexus 5500 プラットフォーム によってサポートされます。 単一スイッチ シャーシは、VM-FEX に接続することができますが、一般的なアプリケーションでは、仮想ポート チャネル（vPC）ドメインとして展開されるスイッチのペアが使用されます。

スイッチでは、vEthernet インターフェイスは vNIC を表します。 ネットワーク管理者が実行するすべての操作は、vEthernet インターフェイスで実行されます。

VM-FEX の用語

VM-FEX のコンポーネントおよびインターフェイスの説明では、次の用語が使用されます。

仮想イーサネット インターフェイス

仮想イーサネット インターフェイス（vEthernet または vEth）は、仮想マシンの vNIC に接続されるスイッチ ポートを表します。 従来のスイッチ インターフェイスとは異なり、vEth インターフェイスの名前は、ポートが関連付けられているモジュールを表しません。 従来のスイッチ ポートが GigX/Y として指定されている場合、X はモジュール番号で、Y はモジュールのポート番号です。vEth インターフェイスは vEthY として指定されます。 この表記法を使用すると、VM が別の物理サーバに移行する際にインターフェイスを同じ名前のままにすることができます。

ダイナミック インターフェイス

ダイナミック インターフェイスとは、アダプタとスイッチの通信結果により自動的に設定される vEthernet インターフェイスです。 ダイナミック インターフェイスのプロビジョニング モデルは、vEthernet ポート プロファイルのスイッチの設定で構成されており、ポート グループとしてネットワーク アダプタに伝播され、その後、ポート グループが vNIC に関連付けられます。 ポート プロファイルは、ネットワーク管理者によってスイッチに作成される一方、vNIC との関連付けがサーバ管理者によってアダプタで実行されます。

スタティック インターフェイス

スタティックインターフェイスは、スイッチとアダプタに手動で設定されます。スタティック仮想アダプタは、vNIC または仮想ホストバスアダプタ（vHBA）にすることができます。スティック インターフェイスは、vEthernet、またはスタティック vEthernet インターフェイスにバインドされている仮想ファイバチャネル（vFC）インターフェイスにすることができます。

スタティック vEthernet を作成する 1 つの方法では、ネットワーク管理者はチャネル番号（VN-Tag または先行標準の IEEE 802.1BR タグ番号）を vEthernet に割り当てます。 サーバ管理者は、アダプタの vNIC を必ず同じチャネル番号で定義します。

別の方法では、ネットワーク管理者は、仮想スイッチング インターフェイス（VSI）MAC アドレスと DVPort ID を使用して vEthernet を設定することで、スタティック浮動 vEthernet を作成できます。

浮動 vEthernet インターフェイス

ハイパーバイザ環境では、ネットワーク アダプタの各 vNIC は 1 つの仮想マシン（VM）に関連付けられます。 VM は、物理サーバ間の移行が可能です。 VM および仮想ネットワーク リンクとともに移行する仮想インターフェイスは、浮動 vEthernet インターフェイスと呼ばれます。

固定 vEthernet インターフェイス

固定 vEthernet インターフェイスとは、物理インターフェイス間の移行をサポートしない仮想インターフェイスです。 固定 vEthernet（スタティックまたはダイナミック）の場合、管理者はいつでも設定を変更できます。 vEthernet インターフェイス番号とチャネル番号のバインディングは、管理者がそれを変更しない限り変化しません。

VM-FEX のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	各 Nexus 5500 シリーズ スイッチ シャーシに VM-FEX ライセンスが必要です。 ライセンス パッケージ名は VMFEX_ FEATURE_PKG であり、PID は N55-VMFEXK9 です。 ライセンス月機能を初めて設定すると、120 日間の猶予期間が始まります。 Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS Licensing Guide*』を参照してください。

VM-FEX のデフォルト設定

次の表に、VM-FEX に関連するパラメータのデフォルト設定を示します。

パラメータ	デフォルト
仮想化フィーチャ セット	ディセーブル
FEX	ディセーブル
VM-FEX	ディセーブル
LLDP	イネーブル
vPC	ディセーブル
svs vethernet auto-setup	イネーブル
FCoE	ディセーブル

VM-FEX の設定

VM-FEX 設定手順の概要

次の手順では、スイッチと VM をホストしているサーバ間で VM-FEX を設定するために必要な一連の手順について簡単に説明します。 スイッチで実行する手順については、このマニュアルに記

載されています。サーバまたはVMware vCenterで実行する手順については、サーバおよびvCenterのマニュアルを参照してください。

ステップ 1 サーバ：VIC アダプタで vNIC を作成します。

a) ホストからアップリンクとして使用する 2 つのスタティック vNIC を作成します。
b) 最大 112 個の VM-FEX インターフェイスを作成します。
c) サーバをリブートします。

ステップ 2 スイッチ: VM-FEX および他の必須サービスをイネーブルにします。
VM-FEX に必要な機能のイネーブル化, （356 ページ） を参照してください。

ステップ 3 スイッチ：2 つのスタティック vEthernet インターフェイスを設定し、それらを物理ポートおよびチャネルにバインドします。
固定スタティック インターフェイスの設定, （358 ページ） を参照してください。

ステップ 4 スイッチ：VM に関連付けるポート プロファイルを定義します。
ダイナミック インターフェイスのポート プロファイルの設定, （363 ページ） を参照してください。

ステップ 5 スイッチ：2 つのスタティック vEthernet インターフェイスがアクティブで、スイッチの vEthernet インターフェイスに関連付けられていることを確認します。
仮想インターフェイスのステータスの確認, （368 ページ） を参照してください。

ステップ 6 スイッチおよび vCenter：XML 証明書をスイッチから vCenter にインストールします。

a) スイッチ：設定モードで **feature http** コマンドを使用して HTTP をイネーブルにします。
b) Web ブラウザから、スイッチの IP アドレスにアクセスして表示された XML 証明書をダウンロードします。
c) スイッチ：設定モードで **no feature http** コマンドを使用して HTTP をディセーブルにします。
d) vCenter：XML 証明書プラグインをインストールします。

ステップ 7 スイッチ：vPC をイネーブルにし、vPC システムを分散仮想スイッチ（DVS）として vCenter に登録します。
vCenter Server への SVS 接続の設定, （364 ページ） を参照してください。

ステップ 8 vCenter：vCenter でデータセンターを作成します。

ステップ 9 スイッチ：vCenter への SVS 接続をアクティブにして確認します。
vCenter Server への SVS 接続のアクティブ化, （367 ページ）および vCenter Server への接続の確認, （370 ページ）を参照してください。

ステップ 10 vCenter：ポート プロファイル（ポート グループ）が vCenter に伝播されていることを確認します。

ステップ 11 サーバ：リソースを DVS に追加します。

a) ESX ホストを DVS に追加します。
b) スタティック vNIC をアップリンクとして DVS に追加します。
c) VM を、スイッチによって定義されているポート グループに関連付けます。

d) VM をアクティブにします。

ステップ 12 スイッチ：ダイナミック vNIC がアクティブであり、スイッチの vEthernet インターフェイスに接続されていることを確認します。
仮想インターフェイスのステータスの確認, （368 ページ） を参照してください。

ステップ 13 サーバ：インターフェイスがアクティブであり、VM に割り当てられていることを確認します。

ステップ 14 vCenter：ダイナミック vNICs がアクティブであることを確認します。

VM-FEX に必要な機能のイネーブル化

手順の概要

1. **configure terminal**
2. **install feature-set virtualization**
3. **feature-set virtualization**
4. **feature fex**
5. **feature vmfex**
6. **feature vpc**
7. （任意） **vethernet auto-create**
8. （任意） **feature fcoe**
9. （任意） **end**
10. （任意） **copy running-config startup-config**
11. （任意） **reload**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**install feature-set virtualization** 例： `switch(config)# install feature-set virtualization`	仮想化フィーチャ セットをスイッチにインストールします。

	コマンドまたはアクション	目的
ステップ 3	**feature-set virtualization** 例： `switch(config)# feature-set virtualization`	スイッチで仮想化フィーチャ セットをイネーブルにします。 このフィーチャ セットにより、スタティック vEthernet インターフェイスが使用できるようなります。
ステップ 4	**feature fex** 例： `switch(config)# feature fex`	スイッチで FEX 機能をイネーブルにします。
ステップ 5	**feature vmfex** 例： `switch(config)# feature vmfex`	スイッチで VM-FEX 機能をイネーブルにします。 このフィーチャ セットにより、ダイナミック vEthernet インターフェイスが使用できるようになります。
ステップ 6	**feature vpc** 例： `switch(config)# feature vpc`	スイッチで仮想ポート チャネル（vPC）をイネーブルにします。
ステップ 7	**vethernet auto-create** 例： `switch(config)# vethernet auto-create`	（任意） 仮想イーサネット インターフェイスの自動作成をグローバルにイネーブルにします。 固定 vEthernet インターフェイスが静的に設定されている場合、この機能は不要です。
ステップ 8	**feature fcoe** 例： `switch(config)# feature fcoe`	（任意） スイッチで Fibre Channel over Ethernet（FCoE）をイネーブルにします。

ステップ 9	**end**
	
	例：
	`switch(config-mvr)# end`
	`switch#`
		（任意）
		特権 EXEC モードに戻ります。

ステップ 10	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
ステップ 11	**reload** 例： `switch# reload`	（任意） スイッチをリロードします。

次に、VM-FEX に必要な機能をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# install feature-set virtualization
switch(config)# feature-set virtualization
switch(config)# feature fex
switch(config)# feature vmfex
switch(config)# feature vpc
switch(config)# vethernet auto-create
switch(config)# feature fcoe
switch(config)# end
switch# copy running-config startup-config
switch# reload
```

固定スタティック インターフェイスの設定

次の手順では、2 つの物理インターフェイスを設定し、2 つの仮想インターフェイスを物理インターフェイスにバインドして、固定スタティック vEthernet インターフェイスを作成します。固定スタティック インターフェイスの設定に関する詳細については、『*Cisco Nexus 5000 NX-OS Adapter-FEX Configuration Guide*』を参照してください。

冗長スイッチを使用して、プライマリとセカンダリの両方のスイッチでこの手順を同じ設定で実行します。

はじめる前に

- VM-FEX および他の必須サービスをスイッチでイネーブルにする必要があります。
- ホスト サーバにインストールされている VIC アダプタで 2 つのスタティック vNIC を設定する必要があります。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **shutdown**
4. **switchport mode vntag**
5. **interface ethernet** *slot/port*
6. **shutdown**
7. **switchport mode vntag**
8. **interface vethernet** *interface-number*
9. **bind interface ethernet** *slot/port* **channel** *channel-number*
10. **no shutdown**
11. **interface vethernet** *interface-number*
12. **bind interface ethernet** *slot/port* **channel** *channel-number*
13. **no shutdown**
14. **interface vethernet** *interface-number*
15. **bind interface ethernet** *slot/port* **channel** *channel-number*
16. **no shutdown**
17. **interface vethernet** *interface-number*
18. **bind interface ethernet** *slot/port* **channel** *channel-number*
19. **no shutdown**
20. **interface ethernet** *slot/port*
21. **no shutdown**
22. **interface ethernet** *slot/port*
23. **no shutdown**
24. 冗長スイッチを使用して、セカンダリ スイッチでこの手順を同じ設定で繰り返します。

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**interface ethernet** *slot/port*
	
	例：
	`switch(config)# interface ethernet1/17`
	`switch(config-if)#`
		最初のイーサネット ポートの設定モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**shutdown** 例： `switch(config-if)# shutdown`	インターフェイスでローカル トラフィックをディセーブルにします。 （注） VN-Tag モードをイネーブルにする前にインターフェイスをシャットダウンすると、固定 vEthernet インターフェイスのダイナミック作成は行われません。
ステップ 4	**switchport mode vntag** 例： `switch(config-if)# switchport mode vntag`	インターフェイスでポート エクステンダのサポートをイネーブルにします。

ステップ 5	**interface ethernet** *slot/port*
	
	例：
	`switch(config)# interface ethernet1/18`
	`switch(config-if)#`
		2 番目のイーサネット ポートの設定モードを開始します。

ステップ 6	**shutdown** 例： `switch(config-if)# shutdown`	インターフェイスでローカル トラフィックをディセーブルにします。
ステップ 7	**switchport mode vntag** 例： `switch(config-if)# switchport mode vntag`	インターフェイスでポート エクステンダのサポートをイネーブルにします。

ステップ 8	**interface vethernet** *interface-number*
	
	例：
	`switch(config-if)# interface vethernet 1`
	`switch(config-if)#`
		最初のイーサネット ポートの 1 番目の仮想インターフェイスの設定モードを開始します。

ステップ 9	**bind interface ethernet** *slot/port* **channel** *channel-number* 例： `switch(config-if)# bind interface ethernet 1/17 channel 10`	仮想インターフェイスを物理インターフェイスと指定されたポート チャネルにバインドします。 （注） 仮想インターフェイスのポート チャネル数は、vNIC で設定されているポート チャネル数と一致している必要があります。
ステップ 10	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスでローカル トラフィックをイネーブルにします。

ステップ 11	**interface vethernet** *interface-number*
	
	例：
	`switch(config-if)# interface vethernet 3`
	`switch(config-if)#`
		最初のイーサネット ポートの 2 番目の仮想インターフェイスの設定モードを開始します。

	コマンドまたはアクション	目的
ステップ 12	**bind interface ethernet** *slot/port* **channel** *channel-number* 例： `switch(config-if)# bind interface ethernet 1/17 channel 11`	仮想インターフェイスを物理インターフェイスと指定されたポート チャネルにバインドします。
ステップ 13	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスでローカル トラフィックをイネーブルにします。

ステップ 14	**interface vethernet** *interface-number*
	
	例：
	`switch(config-if)# interface vethernet 2`
	`switch(config-if)#`
		2 番目のイーサネット ポートの 1 番目の仮想インターフェイスの設定モードを開始します。

ステップ 15	**bind interface ethernet** *slot/port* **channel** *channel-number* 例： `switch(config-if)# bind interface ethernet 1/18 channel 10`	仮想インターフェイスを物理インターフェイスと指定されたポート チャネルにバインドします。
ステップ 16	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスでローカル トラフィックをイネーブルにします。

ステップ 17	**interface vethernet** *interface-number*
	
	例：
	`switch(config-if)# interface vethernet 4`
	`switch(config-if)#`
		2 番目のイーサネット ポートの 2 番目の仮想インターフェイスの設定モードを開始します。

ステップ 18	**bind interface ethernet** *slot/port* **channel** *channel-number* 例： `switch(config-if)# bind interface ethernet 1/18 channel 11`	仮想インターフェイスを物理インターフェイスと指定されたポート チャネルにバインドします。
ステップ 19	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスでローカル トラフィックをイネーブルにします。

ステップ 20	**interface ethernet** *slot/port*
	
	例：
	`switch(config)# interface ethernet1/17`
	`switch(config-if)#`
		最初のイーサネット ポートの設定モードを開始します。

	コマンドまたはアクション	目的
ステップ 21	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスでローカル トラフィックをイネーブルにします。

ステップ 22	**interface ethernet** *slot/port*
	
	例：
	`switch(config)# interface ethernet1/18`
	`switch(config-if)#`
		2 番目のイーサネット ポートの設定モードを開始します。

ステップ 23	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスでローカル トラフィックをイネーブルにします。
ステップ 24	冗長スイッチを使用して、セカンダリ スイッチでこの手順を同じ設定で繰り返します。	

次に、2つの物理インターフェイスを設定し、2つの仮想インターフェイスを各物理インターフェイスにバインドして、インターフェイスをイネーブルにする例を示します。

```
switch-1# configure terminal
switch-1(config)# interface ethernet 1/17
switch-1(config-if)# shutdown
switch-1(config-if)# switchport mode vntag
switch-1(config-if)# interface ethernet 1/18
switch-1(config-if)# shutdown
switch-1(config-if)# switchport mode vntag

switch-1(config-if)# interface vethernet 1
switch-1(config-if)# bind interface ethernet 1/17 channel 10
switch-1(config-if)# no shutdown
switch-1(config-if)# interface vethernet 3
switch-1(config-if)# bind interface ethernet 1/17 channel 11
switch-1(config-if)# no shutdown

switch-1(config-if)# interface vethernet 2
switch-1(config-if)# bind interface ethernet 1/18 channel 10
switch-1(config-if)# no shutdown
switch-1(config-if)# interface vethernet 4
switch-1(config-if)# bind interface ethernet 1/18 channel 11
switch-1(config-if)# no shutdown

switch-1(config-if)# interface ethernet 1/17
switch-1(config-if)# no shutdown
switch-1(config-if)# interface ethernet 1/18
switch-1(config-if)# no shutdown

switch-1(config-if)#
```

次の作業

ホスト サーバでスタティック サーバとスタティック vNIC 間の接続ステータスを確認します。

ダイナミック インターフェイスのポート プロファイルの設定

次の手順では、ダイナミック仮想インターフェイスのポート プロファイルを設定します。 このポート プロファイルは、ポート グループとして VMware vCenter 分散仮想スイッチ（DVS）にエクスポートされます。

冗長スイッチを使用して、プライマリとセカンダリの両方のスイッチでこの手順を同じ設定で実行します。

はじめる前に

- ホスト サーバにインストールされている VIC アダプタでダイナミック vNIC を設定する必要があります。
- ポート プロファイルで指定されている VLAN を作成する必要があります。

手順の概要

1. **configure terminal**
2. **port-profile type vethernet** *profilename*
3. （任意） **switchport mode access**
4. （任意） **switchport access vlan** *vlan-id*
5. **dvs-name** {**all** | *name*}
6. （任意） **port-binding dynamic**
7. **state enabled**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**port-profile type vethernet** *profilename*
	
	例：
	`switch(config)# port-profile type vethernet vm-fex-vlan-60`
	`switch(config-port-prof)#`
		指定されたポート プロファイルの設定モードを開始し、必要に応じてそのプロファイルを作成します。

ステップ 3	**switchport mode access** 例： `switch(config-port-prof)# switchport mode access`	（任意） アクセス モードになるようにインターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 4	**switchport access vlan** *vlan-id* 例： `switch(config-port-prof)# switchport access vlan 60`	（任意） インターフェイスがアクセス モードのときに VLAN を設定します。
ステップ 5	**dvs-name** {**all** | *name*} 例： `switch(config-port-prof)# dvs-name all`	ポートプロファイルがポート グループとしてエクスポートされる vCenter DVS を指定します。 キーワード **all** を使用すると、ポート プロファイルが vCenter のすべての DVS にエクスポートされます。
ステップ 6	**port-binding dynamic** 例： `switch(config-port-prof)# port-binding dynamic`	（任意） ダイナミック ポート バインディングを指定します。 ポートは、VM の電源がオンになると接続され、オフになると接続解除されます。 max-port 制限値が適用されます。 デフォルトは、スタティック ポート バインディングです。
ステップ 7	**state enabled** 例： `switch(config-port-prof)# state enabled`	ポート プロファイルをイネーブルにします。

次に、ダイナミック仮想インターフェイスのポート プロファイルを設定する例を示します。

```
switch-1# configure terminal
switch-1(config)# port-profile type vethernet vm-fex-vlan-60
switch-1(config-port-prof)# switchport mode access
switch-1(config-port-prof)# switchport access vlan 60
switch-1(config-port-prof)# dvs-name all
switch-1(config-port-prof)# port-binding dynamic
switch-1(config-port-prof)# state enabled
switch-1(config-port-prof)# end
switch-1#
```

vCenter Server への SVS 接続の設定

この手順では、スイッチから vCenter Server への安全な接続を設定します。

冗長スイッチを使用して、プライマリとセカンダリの両方のスイッチでこの手順を実行します。 通常の操作では、プライマリ スイッチのみが vCenter に接続され、プライマリに障害が発生した場合に限り、セカンダリ スイッチが接続されます。

手順の概要

1. **configure terminal**
2. **svs connection** *svs-name*
3. **protocol vmware-vim**
4. **vmware dvs datacenter-name** *dc-name*
5. **dvs-name** *dvs-name*
6. 次のいずれかを選択します。
   - **remote ip address** *ipv4-addr* [**port** *port-num*] [**vrf** {*vrf-name* | **default** | **management**}]
   - **remote hostname** *host-name* [**port** *port-num*] [**vrf** {*vrf-name* | **default** | **management**}]
7. **install certificate** {**bootflash:**[*//server/*] | **default**}
8. **extension-key:** *extn-ID*

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`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	**svs connection** *svs-name*
	
	例：
	`switch(config)# svs connection vCenter`
	`switch(config-svs-conn)#`
		スイッチから vCenter Server への SVS 接続の設定モードをイネーブルにして開始します。

ステップ 3	**protocol vmware-vim** 例： `switch(config-svs-conn)# protocol vmware-vim`	VMware インフラストラクチャ ソフトウェア開発キット（VI SDK）をイネーブルにし、クライアントと vCenter の通信を可能にします。
ステップ 4	**vmware dvs datacenter-name** *dc-name* 例： `switch(config-svs-conn)# vmware dvs datacenter-name DC1`	指定されたデータセンターで VMware 分散仮想スイッチ（DVS）を作成します。
ステップ 5	**dvs-name** *dvs-name* 例： `switch(config-svs-conn)# dvs-name Pod1`	vCenter Server で DVS の名前を設定します。
ステップ 6	次のいずれかを選択します。 • **remote ip address** *ipv4-addr* [**port** *port-num*] [**vrf** {*vrf-name* | **default** | **management**}]	vCenter Server のホスト名または IP アドレスを指定します。 任意でポート番号と VRF を指定します。

	コマンドまたはアクション	目的
	• **remote hostname** *host-name* [**port** *port-num*] [**vrf** {*vrf-name* | **default** | **management**}] 例： `switch(config-svs-conn)# remote ip address 192.0.20.125 port 80 vrf management`	
ステップ 7	**install certificate** {**bootflash:**[*//server/*] | **default**} 例： `switch(config-svs-conn)# install certificate default`	vCenter Server への接続に使用される証明書をインストールします。 *server* 引数には、その証明書をインストールするブート フラッシュ メモリの場所を指定します。 引数の値には、**module-1**、**sup-1**、**sup-active**、または **sup-local** を指定できます。
ステップ 8	**extension-key:** *extn-ID* 例： `switch(config-svs-conn)# extension-key: Cisco_Nexus_5500_1543569268`	vCenter Server への接続に使用される拡張キーを設定します。 （注） 冗長スイッチを使用して、プライマリ スイッチでのみこの手順を実行します。 このキーは、自動的にセカンダリ スイッチと同期されます。

次に、プライマリ スイッチとセカンダリ スイッチで SVS 接続を設定する例を示します。

```
switch-1# configure terminal
switch-1(config)# svs connection 2VC
switch-1(config-svs-conn)# protocol vmware-vim
switch-1(config-svs-conn)# vmware dvs datacenter-name DC1
switch-1(config-svs-conn)# dvs-name Pod1
switch-1(config-svs-conn)# remote ip address 192.0.20.125 port 80 vrf management
switch-1(config-svs-conn)# install certificate default
switch-1(config-svs-conn)# extension-key: Cisco_Nexus_5500_1543569268
switch-1(config-svs-conn)#

switch-2# configure terminal
switch-2(config)# svs connection 2VC
switch-2(config-svs-conn)# protocol vmware-vim
switch-2(config-svs-conn)# vmware dvs datacenter-name DC1
switch-2(config-svs-conn)# dvs-name Pod1
switch-2(config-svs-conn)# remote ip address 192.0.20.125 port 80 vrf management
switch-2(config-svs-conn)# install certificate default
switch-2(config-svs-conn)#
```

次の作業

プライマリ スイッチでのみ SVS 接続をアクティブにします。

vCenter Server への SVS 接続のアクティブ化

スイッチでこの手順を実行し、vCenter Server への接続をアクティブにします。

はじめる前に

- vCenter Server が実行され、到達可能であることが必要です。
- 拡張ファイルが vCenter Server に登録済みであることが必要です。
- スイッチで SVS 接続を設定する必要があります。

手順の概要

1. **configure terminal**
2. **svs connection** *svs-name*
3. [**no**] **connect**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**svs connection** *svs-name*
	
	例：
	`switch(config)# svs connection vCenter`
	`switch(config-svs-conn)#`
		スイッチから vCenter Server への SVS 接続の設定モードをイネーブルにして開始します。

ステップ 3	[**no**] **connect** 例： `switch(config-svs-conn)# connect`	vCenter Server との接続を開始します。 （注） 冗長スイッチを使用して、プライマリとセカンダリの両方のスイッチでこの手順を実行します。プライマリのみが接続されます。 スイッチが vCenter に接続され、DVS になります。

次に、vCenter Server に接続する例を示します。

```
switch-1# configure terminal
switch-1(config)# svs connection 2VC
switch-1(config-svs-conn)# connect
Note: Command execution in progress..please wait
switch-1(config-svs-conn)#
```

VM-FEX 設定の確認

仮想インターフェイスのステータスの確認

仮想インターフェイスのステータス情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show interface vethernet *interface-number* [**detail**]	仮想インターフェイスのステータスを表示します。各スタティック仮想インターフェイスでこの手順を実行し、各インターフェイスがアクティブであり、物理インターフェイスにバインドされていることを確認します。
show interface virtual status vm-fex	すべての浮動仮想インターフェイスに関する情報を表示します。
show interface virtual summary vm-fex	仮想イーサネットインターフェイスに関するサマリー情報を表示します。
show interface virtual status bound interface ethernet *port/slot*	バインドされたイーサネットインターフェイスの仮想インターフェイスに関する情報を表示します。
show interface virtual summary bound interface ethernet *port/slot*	バインドされたイーサネットインターフェイスの仮想インターフェイスに関するサマリー情報を表示します。

例

次に、スタティック インターフェイスに関するステータスおよび設定情報を表示する例を示します。

```
switch-1# show interface vethernet 1

Vethernet1 is up
Bound Interface is Ethernet1/17
Hardware is Virtual, address is 0005.73fc.24a0
Port mode is access
Speed is auto-speed
Duplex mode is auto
300 seconds input rate 0 bits/sec, 0 packets/sec
300 seconds output rate 0 bits/sec, 0 packets/sec
Rx
0 unicast packets  0 multicast packets  0 broadcast packets
0 input packets  0 bytes
0 input packet drops
Tx
0 unicast packets  0 multicast packets  0 broadcast packets
0 output packets  0 bytes
```

```
0 flood packets
0 output packet drops

switch-1# show interface vethernet 1 detail

vif_index: 20
--------------------------
  veth is bound to interface Ethernet1/17 (0x1a010000)
  priority: 0
  vntag: 16
  status: active
  channel id: 10
  registered mac info:
      vlan 0 - mac 00:00:00:00:00:00
      vlan 0 - mac 58:8d:09:0f:0b:3c
      vlan 0 - mac ff:ff:ff:ff:ff:ff

switch-1#
```

次に、すべての仮想インターフェイスに関するステータスおよびサマリー情報を表示する例を示します。

```
switch-1# show interface virtual status vm-fex

Interface VIF-index   Bound If      Chan  Vlan  Status     Mode     Vntag
-------------------------------------------------------------------------
Veth32769 VIF-37      Eth1/20       ----   101  Up         Active       7
Veth32770 VIF-39      Eth1/20       ----     1  Up         Active       8
Veth32771 VIF-41      Eth1/20       ----     1  Up         Standby      9
Veth32772 VIF-43      Eth1/20       ----     1  Up         Active      10
Veth32773 VIF-47      Eth1/20       ----     1  Up         Active      12
Veth32774 VIF-48      Eth1/20       ----     1  Up         Standby     13
Veth32775 VIF-49      Eth1/20       ----     1  Up         Active      14


switch-1# show interface virtual summary vm-fex

Veth       Bound      Channel/  Port                     Mac               VM
Interface  Interface  DV-Port   Profile                  Address           Name
-------------------------------------------------------------------------------------
Veth32769  Eth1/20    7415    Unused_Or_Quarantine_Veth  00:50:56:9b:33:a7  ESX145_1_RH55.
Veth32770  Eth1/20    7575    Unused_Or_Quarantine_Veth  00:50:56:9b:33:a8  ESX145_1_RH55.
Veth32771  Eth1/20    7576    Unused_Or_Quarantine_Veth  00:50:56:9b:33:a9  ESX145_1_RH55.
Veth32772  Eth1/20    7577    Unused_Or_Quarantine_Veth  00:50:56:9b:33:aa  ESX145_1_RH55.
Veth32773  Eth1/20    7578    Unused_Or_Quarantine_Veth  00:50:56:9b:33:ac  ESX145_1_RH55.
Veth32774  Eth1/20    7579    Unused_Or_Quarantine_Veth  00:50:56:9b:33:ad  ESX145_1_RH55.
Veth32775  Eth1/20    7580    Unused_Or_Quarantine_Veth  00:50:56:9b:33:ae  ESX145_1_RH55.
Veth32776  Eth1/20    7607    Unused_Or_Quarantine_Veth  00:50:56:9b:33:ab  ESX145_1_RH55.

switch-1#
```

次に、固定vEthernetインターフェイスに関するステータスおよびサマリー情報を表示する例を示します。

```
switch-1# show interface virtual status bound interface ethernet 1/20

Interface VIF-index   Bound If      Chan  Vlan  Status     Mode     Vntag
-------------------------------------------------------------------------
Veth32769 VIF-16      Eth1/20          1     1  Up         Active       2
Veth32770 VIF-17      Eth1/20          5     1  Up         Active      46
Veth32771 VIF-18      Eth1/20          8     1  Up         Active      49
Veth32772 VIF-19      Eth1/20          9     1  Up         Active      50
Veth32773 VIF-20      Eth1/20         11     1  Up         Active      52
Veth32774 VIF-21      Eth1/20         12     1  Up         Active      53
Veth32775 VIF-22      Eth1/20         13     1  Up         Active      54
Veth32776 VIF-23      Eth1/20         14     1  Up         Active      55
Veth32777 VIF-24      Eth1/20         15     1  Up         Active      56
Total 9 Veth interfaces
```

```
switch-1# show interface virtual summary bound interface ethernet 1/20

Veth       Bound        Channel/  Port        Mac               VM
Interface  Interface    DV-Port   Profile     Address           Name
--------------------------------------------------------------------------------
Veth32769  Eth1/20         1    sample
Veth32770  Eth1/20         5    sample
Veth32771  Eth1/20         8    sample
Veth32772  Eth1/20         9    sample
Veth32773  Eth1/20        11    sample
Veth32774  Eth1/20        12    sample
Veth32775  Eth1/20        13    sample
Veth32776  Eth1/20        14    sample
Veth32777  Eth1/20        15    sample
Total 9 Veth interfaces

switch-1#
```

vCenter Server への接続の確認

手順の概要

1. **configure terminal**
2. **show svs connections** [*svs-name*]

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**show svs connections** [*svs-name*] 例： `switch(config)# show svs connection`	現在の SVS 接続を表示します。

次に、SVS 接続の詳細を表示する例を示します。

```
switch-1# configure terminal
switch-1(config)# show svs connections

Local Info:
-----------
connection 2VC:
    ip address: 192.0.20.125
    remote port: 80
    vrf: management
    protocol: vmware-vim https
    certificate: default
    datacenter name: DC1
    extension key: Cisco_Nexus_5500_1945593678
    dvs name: Pod1
    DVS uuid: cd 05 25 50 6d a9 a5 c4-eb 9c 8f 6b fa 51 b1 aa
```

```
    config status: Enabled
    operational status: Connected
    sync status: in progress
    version: VMware vCenter Server 5.0.0 build-388657


Peer Info:
----------
    hostname: -
    ip address: -
    vrf:
    protocol: -
    extension key: Cisco_Nexus_5500_1945593678
    certificate: default
      certificate match: TRUE
    datacenter name: DC1
    dvs name: Pod1
    DVS uuid: cd 05 25 50 6d a9 a5 c4-eb 9c 8f 6b fa 51 b1 aa
    config status: Disabled
    operational status: Connected

switch-1(config)#
```

索 引

数字

A

B

C

D

E

F

I

L

M

N

P

Q

R

S

U

V

あ

い

た

ち

て

と

ね

は

ひ

ふ

ほ

ま

む

ゆ

よ

ら

り

る

れ

ろ