Cisco Nexus 5600 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 7.x

初版：2014 年 03 月 15 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-31636-01-J

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

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

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

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

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

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

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。 マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。 説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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

© 2014 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xiii

対象読者 xiii

表記法 xiii

Cisco Nexus 6000 シリーズ NX-OS ソフトウェアの関連資料 xv

マニュアルに関するフィードバック xvii

マニュアルの入手方法およびテクニカル サポート xvii

概要 1

レイヤ 2 イーサネット スイッチングの概要 1

VLAN 1

プライベート VLAN 2

スパニングツリー 2

STP の概要 3

Rapid PVST+ 3

MST 3

STP 拡張機能 4

VLAN の設定 5

VLAN について 5

VLAN の概要 5

VLAN 範囲の概要 7

VLAN の作成、削除、変更 8

VLAN トランキング プロトコルについて 8

VTP の注意事項と制約事項 9

VLAN の設定 10

VLAN の作成および削除 10

予約された VLAN の範囲の変更 11

VLAN の設定 12

VLAN へのポートの追加 14
VTP の設定 14
VLAN の設定の確認 16
プライベート VLAN の設定 17
プライベート VLAN について 17
プライベート VLAN のプライマリ VLAN とセカンダリ VLAN 18
プライベート VLAN ポート 19
プライマリ、独立、およびコミュニティ プライベート VLAN 20
プライマリ VLAN とセカンダリ VLAN の関連付け 21
プライベート VLAN 無差別トランク 22
プライベート VLAN 独立トランク 22
プライベート VLAN 内のブロードキャスト トラフィック 22
プライベート VLAN ポートの分離 23
プライベート VLAN に関する注意事項および制約事項 23
プライベート VLAN の設定 24
プライベート VLAN をイネーブルにするには 24
プライベート VLAN としての VLAN の設定 24
セカンダリ VLAN のプライマリ プライベート VLAN との関連付け 25
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 27
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 28
無差別トランク ポートの設定 29
独立トランク ポートの設定 30
FEX トランク ポートでのプライベート VLAN の設定 31
PVLAN トランキング ポートの許可 VLAN の設定 32
プライベート VLAN のネイティブ 802.1Q VLAN の設定 33
プライベート VLAN 設定の確認 34
アクセス インターフェイスとトランク インターフェイスの設定 37
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 37
アクセス インターフェイスとトランク インターフェイスの概要 37
IEEE 802.1Q カプセル化の概要 39
アクセス VLAN の概要 39
トランク ポートのネイティブ VLAN ID の概要 40

許可 VLAN の概要 40
ネイティブ 802.1Q VLAN の概要 40
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 41
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 41
アクセス ホスト ポートの設定 42
トランク ポートの設定 43
802.1Q トランク ポートのネイティブ VLAN の設定 44
トランキング ポートの許可 VLAN の設定 45
ネイティブ 802.1Q VLAN の設定 46
インターフェイスの設定の確認 47
拡張仮想ポート チャネルの設定 49
拡張 vPC について 49
拡張仮想ポート チャネルの概要 49
サポートされているプラットフォームとトポロジ 50
拡張 vPC のスケーラビリティ 51
拡張 vPC の失敗応答 51
拡張 vPC のライセンス要件 52
拡張 vPC の設定 53
拡張 vPC 設定手順の概要 53
拡張 vPC の確認 54
拡張 vPC 設定の確認 54
ポート チャネル番号の整合性の確認 55
共通のポート チャネル番号の確認 56
拡張 vPC のインターフェイス レベルの整合性の確認 57
拡張 vPC の設定例 58
Rapid PVST+ の設定 61
Rapid PVST+ について 61
STP の概要 62
STP の概要 62
トポロジ形成の概要 62
ブリッジ ID の概要 63
ブリッジ プライオリティ値 63

拡張システム ID 63
STP MAC アドレス割り当て 64
BPDU の概要 65
ルート ブリッジの選定 66
スパニングツリー トポロジの作成 66
Rapid PVST+ の概要 67
Rapid PVST+ の概要 67
Rapid PVST+ BPDU 69
提案と合意のハンドシェイク 70
プロトコル タイマー 71
ポート ロール 71
ポート ステート 73
Rapid PVST+ ポート ステートの概要 73
ブロッキング ステート 73
ラーニング ステート 74
フォワーディング ステート 74
ディセーブル ステート 74
ポート ステートの概要 75
ポート ロールの同期 75
優位 BPDU 情報の処理 76
下位 BPDU 情報の処理 76
スパニングツリー検証メカニズム 77
ポート コスト 77
ポート プライオリティ 78
Rapid PVST+ と IEEE 802.1Q トランク 78
Rapid PVST+ のレガシー 802.1D STP との相互運用 79
Rapid PVST+ の 802.1s MST との相互運用 79
Rapid PVST+ の設定 80
Rapid PVST+ のイネーブル化 80
Rapid PVST+ の VLAN ベースのイネーブル化 81
ルート ブリッジ ID の設定 82
セカンダリ ルート ブリッジの設定 83

Rapid PVST+ のポート プライオリティの設定 84
Rapid PVST+ パスコスト方式およびポート コストの設定 85
VLAN の Rapid PVST+ のブリッジ プライオリティの設定 86
VLAN の Rapid PVST+ の hello タイムの設定 87
VLAN の Rapid PVST+ の転送遅延時間の設定 87
VLAN の Rapid PVST+ の最大エージング タイムの設定 88
リンク タイプの設定 88
プロトコルの再開 89
Rapid PVST+ の設定の確認 90
マルチ スパニングツリーの設定 91
MST について 91
MST の概要 91
MST リージョン 92
MST BPDU 92
MST 設定情報 93
IST、CIST、CST 94
IST、CIST、CST の概要 94
MST リージョン内でのスパニングツリーの動作 94
MST リージョン間のスパニングツリー動作 95
MST 用語 96
ホップ カウント 97
境界ポート 97
スパニングツリー検証メカニズム 98
ポート コストとポート プライオリティ 99
IEEE 802.1D との相互運用性 99
Rapid PVST+ の相互運用性と PVST シミュレーションについて 100
MST の設定 100
MST 設定時の注意事項 100
MST のイネーブル化 101
MST コンフィギュレーション モードの開始 102
MST の名前の指定 103
MST 設定のリビジョン番号の指定 104

MST リージョンでの設定の指定 104
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 106
プライベート VLAN でセカンダリ VLAN をプライマリ VLAN として同じ MSTI にマッピングするには 107
ルート ブリッジの設定 108
セカンダリ ルート ブリッジの設定 109
ポートのプライオリティの設定 110
ポート コストの設定 111
スイッチのプライオリティの設定 112
hello タイムの設定 113
転送遅延時間の設定 114
最大エージング タイムの設定 114
最大ホップ カウントの設定 115
PVST シミュレーションのグローバル設定 116
ポートごとの PVST シミュレーションの設定 116
リンク タイプの設定 117
プロトコルの再開 118
MST の設定の確認 119
STP 拡張機能の設定 121
STP 拡張機能 121
STP 拡張機能について 121
STP ポート タイプの概要 121
スパニングツリー エッジ ポート 122
スパニングツリー ネットワーク ポート 122
スパニングツリー標準ポート 122
Bridge Assurance の概要 122
BPDU ガードの概要 123
BPDU フィルタリングの概要 123
ループ ガードの概要 125
ルート ガードの概要 126
STP 拡張機能の設定 126
STP 拡張機能の設定における注意事項 126

スパニングツリー ポート タイプのグローバルな設定 127
指定インターフェイスでのスパニングツリー エッジ ポートの設定 128
指定インターフェイスでのスパニングツリー ネットワーク ポートの設定 129
BPDU ガードのグローバルなイネーブル化 130
指定インターフェイスでの BPDU ガードのイネーブル化 131
BPDU フィルタリングのグローバルなイネーブル化 132
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 133
ループ ガードのグローバルなイネーブル化 135
指定インターフェイスでのループ ガードまたはルート ガードのイネーブル化 136
STP 拡張機能の設定の確認 137
LLDP の設定 139
グローバル LLDP コマンドの設定 139
インターフェイス LLDP の設定 141
MAC アドレス テーブルの設定 145
MAC アドレスに関する情報 145
MAC アドレスの設定 146
スタティック MAC アドレスの設定 146
MAC テーブルのエージング タイムの設定 146
MAC テーブルからのダイナミック アドレスのクリア 147
MAC アドレスの設定の確認 147
IGMP スヌーピングの設定 149
IGMP スヌーピングの情報 149
IGMPv1 および IGMPv2 150
IGMPv3 151
IGMP スヌーピング クエリア 151
IGMP 転送 151
IGMP スヌーピング パラメータの設定 152
IGMP スヌーピングの設定確認 156
MVR の設定 159
MVR について 159
MVR の概要 159
MVR の他の機能との相互運用性 160

MVR のライセンス要件 160
MVR に関する注意事項と制約事項 161
デフォルトの MVR 設定 161
MVR の設定 162
MVR グローバル パラメータの設定 162
MVR インターフェイスの設定 163
MVR 設定の確認 165
トラフィック ストーム制御の設定 169
トラフィック ストーム制御の概要 169
トラフィック ストーム制御の注意事項と制約事項 171
トラフィック ストーム制御の設定 172
トラフィック ストーム制御の設定の確認 172
トラフィック ストーム制御の設定例 173
デフォルトのトラフィック ストームの設定 173
ファブリック エクステンダの設定 175
Cisco Nexus 2000 シリーズ ファブリック エクステンダについて 176
ファブリック エクステンダの用語 177
ファブリック エクステンダの機能 177
レイヤ 2 ホスト インターフェイス 178
ホスト ポート チャネル 178
VLAN およびプライベート VLAN 179
仮想ポート チャネル 179
Fibre Channel over Ethernet（FCoE）のサポート 181
プロトコル オフロード 181
Quality of Service 181
アクセス コントロール リスト 182
IGMP スヌーピング 182
スイッチド ポート アナライザ 182
ファブリック インターフェイスの機能 183
オーバーサブスクリプション 184
管理モデル 185
フォワーディング モデル 186

接続モデル 187
静的ピン接続ファブリック インターフェイス接続 187
ポート チャネル ファブリック インターフェイス接続 189
ポート番号の表記法 190
ファブリック エクステンダのイメージ管理 190
ファブリック エクステンダのハードウェア 191
シャーシ 191
イーサネット インターフェイス 191
ファブリック インターフェイスへのファブリック エクステンダの関連付け 192
イーサネット インターフェイスへのファブリック エクステンダの関連付け 193
ポート チャネルへのファブリック エクステンダの関連付け 194
インターフェイスからのファブリック エクステンダの関連付けの解除 196
ファブリック エクステンダ グローバル機能の設定 196
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 199
リンクの再配布 200
リンク数の変更 200
ピン接続順序の維持 201
ホスト インターフェイスの再配布 201
ファブリック エクステンダの設定の確認 202
シャーシ管理情報の確認 205
Cisco Nexus N2248TP-E ファブリック エクステンダの設定 210
共有バッファの設定 210
グローバル レベルでのキュー制限の設定 211
ポート レベルでのキュー制限の設定 212
アップリンク距離の設定 213
Cisco Nexus N2248PQ ファブリック エクステンダの設定 214
共有バッファの設定 214
アップリンク距離の設定 215
低速ドレインの設定 216
FEX グローバル レベルでのロードバランシング キュー 217
VM-FEX の設定 219
VM-FEX について 219

VM-FEX の概要 219
VM-FEX のコンポーネント 219
VM-FEX の用語 220
VM-FEX のライセンス要件 222
VM-FEX のデフォルト設定 222
VM-FEX の設定 222
VM-FEX 設定手順の概要 222
VM-FEX に必要な機能のイネーブル化 224
固定スタティック インターフェイスの設定 225
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 229
vCenter Server への SVS 接続の設定 230
vCenter Server への SVS 接続のアクティブ化 232
VM-FEX 設定の確認 233
仮想インターフェイスのステータスの確認 233
vCenter Server への接続の確認 235
MAC/ARP ハードウェア リソース カービング テンプレートの設定 237
MAC/ARP ハードウェア リソース カービング テンプレートについて 237
MAC/ARP ハードウェア リソース テンプレートの設定 238
デフォルト テンプレートの適用 239
MAC/ARP ハードウェア リソース カービング テンプレート設定の確認 240
VN-Segment の設定 241
VN-Segment について 241
VN-Segment の注意事項と制約事項 243
VN-Segment のイネーブル化 244
VLAN 用の VN-Segment の設定 244
Configure Sync での VLAN 用の VN-Segment の設定 245
トランジット モードでの VN-Segment の設定 246
非トランジット モードでの VN-Segment の設定 247
VN-Segment のディセーブル化 247
VN-Segment 設定の確認 248

はじめに

ここでは、次の項について説明します。

- 対象読者，xiii ページ
- 表記法，xiii ページ
- Cisco Nexus 6000 シリーズ NX-OS ソフトウェアの関連資料，xv ページ
- マニュアルに関するフィードバック，xvii ページ
- マニュアルの入手方法およびテクニカル サポート，xvii ページ

対象読者

このマニュアルは、Cisco Nexus デバイスおよび Cisco Nexus 2000 シリーズ ファブリック エクステンダのコンフィギュレーションおよびメンテナンスを担当するネットワーク管理者を対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。

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

例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。

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

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

Cisco Nexus 6000 シリーズ NX-OS ソフトウェアの関連資料

完全な Cisco NX-OS 6000 シリーズ マニュアル セットは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps12806/tsd_products_support_series_home.html

リリース ノート

リリース ノートは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/products-release-notes-list.html

コンフィギュレーション ガイド

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/products-installation-and-configuration-guides-list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 6000 Series NX-OS Adapter-FEX Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS FabricPath Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS FCoE Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Fundamentals Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Interfaces Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Layer 2 Switching Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Multicast Routing Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Quality of Service Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS SAN Switching Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Security Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS System Management Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Unicast Routing Configuration Guide*』

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

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/products-installation-guides-list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 6000 Series NX-OS Software Upgrade and Downgrade Guides*』

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 から入手できます。

コマンド リファレンス

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/products-command-reference-list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 6000 Series NX-OS Fabric Extender Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS FabricPath Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Fundamentals Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Interfaces Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Layer 2 Interfaces Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Multicast Routing Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Quality of Service Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Security Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS System Management Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS TrustSec Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Unicast Routing Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Virtual Port Channel Command Reference*』

テクニカル リファレンス

『*Cisco Nexus 6000 Series NX-OS MIB Reference*』は http://www.cisco.com/en/US/docs/switches/datacenter/nexus6000/sw/mib/reference/NX6000_MIBRef.html から入手できます。

エラー メッセージおよびシステム メッセージ

『*Cisco Nexus 6000 Series NX-OS System Message Guide*』は、http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus6000/sw/system_messages/reference/sl_nxos_book.html から入手できます。

トラブルシューティング ガイド

『*Cisco Nexus 6000 Series NX-OS Troubleshooting Guide*』は、http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/tsd-products-support-troubleshoot-and-alerts.html から入手できます。

マニュアルに関するフィードバック

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

- nexus5k-docfeedback@cisco.com

ご協力をよろしくお願いいたします。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html から入手できます。

『*What's New in Cisco Product Documentation*』はシスコの新規および改訂版の技術マニュアルの一覧を提供するもので、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すると、コンテンツがデスクトップに直接配信されるようになります。 RSS フィードは無料のサービスです。

第 1 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，1 ページ
- VLAN，1 ページ
- プライベート VLAN，2 ページ
- スパニングツリー，2 ページ

レイヤ 2 イーサネット スイッチングの概要

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

デバイスでは、高帯域デバイスや多数のユーザに起因する輻輳問題を解決するために、（サーバなどの）デバイスごとに専用のドメインを割り当てます。 各 LAN ポートが個別のイーサネット コリジョン ドメインに接続されるので、スイッチド環境のサーバは全帯域幅にアクセスできます。

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

VLAN

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

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

どのようなスイッチポートでもVLANに属すことができ、ユニキャスト、ブロードキャスト、マルチキャストのパケットは、その VLAN に属する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される必要があります。

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

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

（注） スイッチ間リンク（ISL）トランキングはサポートされません。

プライベート VLAN

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

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

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

スパニングツリー

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

STP の概要

STP は、レイヤ 2 レベルで、ループのないネットワークを実現します。 レイヤ 2 LAN ポートは STP フレーム（Bridge Protocol Data Unit（BPDU:ブリッジ プロトコル データ ユニット））を一定の時間間隔で送受信します。 ネットワークデバイスは、これらのフレームを転送せずに、フレームを使用してループフリー パスを構築します。

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

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

ソフトウェアは、従来の 802.1D システムで相互運用できますが、デバイスでは Rapid PVST+ および MST が実行されます。 特定の VDC に、Rapid PVST+ または MST のどちらかを使用できます。 1 つの VDC では両方は使用できません。 Rapid PVST+ はデフォルトの STP プロトコルです。

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

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

Rapid PVST+

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

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

MST

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

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

（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 ガードを使用すると、ポイントツーポイント リンク上の単方向リンク障害によって発生するブリッジング ループを防止できます。
- ルート ガード：ルート ガード機能は、ポートがルート ポートになること、またはブロックされることを防ぎます。 ルート ガードに設定されたポートが上位 BPDU を受信すると、このポートはただちにルート不整合（ブロックされた）状態になります。

第 2 章

VLAN の設定

この章の内容は、次のとおりです。

- VLAN について，5 ページ
- VLAN の設定，10 ページ

VLAN について

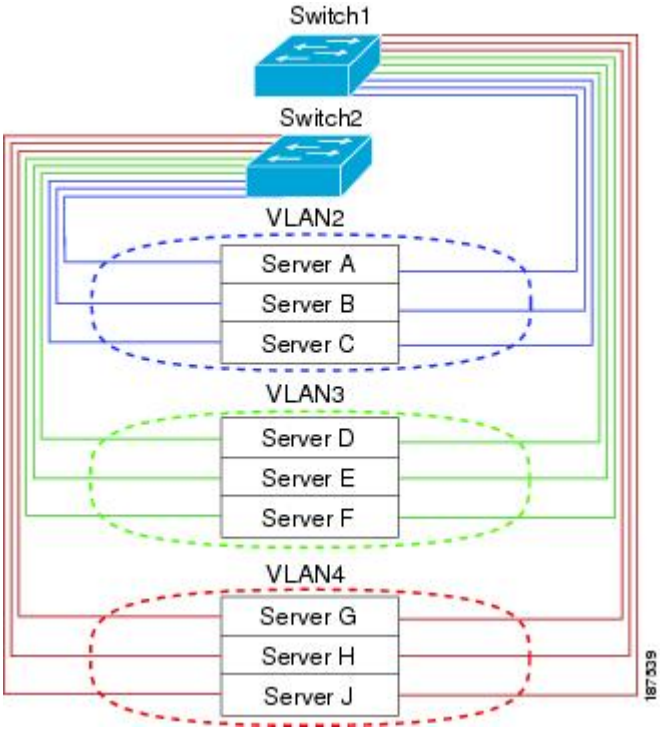
VLAN の概要

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 を示します。 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 *1*： 論理的に定義されたネットワークとしての *VLAN*



VLAN は、通常 IP サブネットワークに関連付けます。 たとえば、特定の IP サブネットに含まれるすべてのエンド ステーションを同じ VLAN に属させる場合などです。 VLAN 間で通信するには、トラフィックをルーティングする必要があります。

デフォルトでは、新規に作成された VLAN は動作可能です。 VLAN をディセーブルにするには、**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。 このプロセスは、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）としても設定できます。 この場合、VLAN のスイッチポートはルーティング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相当します。 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ため、またはスイッチのインバンド管理のためのレイヤ 3 プロトコルをサポートしている場合、SVI はルーティングに設定できます。

VLAN 範囲の概要

Cisco Nexus デバイスでは、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 の設定の制限の詳細については、デバイスの設定の制限に関するマニュアルを参照してください。

次の表に、VLAN 範囲の詳細を示します。

表 *1*： *VLAN* の範囲

VLAN 番号	範囲	用途
1	標準	シスコ システムズのデフォルトです。 この VLAN は使用できますが、変更や削除はできません。
2 ～ 1005	標準	これらの VLAN は、作成、使用、変更、削除できます。
1006 ～ 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） 内部的に割り当てられている VLAN（予約済みの VLAN）を設定できます。

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）はデフォルト値だけを使用します。 デフォルト VLAN のアクティビティは作成、削除、または一時停止できません。

それに番号を割り当てることによって、VLAN を作成します。 VLAN の削除、およびそれらのアクティブ動作ステートから一時停止動作ステートへの移行ができます。 既存の VLAN ID で VLAN を作成しようとすると、スイッチは VLAN サブモードになりますが、同一の VLAN は再作成しません。

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

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

- VLAN 名
- シャットダウンまたは非シャットダウン

特定の VLAN を削除すると、その VLAN に関連するポートはシャットダウンされ、トラフィックは流れなくなります。 しかしシステムはその VLAN の VLAN/ポート マッピングをすべて維持するため、この指定 VLAN の再イネーブル化や再作成を行うと、その VLAN の元のすべてのポートはシステムによって自動的に回復されます。

VLAN トランキング プロトコルについて

VTP はドメイン全体で VTP VLAN データベースを同期する分散 VLAN データベース管理プロトコルです。 VTP ドメインは、同じ VTP ドメイン名を共有し、トランク インターフェイスを使用して接続される、1 つ以上のネットワーク スイッチで構成されます。 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。 クライアント モードまたはサーバ モードで VTP を設定できます。 以前のリリースでは、VTP はトランスペアレント モードだけで動作していました。

VTP モードは次のとおりです。

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

VTP 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 デバイス では、512 個の VLAN がサポートされます。 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 デバイス では、512 個の VLAN がサポートされます。 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。 Cisco Nexus デバイス のクライアント/サーバが VTP サーバから追加の VLAN を受け取った場合は、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。
- Cisco Nexus ファブリック エクステンダ ポートでは、VTP アドバタイズメントは送信されません。
- VTP プルーニングはサポートされません。
- スイッチがトランスペアレント モードにある場合にだけ、プライベート VLAN（PVLAN）がサポートされます。
- 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。
- 予約済みの VLAN の範囲の変更後に、**copy running-config startup-config** コマンドを入力してリロードする必要があります。 次に例を示します。

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

  スイッチのリロード後、VLAN 2000 ～ 2127 は内部使用のために予約されます。そのため、スイッチのリロード前に **copy running-config startup-config** コマンドを入力する必要があります。 この範囲内の VLAN を作成することはできません。

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 に関連付けられたポートはシャットダウンします。 トラフィックは流れなくなり、パケットはドロップされます。

手順

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

	コマンドまたはアクション	目的
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。

予約された VLAN の範囲の変更

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

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

手順

	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)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**system vlan** *start-vlan* **reserve** 例： `switch(config)# system vlan 3968 reserve`	目的の範囲の開始 VLAN ID を指定することにより、予約済みの VLAN の範囲を変更できます。 予約済みの VLAN を、80 の隣接する他の VLAN 範囲に変更できます。 このような範囲を予約すると、内部使用のためにデフォルトで割り当てられた VLAN 範囲が解放され、それらの VLAN はすべて VLAN 4094 を除くユーザ設定に使用できます。 （注） 予約済み VLAN（3968 ～ 4094）のデフォルトの範囲に戻すには、**no system vlan** *start-vlan* **reserve** コマンドを入力する必要があります。

	コマンドまたはアクション	目的
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 （注） 予約済みのブロックを変更した場合、このコマンドを入力する必要があります。
ステップ 4	**reload** 例： `switch(config)# reload`	ソフトウェアをリロードし、VLAN の範囲の変更が有効になります。 このコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x*』を参照してください。
ステップ 5	**show system vlan reserved** 例： `switch(config)# show system vlan reserved`	（任意） VLAN 範囲に対して設定された変更を表示します。

次に、予約済みの VLAN 範囲を変更する例を示します。

```
switch# configuration terminal
switch(config)# system vlan 1006 reserve
This will delete all configs on vlans 1006-1085. Continue anyway? (y/n) [no] yes
Note: After switch reload, VLANs 1006-1085 will be reserved for internal use.
      This requires copy running-config to startup-config before
      switch reload.  Creating VLANs within this range is not allowed.
switch(config)# copy running-config startup-config
switch(config)# reload
switch(config)# show system vlan reserved
```

（注） この変更を有効にするには、デバイスをリロードする必要があります。

VLAN の設定

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

- 名前
- シャットダウン

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {**ethernet** *slot*/*port* | **port-channel** *number*}	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスには、物理イーサネット ポートまたは EtherChannel を指定できます。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **switchport access vlan** *vlan-id*	インターフェイスのアクセス モードを指定 VLAN に設定します。

次の例は、VLAN 5 に参加するようにイーサネット インターフェイスを設定する方法を示しています。

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

VTP の設定

Cisco Nexus デバイス では、クライアント モードまたはサーバ モードで VTP を設定できます。

VPT をイネーブルにした後、VTP モード（server [default]、client、transparent、または off）を設定できます。 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

	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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **feature vtp**	デバイスの VTP をイネーブルにします。 デフォルトはディセーブルです。
ステップ 3	switch(config)# **vtp domain** *domain-name*	このデバイスを参加させる VTP ドメインの名前を指定します。 デフォルトは空白です。
ステップ 4	switch(config)# **vtp version** {**1** | **2**}	使用する VTP バージョンを設定します。 デフォルトはバージョン 1 です。
ステップ 5	switch(config)# **vtp mode** {**client** | **server**| **transparent**| **off**}	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。 クライアントモードまたはサーバモードで VTP を設定できます。
ステップ 6	switch(config)# **vtp file** *file-name*	VTP コンフィギュレーションを保存する IFS ファイル システムのファイルの ASCII ファイル名を指定します。
ステップ 7	switch(config)# **vtp password** *password-value*	VTP 管理ドメインのパスワードを指定します。
ステップ 8	switch(config)# **exit**	コンフィギュレーション サブモードを終了します。
ステップ 9	switch# **show vtp status**	（任意） バージョン、モードおよびリビジョン番号などのデバイスの VTP 設定に関する情報を表示します。
ステップ 10	switch# **show vtp counters**	（任意） デバイスの VTP アドバタイズメントの統計に関する情報を表示します。
ステップ 11	switch# **show vtp interface**	（任意） VTP-enabled インターフェイスのリストを表示します。
ステップ 12	switch# **show vtp password**	（任意） 管理 VTP ドメインのパスワードを表示します。
ステップ 13	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、デバイス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#
```

次に、VTP ステータスを表示する例を示します。スイッチがバージョン 2 をサポート可能であること、およびスイッチが現在バージョン 1 を実行していることがわかります。

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

VLAN の設定の確認

設定を確認するには、次のいずれかのコマンドを使用します。

コマンド	目的
switch# **show running-config vlan** [*vlan_id* | *vlan_range*]	VLAN 情報を表示します。
switch# **show vlan** [**brief** | **id** [*vlan_id* | *vlan_range*] | **name** *name* | **summary**]	定義済み VLAN の選択した設定情報を表示します。
switch# **show system vlan reserved**	システムに予約されている VLAN 範囲を表示します。

第 3 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。

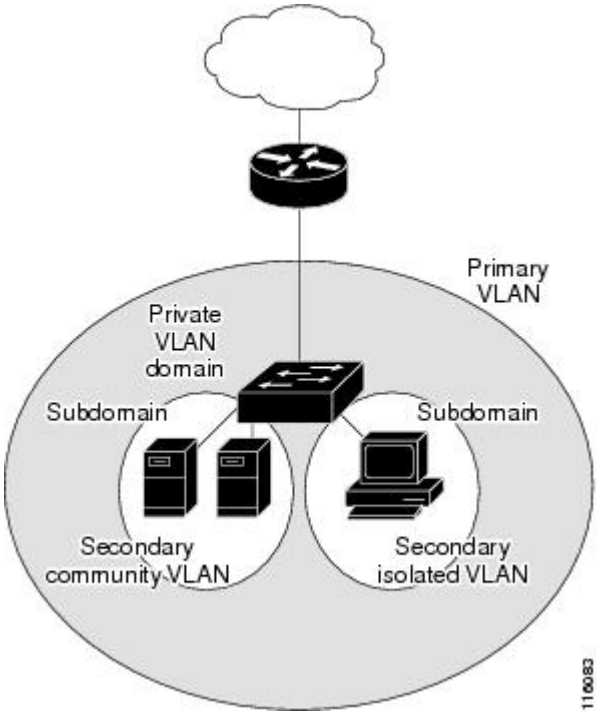
- プライベート VLAN について，17 ページ
- プライベート VLAN に関する注意事項および制約事項，23 ページ
- プライベート VLAN の設定，24 ページ
- プライベート VLAN 設定の確認，34 ページ

プライベート VLAN について

プライベート VLAN（PVLAN）では VLAN のイーサネット ブロードキャスト ドメインがサブドメインに分割されるため、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 上で関連付けら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関連付けられている無差別ポートと通信できますが、他のコミュニティ VLAN にあるポートとは通信できません。

図 *2*：プライベート *VLAN* ドメイン



（注） 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、無差別ポートと関連付けられているセカンダリ VLAN に属し、プライマリ VLAN と関連付けられている、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 を、複数の無差別ポートと関連付けることができます。 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。 無差別ポートと関連付けら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：独立セカンダリ 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、無差別ポートだけに転送されます。 指定した独立 VLAN には、複数の独立ポートを含めることができます。 各ポートは、独立 VLAN にある他のすべてのポートから、完全に隔離されています。

  独立ポートは、アクセス ポートまたはトランク 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 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関連付けら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。

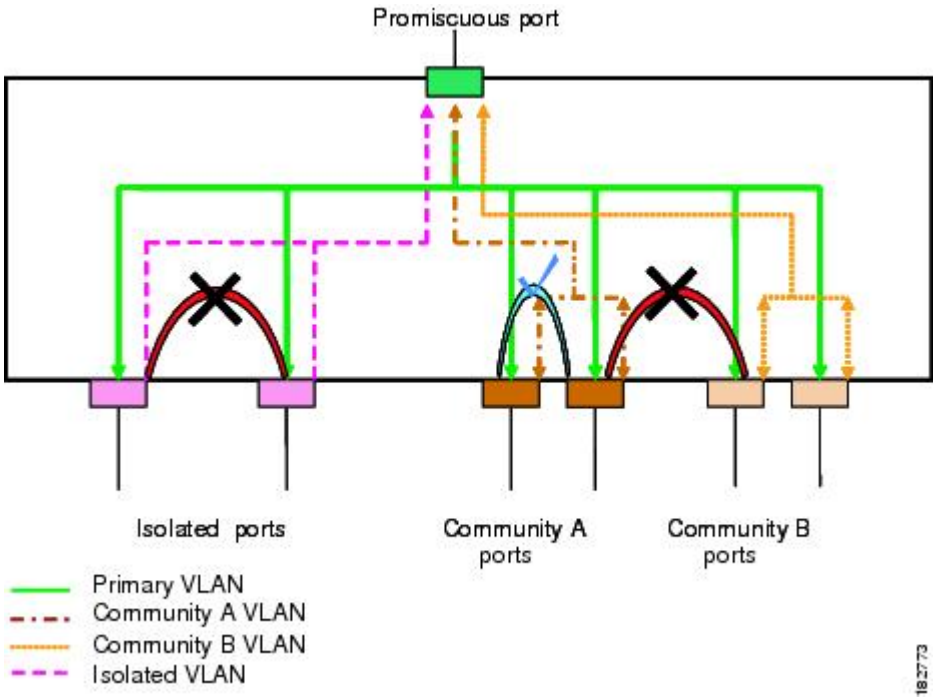
プライマリ、独立、およびコミュニティ プライベート VLAN

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 には、複数の独立ポートを設定できます。 各独立ポートからのトラフィックも完全に隔離されたままです。
- コミュニティ VLAN：コミュニティ VLAN は、コミュニティ ポートから、無差別ポートおよび同じコミュニティにある他のホスト ポートへ、アップストリーム トラフィックを送信するセカンダリ VLAN です。 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 *3*：プライベート *VLAN* のトラフィック フロー



（注） PVLAN のトラフィック フローは、ホスト ポートから無差別ポートへの単方向です。 プライマリ VLAN で受信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、1 つだけのプライマリ VLAN と複数のセカンダリ VLAN（コミュニティ VLAN および独立 VLAN）を処理できます。 無差別トランク 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。 指定されたプライマリ VLAN の複数のセカンダリ VLAN を無差別トランク ポートにマッピングできます。 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。 プライベート VLAN の外部と通信するには、エンドステーションでは、デフォルト ゲートウェイのみと通信する必要があります。

プライマリ VLAN とセカンダリ VLAN の関連付け

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。 関連付け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 のみに関連付けることができます。

関連付け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 無差別トランク

無差別トランク ポートは、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。 無差別ポートのトラフィックはプライマリ VLAN タグとともに送受信されます。

プライベート VLAN 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 ポートで伝送されません。 独立トランク ポートのトラフィックは、独立 VLAN タグとともに送受信されます。 独立トランク ポートは、ホスト サーバに接続するように設計されています。

Cisco Nexus ファブリック エクステンダ の独立 PVLAN ポートをサポートするためには、Cisco Nexus デバイスにより 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、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、独立ポートに関連付けられているプライマリ VLAN にある無差別ポートにのみ配信されます。
- コミュニティ ポートからのブロードキャスト トラフィックは、そのポートのコミュニティ内のすべてのポート、およびそのコミュニティ ポートに関連付けられているすべての無差別ポートに配信されます。 このブロードキャスト パケットは、プライマリ VLAN 内の他のコミュニティまたは独立ポートには配信されません。

プライベート VLAN ポートの分離

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

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

プライベート VLAN に関する注意事項および制約事項

PVLAN を設定する場合は、次の注意事項に従ってください。

- 指定した VLAN をプライベート VLAN として割り当てる前に、VLAN を作成しておく必要があります。
- スイッチで 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。
- プライマリ VLAN と同じ MST インスタンスにセカンダリ VLAN をマッピングするには、Multiple Spanning Tree（MST）リージョン定義内から **private-vlan synchronize** コマンドを入力します。
- 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。
- 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

	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)# **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

	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)# **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 との関連付け

セカンダリ VLAN をプライマリ VLAN に関連付けるときには、次の事項に注意してください。

- *secondary-vlan-list* パラメータには、スペースを含めないでください。 カンマで区切った複数の項目を含めることができます。 各項目は、単一のセカンダリ VLAN ID、またはセカンダリ VLAN ID をハイフンでつないだ範囲にできます。

- *secondary-vlan-list* パラメータには、複数のコミュニティ VLAN ID と 1 つの独立 VLAN ID を指定できます。
- セカンダリ VLAN をプライマリ VLAN に関連付けるには、*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 との関連付けをクリアするには、*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 との関連付けを変更するには、既存の関連付けを削除し、次に必要な関連付けを追加します。

プライマリまたはセカンダリ VLAN のいずれかを削除すると、VLAN は関連付けが設定されたポートで非アクティブになります。 **no private-vlan** コマンドを入力すると、VLAN は通常の VLAN モードに戻ります。 その VLAN における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

	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)# **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 との関連付けをクリアするには、*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 からすべての関連付けを削除し、通常の VLAN モードに戻します。

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

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

インターフェイスをプライベート VLAN ホスト ポートとして設定するには

PVLAN では、ホスト ポートはセカンダリ 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 関連付け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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type* [*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）。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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。

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

はじめる前に

PVLAN 機能がイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	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。 （注） これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/QSFP-module/port* になります。
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*}	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

	コマンドまたはアクション	目的
	{*secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list*}	定した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。
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、無差別ポートとしてイーサネット インターフェイス 1/4 を設定し、プライマリ VLAN 5 およびセカンダリ独立 VLAN 200 にそのポートを関連付ける方法を示しています。

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

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 ポートは、複数のプライマリ VLAN を伝送できます。 指定されたプライマリ VLAN の複数のセカンダリ VLAN を無差別トランク ポートにマッピングできます。

無差別ポートの設定には、2 つの手順が必要です。 最初にポートを無差別ポートに定義した後で、セカンダリ VLAN とプライマリ VLAN 間のマッピングを設定します。 複数のプライマリ VLAN は複数のマッピングを設定することでイネーブルにできます。

（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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	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。 （注） これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/QSFP-module/port* になります。

	コマンドまたはアクション	目的
ステップ 3	switch(config-if)# **switchport 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。
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 ポートの設定には、2 つの手順が必要です。 最初に、独立トランク ポートとしてポートを定義した後で、独立 VLAN とプライマリ VLAN との関連付けを設定します。 複数の独立 VLAN は複数の関連付けを設定することでイネーブルにできます。

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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type* [*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）。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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** キーワードがない場合は、それが仮定されます。
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。指定されたプライマリ VLAN では、1 つの独立 VLAN だけがマッピングできます。
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。

次に、イーサネット インターフェイス 1/1 を PVLAN の独立トランク ポートとして設定し、セカンダリ VLAN をプライマリ VLAN に関連付ける方法を示します。

```
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 trunk 5 100
switch(config-if)# switchport private-vlan association trunk 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 Nexus デバイス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） FEXインターフェイスでは、無差別ポートを含む設定はサポートされていません。 また、FEXインターフェイスでは、無差別ポートを持つデバイスへの接続もサポートされていません。無差別機能が必要な場合は、Cisco Nexus 1000V などのデバイスを Cisco Nexus デバイスのベース ポートに接続する必要があります。

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 ポートと独立ホスト 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

	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、変更を永続的に保存します。

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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type* [*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）。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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 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。 この設定は、タグなしトラフィックと制御トラフィックが Cisco Nexus デバイスを通過するようにします。 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） トランクは、複数の VLAN のトラフィックを伝送できます。 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ように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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type* [*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）。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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には、次のコマンドを使用します。

コマンド	目的
switch# **show feature**	スイッチでイネーブルになっている機能を表示します。
switch# **show interface switchport**	スイッチ ポートとして設定されているすべてのインターフェイスに関する情報を表示します。
switch# **show vlan private-vlan** [**type**]	PVLAN のステータスを表示します。

次の例は、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
```

次に、イネーブルになっている機能を表示する方法を示します（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 4 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，37 ページ
- アクセス インターフェイスとトランク インターフェイスの設定，41 ページ
- インターフェイスの設定の確認，47 ページ

アクセスインターフェイスとトランクインターフェイスについて

アクセス インターフェイスとトランク インターフェイスの概要

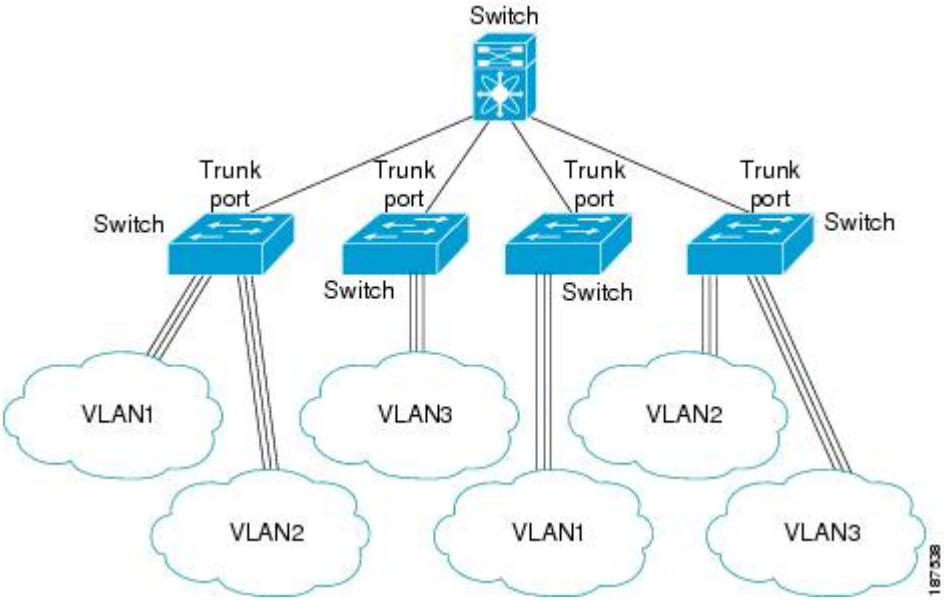
イーサネット インターフェイスは、次のように、アクセス ポートまたはトランク ポートとして設定できます。

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

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

次の図は、ネットワーク内でのトランク ポートの使用方法を示します。 トランク ポートは、2 つ以上の VLAN のトラフィックを伝送します。

図 *4*： トランキング環境におけるデバイス



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

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

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

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

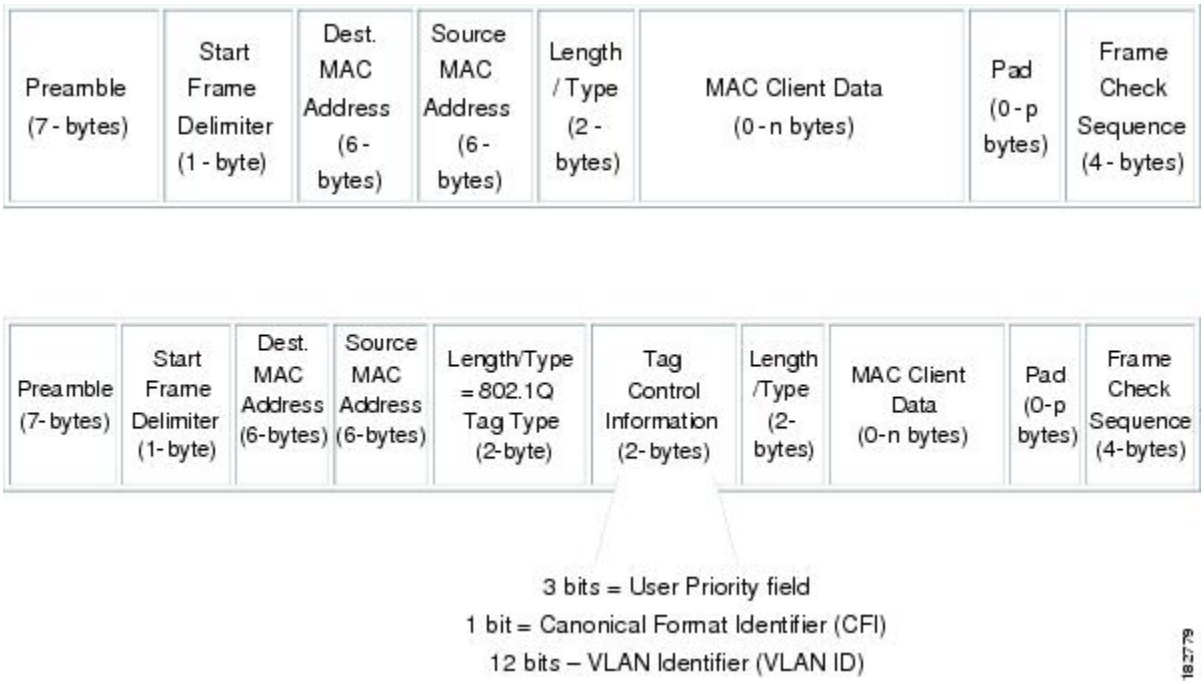
（注） イーサネット インターフェイスはアクセス ポートまたはトランク ポートとして動作できますが、両方のポート タイプとして同時に動作することはできません。

IEEE 802.1Q カプセル化の概要

トランクは、デバイスと他のネットワーク デバイス間のポイントツーポイント リンクです。 トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張することができます。

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

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



アクセス VLAN の概要

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

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

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

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

トランク ポートのネイティブ VLAN ID の概要

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

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

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

許可 VLAN の概要

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

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

ネイティブ 802.1Q VLAN の概要

802.1Q トランク ポートを通過するトラフィックのセキュリティを強化するために、**vlan dot1q tag native** コマンドが追加されました。 この機能は、802.1Q トランク ポートから出ていくすべてのパ

ケットがタグ付けされていることを確認し、802.1Q トランク ポート上でタグなしパケットの受信を防止するための手段を提供します。

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

この動作は、ハッカーが別の VLAN へのフレーム ジャンプを試みて実行する「VLAN ホッピング」の取り込みに不正利用できる可能性があります。 また、タグなしパケットを 802.1Q トランク ポートに送信することによって、トラフィックがネイティブ VLAN の一部になる可能性もあります。

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

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

この機能は、すべての直接接続されたイーサネット インターフェイスおよびポート チャネル インターフェイスでサポートされます。 また、接続されたファブリック エクステンダ（FEX）のすべてのホスト インターフェイス ポートでサポートされます。

（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 モードで入力することで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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {{*type slot*/*port*} | {**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。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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ンニングツリーエッジポートにすることが可能であり、BPDU フィルタリングおよび BPDU ガードを同時にイネーブルにすることができます。

はじめる前に

正しいインターフェイスを設定していることを確認します。これは、エンド ステーションに接続されているインターフェイスである必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	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。 （注） これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/QSFP-module/port* になります。
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。

手順

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

	コマンドまたはアクション	目的
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。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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。

次に、インターフェイスをイーサネット トランク ポートとして設定する例を示します。

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

802.1Q トランク ポートのネイティブ VLAN の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {*type slot*/*port* | **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。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **switchport trunk native vlan** *vlan-id*	802.1Q トランクのネイティブ VLAN を設定します。指定できる範囲は 1 ～ 4094 です（ただし、内部使

	コマンドまたはアクション	目的
		用に予約されている VLAN は除きます）。 デフォルト値は VLAN 1 です。

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

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

トランキング ポートの許可 VLAN の設定

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {*type slot*/*port* | **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。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config-if)# **switchport trunk allowed vlan** {*vlan-list* **all** | **none** [**add** |except | none | **remove** {*vlan-list*}]}	トランク インターフェイスの許可 VLAN を設定します。デフォルトでは、トランク インターフェイス上のすべての VLAN（1 ～ 3967 および 4048 ～ 4094）が許可されます。 VLAN 3968 ～ 4047 は、内部利用のためにデフォルトで予約されている VLAN です。この VLAN グループは設定できません。 デフォルトでは、すべてのトランク インターフェイスですべての VLAN が許可されます。 （注） 内部で割り当て済みの VLAN を、トランク ポート上の許可 VLAN として追加することはできません。 内部で割り当て済みの VLAN を、トランク ポートの許可 VLAN として登録しようとすると、メッセージが返されます。

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

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

ネイティブ 802.1Q VLAN の設定

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

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

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **vlan dot1q tag native** [**tx-only**]	Cisco Nexus デバイス上のすべてのトランク ポートのすべてのネイティブ VLAN の dot1q（IEEE 802.1Q）タギングをイネーブルにします。 デフォルトでは、この機能は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** [**tx-only**]	（任意） スイッチ上のすべてのトランキング ポートのすべてのネイティブ VLAN の dot1q（IEEE 802.1Q）タギングをディセーブルにします。

	コマンドまたはアクション	目的
ステップ 4	switch# **show vlan dot1q tag native**	（任意） ネイティブ VLAN のタギングのステータスを表示します。

次に、スイッチ上の 802.1Q タギングをイネーブルにする方法を示します。

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

インターフェイスの設定の確認

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

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

第 5 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，49 ページ
- 拡張 vPC のライセンス要件，52 ページ
- 拡張 vPC の設定，53 ページ
- 拡張 vPC の確認，54 ページ
- 拡張 vPC の設定例，58 ページ

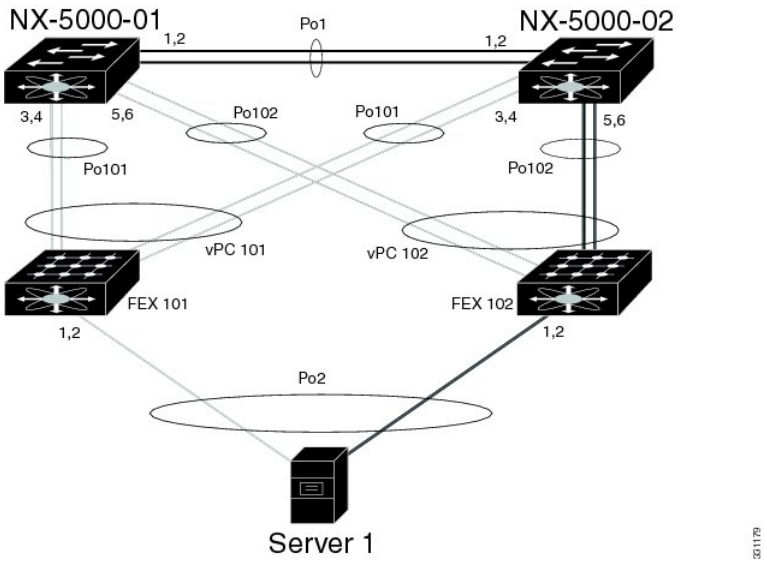
拡張 vPC について

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。

図 *6* : デュアル ホーミング トポロジ



拡張 vPCs 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

サポートされるプラットフォーム

拡張 vPC は、Cisco Nexus デバイスでサポートされます。

すべての Cisco Nexus 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 チャネルとリンク アグリケーション制御プロトコル（LACP）ベースのポート チャネルがサポートされています。

- Fibre Channel over Ethernet（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 デバイスは、最大 24 台の FEX（レイヤ 2 設定またはレイヤ 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不要です。 ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 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 FEX へのデュアルホーム接続と FEX 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、次の手順を実行します。 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。 設定の同期の詳細については、デバイスの『*Operations Guide*』を参照してください。

手順

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 つのスイッチに関連付け、2 番めの FEX をもう一方のスイッチに関連付けます。
デバイスの『*Fibre Channel over Ethernet Configuration Guide*』の「Configuring FCoE over Enhanced vPC」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 vPCs 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vPCs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 vPCs 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。

これらのコマンドからの出力フィールドの詳細については、デバイスの『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。

手順

	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入力し、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入力し、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

	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。 （注） これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/QSFP-module/port* になります。

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。

手順

	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。

```
switch-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。 設定の同期の詳細については、デバイスの『Operations Guide』を参照してください。

はじめる前に

Cisco Nexus 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

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：
```
switch-1(config)# feature vpc
switch-1(config)# feature lacp

switch-2(config)# feature vpc
switch-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：
```
switch-1(config)# vlan 10-20

switch-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：
```
switch-1(config)# vpc domain 123
switch-1(config-vpc)# peer-keepalive destination 172.25.182.100

switch-2(config)# vpc domain 123
switch-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：
```
switch-1(config)# interface eth1/1-2
switch-1(config-if)# channel-group 1 mode active
switch-1(config-if)# interface Po1
switch-1(config-if)# switchport mode trunk
switch-1(config-if)# switchport trunk allowed vlan 1, 10-20
switch-1(config-if)# vpc peer-link

switch-2(config)# interface eth1/1-2
switch-2(config-if)# channel-group 1 mode active
switch-2(config-if)# interface Po1
switch-2(config-if)# switchport mode trunk
switch-2(config-if)# switchport trunk allowed vlan 1, 10-20
switch-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：
```
switch-1(config)# fex 101
switch-1(config-fex)# interface eth1/3-4
switch-1(config-if)# channel-group 101
switch-1(config-if)# interface po101
switch-1(config-if)# switchport mode fex-fabric
switch-1(config-if)# vpc 101
switch-1(config-if)# fex associate 101

switch-2(config)# fex 101
switch-2(config-fex)# interface eth1/3-4
switch-2(config-if)# channel-group 101
switch-2(config-if)# interface po101
switch-2(config-if)# switchport mode fex-fabric
switch-2(config-if)# vpc 101
switch-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：
```
switch-1(config)# fex 102
switch-1(config-fex)# interface eth1/5-6
switch-1(config-if)# channel-group 102
switch-1(config-if)# interface po102
switch-1(config-if)# switchport mode fex-fabric
switch-1(config-if)# vpc 102
switch-1(config-if)# fex associate 102

switch-2(config)# fex 102
switch-2(config-fex)# interface eth1/5-6
switch-2(config-if)# channel-group 102
switch-2(config-if)# interface po102
switch-2(config-if)# switchport mode fex-fabric
switch-2(config-if)# vpc 102
switch-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：
```
switch-1(config)# interface eth101/1/1, eth101/1/2
switch-1(config-if)# channel-group 2 mode active
switch-1(config-if)# interface eth102/1/1, eth102/1/2
switch-1(config-if)# channel-group 2 mode active
switch-1(config-if)# int po2
switch-1(config-if)# switchport access vlan 10
```

```
switch-2(config)# interface eth101/1/1, eth101/1/2
switch-2(config-if)# channel-group 2 mode active
switch-2(config-if)# interface eth102/1/1, eth102/1/2
switch-2(config-if)# channel-group 2 mode active
switch-2(config-if)# int po2
switch-2(config-if)# switchport access vlan 10
```

第 6 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，61 ページ
- Rapid PVST+ の設定，80 ページ
- Rapid PVST+ の設定の確認，90 ページ

Rapid PVST+ について

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

Rapid PVST+ は、デフォルト VLAN（VLAN1）と、ソフトウェアで新たに作成された新しい VLAN でデフォルトでイネーブルになります。 Rapid PVST+ はレガシー IEEE 802.1D STP が稼働する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。

- 各スイッチに関連付けられている、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関連付けられているルートのパス コスト
- 各インターフェイスに関連付けら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

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

ブリッジ プライオリティ値

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

（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 *7*： 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 *2*：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。

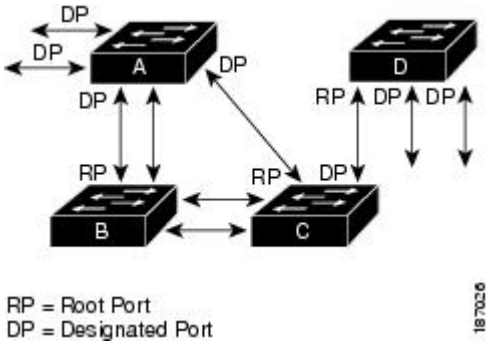
STP ルートブリッジは論理的に、ネットワークで各スパニングツリー トポロジの中心です。 ネットワークの任意の箇所からルート ブリッジに到達するために必要ではないすべてのパスは、STP ブロッキング モードになります。

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。 しかし、トラフィック パターン、フォワーディング ポートの数、リンク タイプによっては、スイッチ A が最適なルート ブリッジでないことがあります。 任意のスイッチのプライオリティを高くする（数値を小さくする）ことでそのスイッチがルート ブリッジになるようにします。これにより STP が強制的に再計算され、そのスイッチをルートとする新しいスパニングツリー トポロジが形成されます。

図 *8*：スパニングツリー トポロジ



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

接続すると、ルート ポートが変更される場合があります。 最高速のリンクをルート ポートにすることが重要です。

たとえば、スイッチ B の 1 つのポートが光ファイバ リンクであり、同じスイッチの別のポート（Unshielded Twisted-Pair（UTP：シールドなしツイストペア）リンク）がルート ポートになっていると仮定します。 ネットワーク トラフィックを高速の光ファイバ リンクに流した方が効率的です。 光ファイバ ポートの STP ポート プライオリティをルート ポートよりも高いプライオリティに変更すると（数値を下げる）、光ファイバ ポートが新しいルート ポートになります。

Rapid PVST+ の概要

Rapid PVST+ の概要

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

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

Rapid PVST+ では、ポイントツーポイントの配線を使用して、スパニングツリーの高速コンバージェンスが行われます。 Rapid PVST+ によりスパニングツリーの再設定を 1 秒未満に発生させることができます（802.1D STP のデフォルト設定では 50 秒）。

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

Rapid PVST+ を使用すると、STP コンバージェンスが急速に発生します。 STP にある各指定ポートまたは各ルート ポートにより、デフォルトで、2 秒ごとに BPDU が送信されます。 トポロジの指定ポートまたはルート ポートで、hello メッセージが 3 回連続で失われた場合、または、最大エージング タイム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、最大エージング タイムの期限が切れた場合、直接のネイバー ルートまたは指定ポートへの接続が失われたと見なされます。 プロトコル情報の急速な経過により、障害検出を迅速に行うことができます。 スイッチは PVID を自動的に確認します。

Rapid PVST+ により、ネットワーク デバイス、スイッチ ポート、または LAN の障害の直後に、接続が迅速に回復されます。 RSTP は、エッジ ポート、新しいルート ポート、およびポイントツーポイント リンクで接続されているポートに次のような高速コンバージェンスを提供します。

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

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

（注） ホストに接続されているすべてのポートを、エッジ ポートとして設定することを推奨します。

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

Rapid PVST+ では、エッジ ポートとポイントツーポイント リンクでのみ、フォワーディング ステートへの急速な移行が達成されます。 リンク タイプは設定が可能ですが、システムでは、ポートのデュプレックス設定からリンク タイプ情報が自動的に引き継がれます。 全二重ポートはポイントツーポイント ポートであると見なされ、半二重ポートは共有ポートであると見なされます。

エッジ ポートでは、トポロジの変更は生成されませんが、直接接続されているネイバーから 3 回連続 BPDU の受信に失敗するか、最大エージング タイム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関連付けられている 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。

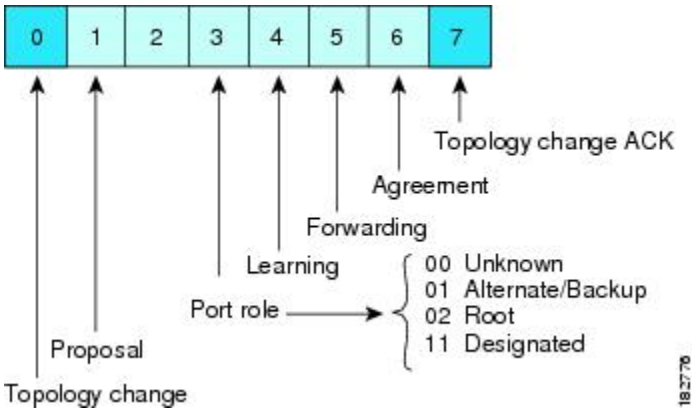
（注） スイッチが、レガシー 802.1D STP を実行しているスイッチと相互に動作しているときにのみ、TCA フラグが使用されます。

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 *9*： ***BPDU*** の ***Rapid PVST+*** フラグ バイト

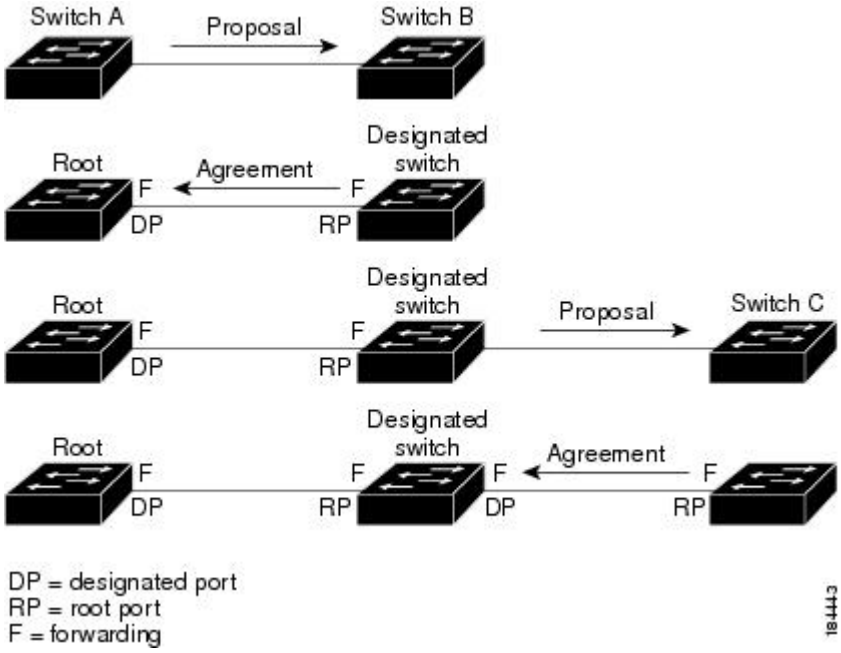


もう一つの重要な変更点は、Rapid PVST+ BPDU がタイプ 2、バージョン 2 であることで、これにより、スイッチでは、接続されているレガシー（802.1D）ブリッジを検出できるようになります。802.1D の BPDU は、バージョン 0 です。

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。 スイッチ A のプライオリティ値がスイッチ B のプライオリティ値より小さい数値であると仮定します。

図 *10*： 高速コンバージェンスの提案と合意のハンドシェイク



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

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

スイッチは、ポート デュプレックス モードからリンク タイプを認識します。全二重ポートはポイントツーポイント接続であると見なされ、半二重ポートは共有接続であると見なされます。デュプレックス設定によって制御されるデフォルト設定は、**spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを入力することで上書きできます。

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

プロトコル タイマー

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

表 3：***Rapid PVST+* のプロトコル タイマー**

変数	説明
hello タイマー	各スイッチから他のスイッチにBPDUをブロードキャストする頻度を決定します。デフォルトは 2 秒で、範囲は 1 ～ 10 です。
転送遅延タイマー	ポートが転送を開始するまでの、リスニング ステートおよびラーニング ステートが継続する時間を決定します。このタイマーは通常、プロトコルによっては使用されませんが、バックアップとして使用されます。デフォルトは15秒で、範囲は 4 ～ 30 秒です。
最大エージング タイマー	ポートで受信したプロトコル情報がスイッチで保存される時間を決めます。このタイマーは通常、プロトコルによっては使用されませんが、802.1D スパニングツリーと相互に動作するときに使用されます。デフォルトは 20 秒で、範囲は 6 ～ 40 秒です

ポート ロール

Rapid PVST+ では、ポート ロールを割り当て、アクティビティ トポロジを認識することによって、高速収束が行われます。Rapid PVST+ は、802.1D STP に構築され、最高のプライオリティ（最小数値のプライオリティの値）のスイッチがルート ブリッジとして選択されます。Rapid PVST+ により、次のポートのロールの 1 つが個々のポートに割り当てられます。

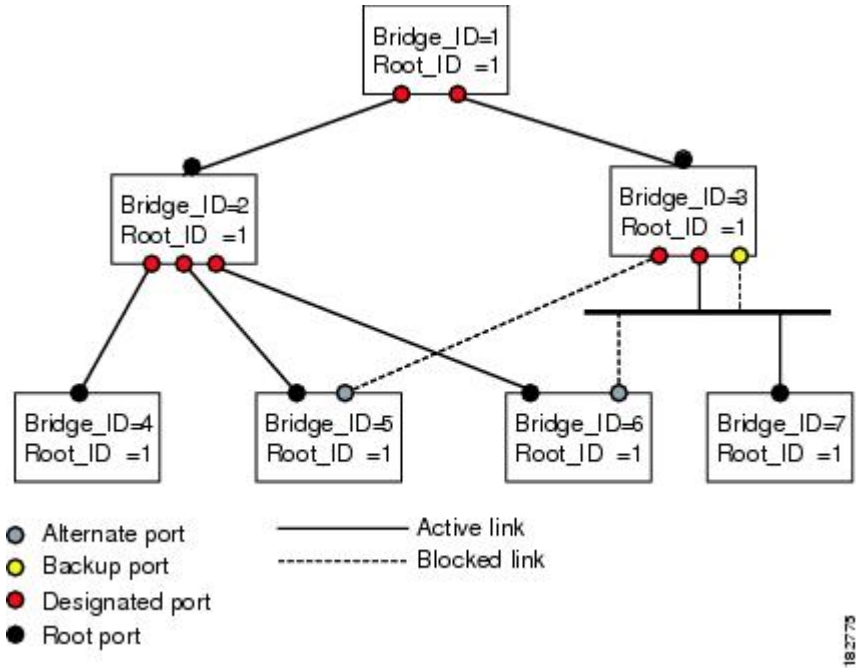
- ルート ポート：スイッチによりパケットがルート ブリッジに転送されるときに、最適のパス（最小コスト）を用意します。

- 指定ポート：指定スイッチに接続します。指定スイッチでは、LAN からルート ブリッジにパケットが転送されるときに、発生するパスコストが最小になります。 指定スイッチがLANに接続するポートのことを指定ポートと呼びます。
- 代替ポート：現在のルート ポートによって用意されているパスに、ルート ブリッジへの代替パスを用意します。 代替ポートにより、トポロジにある別のスイッチへのパスが確保されます。
- バックアップ ポート：指定ポートが提供した、スパニングツリーのリーフに向かうパスのバックアップとして機能します。 バックアップ ポートが存在できるのは、2 つのポートがポイントツーポイント リンクによってループバックで接続されている場合、または 1 つのスイッチに共有 LAN セグメントへの接続が 2 つ以上ある場合です。 バックアップ ポートにより、スイッチに対する別のパスがトポロジ内で確保されます。
- ディセーブル ポート：スパニングツリーの動作においてロールが与えられていません。

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

ルート ポートまたは DP の役割があるポートは、アクティブ トポロジに組み込まれます。 代替ポートまたはバックアップ ポートのロールを持つポートは、アクティブなトポロジから除外されます（次の図を参照）。

図 *11*： ポート ロールをデモンストレーションするトポロジのサンプル



ポート ステート

Rapid PVST+ ポート ステートの概要

プロトコル情報がスイッチド LAN を通過するとき、伝播遅延が生じることがあります。 その結果、スイッチドネットワークのさまざまな時点および場所でトポロジの変化が発生します。 スパニングツリー トポロジで LAN ポートが非伝搬ステートからフォワーディング ステートに直接移行する際、一時的にデータがループすることがあります。 ポートは新しいトポロジ情報がスイッチド LAN 経由で伝播されるまで待機し、それからフレーム転送を開始する必要があります。

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

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

Rapid PVST+ をイネーブルにすると、ソフトウェアのすべてのポート、VLAN、ネットワークは、電源投入時にブロッキング ステートからラーニングの移行ステートに進みます。 各 LAN ポートは、適切に設定されていれば、フォワーディングステートまたはブロッキングステートで安定します。

STP アルゴリズムにより LAN ポートがフォワーディング ステートになると、次の処理が発生します。

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

ブロッキング ステート

ブロッキング ステートにある LAN ポートはフレームを転送しません。

ブロッキング ステートの LAN ポートでは、次の処理が実行されます。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。

- エンド ステーションの場所は、そのアドレス データベースには取り入れません （ブロッキング LAN ポートではラーニングがないため、アドレス データベースは更新されません）。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから受信した BPDU を、処理して送信します。
- ネットワーク管理メッセージを受信して応答します。

ラーニング ステート

ラーニング ステートにある LAN ポートは、フレームの MAC アドレスをラーニングすることによって、フレーム転送の準備をします。 LAN ポートは、ブロッキング ステートからラーニング ステートになります。

ラーニング ステートの LAN ポートでは、次の処理が実行されます。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- エンド ステーションの場所を、そのアドレス データベースに取り入れます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから受信した BPDU を、処理して送信します。
- ネットワーク管理メッセージを受信して応答します。

フォワーディング ステート

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

フォワーディング ステートの LAN ポートでは、次の処理が実行されます。

- 接続セグメントから受信したフレームを転送します。
- 転送用に他のポートからスイッチングされたフレームを転送します。
- エンド ステーションの場所情報を、そのアドレス データベースに取り入れます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから受信した BPDU を処理します。
- ネットワーク管理メッセージを受信して応答します。

ディセーブル ステート

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

ディセーブルの LAN ポートでは、次の処理が実行されます。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- エンド ステーションの場所は、そのアドレス データベースには取り入れません （学習は行われないため、アドレス データベースは更新されません）。
- ネイバーから BPDU を受信しません。
- システム モジュールから送信用の BPDU を受信しません。

ポート ステートの概要

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

表 *4*：アクティブなトポロジのポート ステート

動作ステータス	ポート ステート	ポートがアクティブ トポロジに含まれているか
イネーブル	ブロッキング	No
イネーブル	ラーニング	Yes
イネーブル	フォワーディング	Yes
ディセーブル	ディセーブル	No

ポート ロールの同期

スイッチがいずれかのポートで提案メッセージを受信し、そのポートが新しいルート ポートとして選択されると、Rapid PVST+ は、強制的に、すべての他のポートと新しいルート情報との同期をとります。

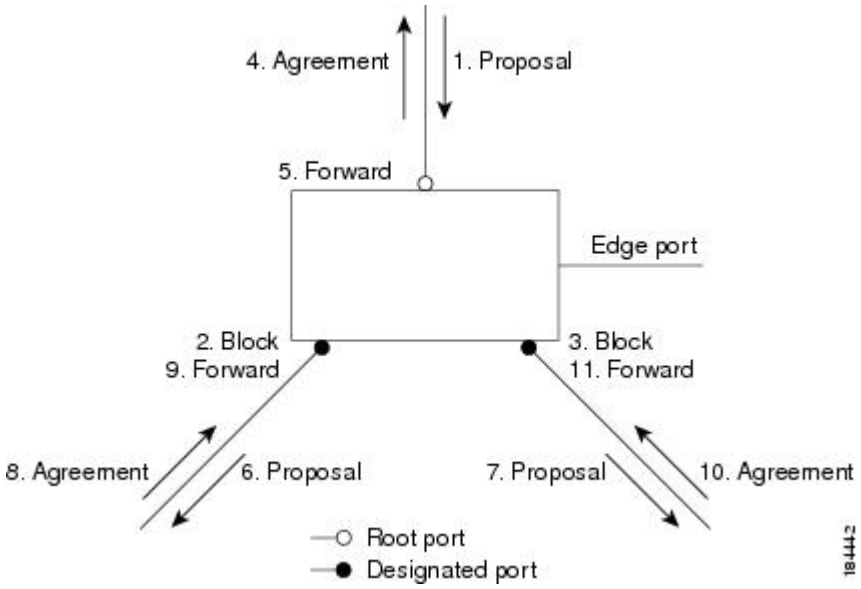
他のすべてのポートが同期化されると、スイッチはルート ポートで受信した優位のルート情報に同期化されます。 次のいずれかが当てはまる場合、スイッチ上の個々のポートで同期がとられます。

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

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

すべてのポートで同期がとられた後で、スイッチから、ルート ポートに対応する指定スイッチへ、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 *12*： 高速コンバージェンス中のイベントのシーケンス



優位 BPDU 情報の処理

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

上位 BPDU がポートで受信されると、Rapid PVST+ は再設定を起動します。 そのポートが新しいルート ポートとして提案、選択されている場合、Rapid PVST+ は残りすべてのポートを同期させます。

受信した BPDU が提案フラグの設定された Rapid PVST+ BPDU の場合、スイッチは残りすべてのポートを同期させたあと、合意メッセージを送信します。 前のポートがブロッキング ステートになるとすぐに、新しいルート ポートがフォワーディング ステートに移行します。

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

下位 BPDU 情報の処理

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

DP は、下位 BPDU を受信すると、独自の情報ですぐに応答します。

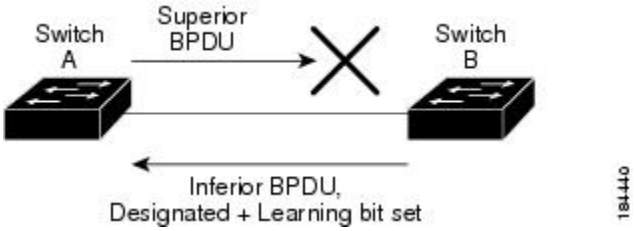
スパニングツリー検証メカニズム

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

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

次の図に、ブリッジング ループ発生の一般的な原因となる単一方向リンク障害を示します。 スイッチAはルートブリッジで、そのBPDUは、スイッチBへのリンク上では失われます。 802.1w規格のBPDUには送信ポートのロールおよびステートが含まれます。 この情報により、送信する上位BPDUに対してスイッチBが反応しないこと、スイッチBはルート ポートではなく指定ポートであることが、スイッチAによって検出できます。 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 *13*： 単一方向リンク障害の検出



ポート コスト

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

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 *5*： 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 コストをポートごとに割り当てます。 トランク ポートでは VLAN ごとにポート コストを割り当てるため、トランク ポート上のすべての VLAN に同じポート コストを設定できます。

ポート プライオリティ

ループが発生し、複数のポートに同じパス コストが割り当てられている場合、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 ポートはフォワーディング ステートに移行するために 2 倍の転送遅延時間を必要とします。

スイッチは、次のように、レガシー 802.1D スイッチと相互動作します。

- 通知：802.1D BPDU とは異なり 802.1w は、TCN BPDU を使用しません。 ただし、802.1D スイッチとの相互運用のため、Cisco NX-OS では、TCN BPDU を処理し、生成します。
- 受信応答：802.1w スイッチでは、802.1D スイッチから指定ポート上に TCN メッセージを受信すると、TCA ビットを設定し、802.1D コンフィギュレーション BPDU で応答します。 ただし、802.1D スイッチに接続されているルート ポートで TC While タイマー（802.1D の TC タイマーと同じ）がアクティブの場合、TCA がセットされたコンフィギュレーション BPDU を受信すると、TC While タイマーはリセットされます。

動作のこの方式は、802.1D スイッチでのみ必要です。 802.1w BPDU では、TCA ビットは設定されません。

- プロトコル移行：802.1D スイッチとの下位互換性のために、802.1w は、802.1D コンフィギュレーション BPDU と TCN BPDU をポートごとに選択的に送信します。

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

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

（注） すべてのスイッチでプロトコルを再ネゴシエーションするには、Rapid PVST+ を再起動する必要があります。

Rapid PVST+ の 802.1s MST との相互運用

Rapid PVST+ は、IEEE 802.1s Multiple Spanning Tree（MST）規格とシームレスに相互運用されます。 ユーザによる設定は不要です。

Rapid PVST+ の設定

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

Rapid PVST+ は VLAN ごとにイネーブルにします。 STP のインスタンスが VLAN ごとに維持されます（STP をディセーブルにした VLAN を除く）。 デフォルトで Rapid PVST+ は、デフォルト VLAN と、作成した各 VLAN でイネーブルになります。

Rapid PVST+ のイネーブル化

スイッチ上で Rapid PVST+ をイネーブルにすると、指定されている VLAN で Rapid PVST+ をイネーブルにする必要があります。

Rapid PVST+ はデフォルトの STP モードです。 MST と Rapid PVST+ は同時には実行できません。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **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+ をイネーブルにするために入力したコマンドは表示されません。

Rapid PVST+ の VLAN ベースのイネーブル化

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **spanning-tree** *vlan-range*	VLAN ごとに Rapid PVST+（デフォルト STP）をイネーブルにします。 *vlan-range* の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。
ステップ 3	switch(config)# **no spanning-tree** *vlan-range*	（任意） 指定 VLAN で Rapid PVST+ をディセーブルにします。 **注意** VLAN のすべてのスイッチおよびブリッジでスパニングツリーがディセーブルになっていない限り、VLAN でスパニングツリーをディセーブルにしないでください。 VLAN の一部のスイッチおよびブリッジでスパニングツリーをディセーブルにして、その他のスイッチおよびブリッジでイネーブルにしておくことはできません。 スパニングツリーをイネーブルにしたスイッチとブリッジに、ネットワークの物理トポロジに関する不完全な情報が含まれることになるため、この処理によって予想外の結果となることがあります。 VLAN 内に物理的なループが存在しないことを保証できる場合以外は、VLAN でスパニングツリーをディセーブルにしないでください。 スパニングツリーは、設定の誤りおよび配線の誤りに対する保護手段として動作します。

次に、VLAN で STP をイネーブルにする例を示します。

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

ルート ブリッジ ID の設定

Rapid PVST+ では、STP のインスタンスはアクティブな VLAN ごとに管理されます。 各 VLAN では、最も小さいブリッジ ID を持つスイッチが VLAN のルート ブリッジになります。

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

spanning-tree vlan *vlan_ID* **root** コマンドを入力すると、各 VLAN 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、最大エージング タイムが自動的に選択されます。これにより、STP 収束の時間が大幅に削減されます。 キーワード **hello-time** を入力すると、自動的に計算された hello タイムを上書きできます。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree vlan** *vlan-range* **root primary** [**diameter** *dia* [**hello-time** *hello-time*]]	ソフトウェア スイッチをプライマリ ルート ブリッジとして設定します。 *vlan-range* の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。*dia* のデフォルトは 7 です。 *hello-time* の範囲は 1 ～ 10 秒で、デフォルト値は 2 秒です。

次の例は、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、最大エージング タイムが自動的に選択されます。これにより、STP コンバージェンスの時間が大幅に削減されます。 キーワード **hello-time** を入力すると、自動的に計算された hello タイムを上書きできます。

複数のスイッチに対して同様に設定すれば、複数のバックアップ ルート ブリッジを設定できます。 プライマリ ルート ブリッジの設定時に使用した値と同じネットワーク直径と hello タイムの値を入力します。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **spanning-tree vlan** *vlan-range* **root secondary** [**diameter** *dia* [**hello-time** *hello-time*]]	ソフトウェア スイッチをセカンダリ ルート ブリッジとして設定します。 *vlan-range* の値は、2 ～ 4094 の範囲です（予約済みの VLAN の値を除く）。 *dia* のデフォルトは 7 です。 *hello-time* の範囲は 1 ～ 10 秒で、デフォルト値は 2 秒です。

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

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

Rapid PVST+ のポート プライオリティの設定

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	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。 （注） これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/QSFP-module/port* になります。
ステップ 3	switch(config-if)# **spanning-tree** [**vlan** *vlan-list*] **port-priority** *priority*	LAN インターフェイスのポート プライオリティを設定します。 *priority* の値は 0 ～ 224 を指定できます。 値が小さいほどプライオリティが高いことを示します。

	コマンドまたはアクション	目的
		プライオリティ値は、0、32、64、96、128、160、192、224 です。 その他すべての値は拒否されます。 デフォルト値は 128 です。

次に、イーサネット インターフェイスのアクセス ポート プライオリティを設定する例を示します。

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

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

Rapid PVST+ パスコスト方式およびポート コストの設定

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

（注） Rapid PVST+ モードでは、ショート型またはロング型のいずれかのパスコスト方式を使用できます。この方式は、インターフェイスまたはコンフィギュレーション サブモードのいずれかで設定できます。デフォルトのパスコスト方式はショート型です。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **spanning-tree pathcost method** {**long** | **short**}	Rapid PVST+ パスコスト計算に使用される方式を選択します。 デフォルト方式は short 型です。
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。 （注） これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/QSFP-module/port* になります。
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。ポート コスト値には、パスコスト計算方式に応じて、次の値を指定できます。

	コマンドまたはアクション	目的
		• 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。 デフォルトの **auto** では、パスコスト計算方式およびメディア速度に基づいてポート コストが設定されます。

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

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

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

VLAN の Rapid PVST+ のブリッジ プライオリティの設定

VLAN の Rapid PVST+ のブリッジ プライオリティを設定できます。

（注） この設定を使用するときは注意が必要です。 ほとんどの場合、プライマリ ルートとセカンダリ ルートを設定して、ブリッジ プライオリティを変更することを推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **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

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

次に、VLAN の hello タイムを設定する例を示します。

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

VLAN の Rapid PVST+ の転送遅延時間の設定

Rapid PVST+ の使用時は、VLAN ごとに転送遅延時間を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **spanning-tree vlan** *vlan-range* **forward-time** *forward-time*	VLAN の転送遅延時間を設定します。 転送遅延時間の値の範囲は 4 ～ 30 秒で、デフォルトは 15 秒です。

次に、VLAN の転送遅延時間を設定する例を示します。

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

VLAN の Rapid PVST+ の最大エージング タイムの設定

Rapid PVST+ の使用時は、VLAN ごとに最大エージング タイムを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree vlan** *vlan-range* **max-age** *max-age*	VLAN の最大エージング タイムを設定します。 最大エージング タイムの値の範囲は 6 ～ 40 秒で、デフォルトは 20 秒です。

次に、VLAN の最大エージング タイムを設定する例を示します。

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

リンク タイプの設定

Rapid の接続性（802.1w 規格）は、ポイントツーポイントのリンク上でのみ確立されます。 リンク タイプは、デフォルトでは、インターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続であると見なされ、半二重ポートは共有接続であると見なされます。

リモート スイッチの 1 つのポートに、ポイントツーポイントで物理的に接続されている半二重リンクがある場合、リンク タイプのデフォルト設定を上書きし、高速移行をイネーブルにできます。

リンクを共有に設定すると、STP は 802.1D に戻ります。

手順

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

	コマンドまたはアクション	目的
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。 （注） これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/QSFP-module/port* になります。
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 リンクまたは共有リンクに設定します。 デフォルト値はスイッチ接続から読み取られ、半二重リンクは共有、全二重リンクはポイントツーポイントです。 リンク タイプが共有の場合、STP は 802.1D に戻ります。 デフォルトは auto で、インターフェイスのデュプレックス設定に基づいてリンク タイプが設定されます。

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。

次に、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、次のコマンドを使用します。

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 7 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，91 ページ
- MST の設定，100 ページ
- MST の設定の確認，119 ページ

MST について

MST の概要

（注） このマニュアルでは、IEEE 802.1w および IEEE 802.1s を指す用語として、「スパニングツリー」を使用します。 IEEE 802.1D STP について説明している箇所では、802.1D と明記します。

MST は、複数の VLAN を 1 つのスパニングツリー インスタンスにマップします。各インスタンスのスパニングツリー トポロジは、他のスパニングツリー インスタンスの影響を受けません。このアーキテクチャでは、データ トラフィックに対して複数のフォワーディング パスがあり、ロードバランシングが可能です。これによって、非常に多数の VLAN をサポートする際に必要な STP インスタンスの数を削減できます。

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

MST の使用中は、MAC アドレスの削減が常にイネーブルに設定されます。 この機能はディセーブルにはできません。

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

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

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

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

MST リージョン

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

同じ MST 設定の相互接続スイッチの集まりが MST リージョンです。 MST リージョンは、同じ MST 設定で MST ブリッジのグループとリンクされます。

MST 設定により、各スイッチが属する MST リージョンが制御されます。 この設定には、リージョンの名前、バージョン番号、MST VLAN とインスタンスの割り当てマップが含まれます。

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

各リージョンは、最大 65 の MST インスタンス（MSTI）までサポートします。 インスタンスは、1 ～ 4094 の範囲の任意の番号によって識別されます。 インスタンス 0 は、特別なインスタンスである IST 用に予約されています。 VLAN は、一度に 1 つの MST インスタンスに対してのみ割り当てることができます。

MST リージョンは、隣接の MST リージョン、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。

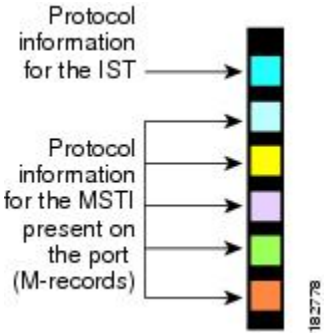
（注） ネットワークを、非常に多数のリージョンに分けることは推奨しません。

MST BPDU

1 つのリージョンに含まれる MST BPDU は 1 つだけで、その BPDU により、リージョン内の各 MSTI について M レコードが保持されます（次の図を参照）。 IST だけが MST リージョンの BPDU を送信します。すべての M レコードは、IST が送信する 1 つの BPDU でカプセル化されていま

す。 MST BPDU にはすべてのインスタンスに関する情報が保持されるため、MSTI をサポートするために処理する必要がある BPDU の数は、非常に少なくなります。

図 *14*： ***MSTI の M レコードが含まれる MST BPDU***



MST 設定情報

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

MST 設定の次の 3 つのパラメータを設定できます。

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

（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関連付けられます。最初（0）と最後（4095）の要素は 0 に設定されています。 要素番号 X の値は、VLAN X がマッピングされるインスタンスを表します。

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 をそのリージョンに受け入れます。 設定属性が 1 つでも異なっていると、MST ブリッジでは、BPDU が別の MST リージョンのものであると見なされます。

IST、CIST、CST

IST、CIST、CST の概要

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

- IST は、MST リージョンで実行されるスパニングツリーです。

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

インスタンス 0 は、IST という、リージョンの特殊インスタンスです。 IST は、すべてのポートに必ず存在します。IST（インスタンス 0）は削除できません。デフォルトでは、すべての VLAN が IST に割り当てられています。 その他の MST インスタンスはすべて 1 ～ 4094 まで番号が付けられます。

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

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

MSTI は、リージョンに対してローカルです。たとえば、リージョン A とリージョン B が相互接続されている場合でも、リージョン A にある MSTI 9 は、リージョン B にある MSTI 9 には依存しません。

- CST は、MST リージョンと、ネットワーク上で実行されている可能性がある 802.1D および 802.1w STP のインスタンスを相互接続します。 CST は、ブリッジ型ネットワーク全体で 1 つ存在する STP インスタンスで、すべての MST リージョン、802.1w インスタンスおよび 802.1D インスタンスを含みます。
- CIST は、各 MST リージョンにある IST の集まりです。 CIST は、MST リージョン内部の IST や、MST リージョン外部の CST と同じです。

MST リージョンで計算されるスパニングツリーは、スイッチ ドメイン全体を含んだ CST 内のサブツリーとして認識されます。 CIST は、802.1w、802.1s、802.1D の各規格をサポートするスイッチで実行されているスパニングツリー アルゴリズムによって形成されています。 MST リージョン内の CIST は、リージョン外の CST と同じです。

MST リージョン内でのスパニングツリーの動作

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

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

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

MST リージョン内のすべてのスイッチが同じ CIST リージョナル ルートを承認する必要があります。 リージョン内にある任意の 2 つのスイッチは、共通 CIST リージョナル ルートに収束する場合、MSTI に対するポート ロールのみを同期します。

MST リージョン間のスパニングツリー動作

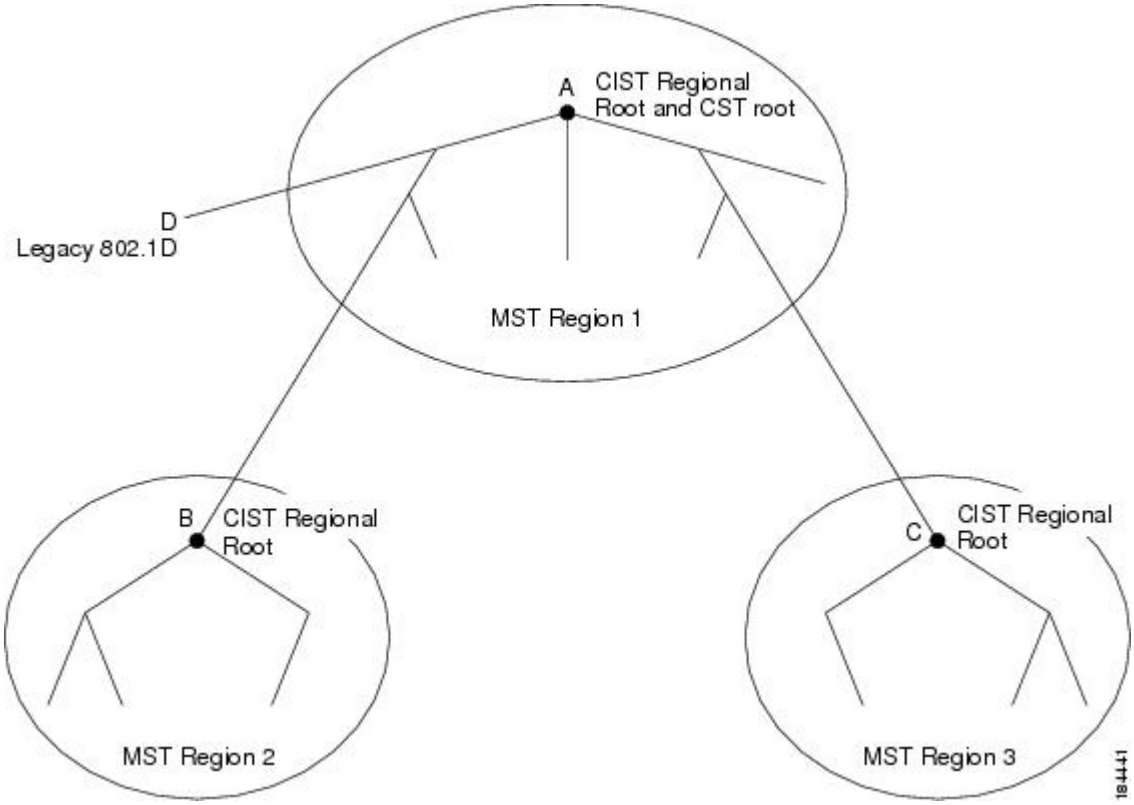
ネットワーク内に複数のリージョン、または 802.1 w や 802.1D STP インスタンスがある場合、MST はネットワーク内のすべての MST リージョン、すべての 802.1w と 802.1D STP スイッチを含む CST を確立して、維持します。 MSTI は、リージョンの境界で IST と結合して CST になります。

IST は、リージョン内のすべての MST スイッチを接続し、スイッチ ドメイン全体を含んだ CIST 内のサブツリーとして認識されます。 サブツリーのルートは CIST リージョナル ルートです。 MST リージョンは、隣接する STP スイッチや MST リージョンからは仮想スイッチとして認識されます。

次の図に、3 つの MST リージョンと 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 *15*： ***MST*** リージョン、***CIST*** リージョナル ルート、***CST*** ルート



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

MST スイッチは、802.1D 専用スイッチと通信する場合、バージョン 3 BPDU または 802.1D STP BPDU を使用します。 MST スイッチは、MST スイッチと通信する場合、MST BPDU を使用します。

MST 用語

MSTの命名規則には、内部パラメータまたはリージョナルパラメータの識別情報が含まれます。これらのパラメータはMSTリージョン内だけで使用され、ネットワーク全体で使用される外部パラメータと比較されます。 CIST だけがネットワーク全体に広がるスパニングツリー インスタン

スなので、CIST パラメータだけに外部修飾子が必要になり、修飾子または領域修飾子は不要です。 MST 用語を次に示します。

- CIST ルートは CIST のルート ブリッジで、ネットワーク全体にまたがる一意のインスタンスです。
- CIST 外部ルート パス コストは、CIST ルートまでのコストです。 このコストは MST リージョン内で変化しません。 MST リージョンは、CIST に対する唯一のスイッチのように見えます。 CIST 外部ルート パス コストは、これらの仮想スイッチとリージョンに属していないスイッチ間を計算して出したルート パス コストです。
- CIST ルートがリージョン内にある場合、CIST リージョナル ルートが CIST ルートになります。 または、CIST リージョナル ルートがそのリージョンで CIST ルートに最も近いスイッチになります。 CIST リージョナル ルートは、IST のルート ブリッジとして動作します。
- CIST 内部ルート パス コストは、リージョン内の CIST リージョナル ルートまでのコストです。 このコストは IST（インスタンス 0）のみに関係します。

ホップ カウント

MST リージョン内の STP トポロジを計算する場合、MST はコンフィギュレーション BPDU のメッセージ有効期間と最大エージング タイムの情報は使用しません。 代わりに、ルートへのパス コストと、IP の存続可能時間（TTL）メカニズムに類似したホップ カウント メカニズムを使用します。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用することにより、リージョン内の最大ホップを設定し、その値をリージョン内の IST インスタンスとすべての MST インスタンスに適用できます。

ホップ カウントを設定すると、メッセージ エージ情報を設定するのと同様の結果が得られます（再構成の開始時期を決定します）。 インスタンスのルート ブリッジは、コストが 0 でホップ カウントが最大値に設定された BPDU（M レコード）を常に送信します。 スイッチがこの BPDU を受信すると、受信 BPDU の残存ホップ カウントから 1 だけ差し引いた値を残存ホップ カウントとする BPDU を生成し、これを伝播します。 このホップ カウントが 0 になると、スイッチはその BPDU を廃棄し、ポート用に維持されていた情報を期限切れにします。

BPDU の 802,1w 部分に格納されているメッセージ有効期間および最大エージング タイムの情報は、リージョン全体で同じです（IST の場合のみ）。同じ値が、境界にあるリージョンの指定ポートによって伝播されます。

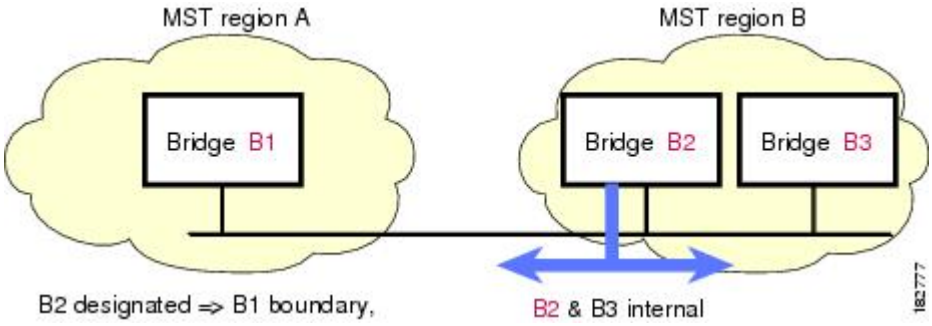
スイッチがスパニングツリー設定メッセージを受信せずに再設定を試行するまで待機する秒数として最大エージング タイムを設定します。

境界ポート

境界ポートは、あるリージョンを別のリージョンに接続するポートです。 指定ポートは、STP ブリッジを検出するか、設定が異なる MST ブリッジまたは Rapid PVST+ ブリッジから合意提案を受信すると、境界にあることを認識します。 この定義により、リージョンの内部にある 2 つのポー

トが、異なるリージョンに属す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 *16*： ***MST*** 境界ポート



境界では、MST ポートのロールは問題ではなく、そのステートは強制的に IST ポート ステートと同じに設定されます。 境界フラグがポートに対してオンに設定されている場合、MST ポートのロールの選択処理では、ポート ロールが境界に割り当てられ、同じステートが IST ポートのステートとして割り当てられます。 境界にある IST ポートでは、バックアップ ポート ロール以外のすべてのポート ロールを引き継ぐことができます。

スパニングツリー検証メカニズム

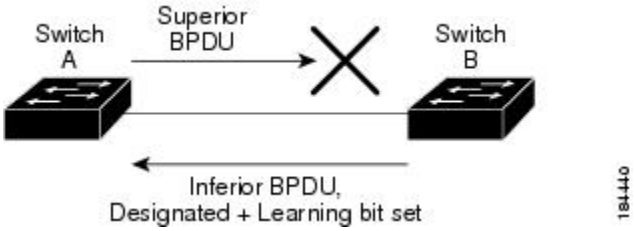
現在、この機能は、IEEE MST 規格にはありませんが、規格準拠の実装に含まれています。 ソフトウェアを使用することで、受信した BPDU からポートの役割とステートの一貫性を確認し、単一方向リンクが失敗してブリッジ処理のループを引き起こしていないかどうかを検証できます。

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

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

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

図 *17*： 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 では常にロング パスコスト計算方式が使用されるため、有効値は 1 ～ 200,000,000 です。

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

IEEE 802.1D との相互運用性

MST が実行されるスイッチでは、802.1D STP スイッチとの相互運用を可能にする、内蔵プロトコル移行機能がサポートされます。 このスイッチで、802.1D コンフィギュレーション BPDU（プロトコル バージョンが 0 に設定されている BPDU）を受信する場合、そのポート上の 802.1D BPDU のみが送信されます。 さらに、MST スイッチでは、802.1D BPDU、異なるリージョンに関連付けられている MST BPDU（バージョン 3）、または 802.1w BPDU（バージョン 2）を受信するときに、ポートがリージョンの境界にあることを検出できます。

ただし、スイッチは、802.1D BPDU を受信しなくなった場合でも、自動的には MSTP モードには戻りません。これは、802.1D スイッチが指定スイッチではない場合、802.1D スイッチがリンクか

ら削除されたかどうかを検出できないためです。 さらにスイッチは、接続先スイッチがリージョンに加入した場合であっても、引き続きポートに境界の役割を指定する可能性があります。

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

リンク上にあるすべての Rapid PVST+ スイッチ（およびすべての 8021.D STP スイッチ）では、MST BPDU を 802.1w BPDU の場合と同様に処理できます。 MST スイッチでは、境界ポート上にある、バージョン 0 コンフィギュレーションおよびトポロジ変更通知（TCN）BPDU、またはバージョン 3 MST BPDU のいずれかを送信できます。 境界ポートは LAN に接続され、その指定スイッチは、単一スパニングツリー スイッチか、MST 設定が異なるスイッチのいずれかです。

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

Rapid PVST+ の相互運用性と PVST シミュレーションについて

MST は、ユーザが設定しなくても、Rapid PVST+ と相互運用できます。 PVST シミュレーション機能により、このシームレスな相互運用性がイネーブルにされます。

（注） PVST シミュレーションは、デフォルトでイネーブルになっています。 つまり、スイッチ上のすべてのインターフェイスは、デフォルトで、MST と Rapid PVST+ との間で相互動作します。

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

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

MST の設定

MST 設定時の注意事項

MST を設定する場合は、次の注意事項に従ってください。

- プライベート VLAN を操作するときには、**private-vlan synchronize** コマンドを使用して、プライマリ VLAN として、セカンダリ VLAN を同じ MST インスタンスにマッピングします。

- MST コンフィギュレーション モードの場合、次の注意事項が適用されます。
  - 各コマンド参照行により、保留中のリージョン設定が作成されます。
  - 保留中のリージョン設定により、現在のリージョン設定が開始されます。
  - 変更を一切コミットすることなく MST コンフィギュレーション モードを終了するには、**abort** コマンドを入力します。
  - モードの終了前に行った変更内容をすべてコミットして MST コンフィギュレーション モードを終了するには、**exit** コマンドを入力します。

MST のイネーブル化

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

注意 スパニングツリー モードを変更すると、変更前のモードのスパニングツリー インスタンスがすべて停止されて新しいモードで起動されるため、トラフィックが中断する場合があります。また、仮想ポート チャネル（vPC）ピア スイッチに 2 種類の異なるスパニングツリー モードを持つことは不整合であるため、この動作は中断を伴います。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch# **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 3	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 4	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 をイネーブルにするために入力したコマンドは表示されません。

MST コンフィギュレーション モードの開始

スイッチ上で、MSTの名前、VLANからインスタンスへのマッピング、MSTリビジョン番号を設定するには、MST コンフィギュレーション モードを開始します。

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

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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 • 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**	変更をコミットして終了、または変更をコミットせずに終了します。 • **exit** コマンドは、すべての変更をコミットして MST コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
		• **abort** コマンドは、変更をコミットせずに MST コンフィギュレーション モードを終了します。
ステップ 4	switch(config)# **no spanning-tree mst configuration**	（任意） MST リージョン設定を次のデフォルト値に戻します。 • 領域名は空の文字列になります。 • VLAN は MSTI にマッピングされません（すべての VLAN は CIST インスタンスにマッピングされます）。 • リビジョン番号は 0 です。

MST の名前の指定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **spanning-tree mst configuration**	MST コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-mst)# **name** *name*	MST リージョンの名前を指定します。 *name* ストリングには 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 リージョンの名前の設定方法を示しています。

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

MST 設定のリビジョン番号の指定

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

手順

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

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

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

MST リージョンでの設定の指定

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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。 MST インスタンスに VLAN をマッピングする場合、マッピングはインクリメンタルに行われ、コマンドで指定された VLAN がすでにマッピング済みの VLAN に対して追加または削除されます。 VLAN 範囲を指定する場合は、ハイフンを使用します。たとえば、**instance 1 vlan 1-63** とコマンドを入力すると、MST インスタンス 1 に VLAN 1 ～ 63 がマッピングされます。 複数の VLAN を指定する場合はカンマで区切ります。たとえば、**instance 1 vlan 10, 20, 30** と指定すると、MST インスタンス 1 に VLAN 10、20、および 30 がマッピングされます。
ステップ 4	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 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 リージョン設定に戻すには、**no spanning-tree mst configuration** コンフィギュレーション コマンドを入力します。
- VLAN インスタンス マッピングをデフォルトの設定に戻すには、**no instance** *instance-id* **vlan** *vlan-range* MST コンフィギュレーション コマンドを使用します。

- デフォルトの名前に戻すには、**no name** MST コンフィギュレーション コマンドを入力します。
- デフォルトのリビジョン番号に戻すには、**no revision** MST コンフィギュレーション コマンドを入力します。
- Rapid PVST+ を再度イネーブルにするには、**no spanning-tree mode** または **spanning-tree mode rapid-pvst** 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、リージョンに region1 という名前を付けて、設定リビジョンを 1 に設定し、保留中の設定を表示し、変更を適用してグローバルコンフィギュレーションモードに戻る方法を示しています。

```
switch(config)# spanning-tree mst configuration
switch(config-mst)# instance 1 vlan 10-20
switch(config-mst)# name region1
switch(config-mst)# revision 1
switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instances configured 2
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------
```

VLAN から MST インスタンスへのマッピングとマッピング解除

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

（注） MSTI はディセーブルにできません。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **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。

	コマンドまたはアクション	目的
		• *instance-id* の範囲は 1 ～ 4094 です。 インスタンス 0 は、各 MST リージョンでの IST 用に予約されています。 • *vlan-range* の範囲は 1 ～ 4094 です。 VLAN を MSTI にマッピングすると、マッピングは差分で実行され、コマンドで指定された VLAN が、以前マッピングされた VLAN に追加または VLAN から削除されます。
ステップ 4	switch(config-mst)# **no instance** *instance-id* **vlan** *vlan-range*	指定したインスタンスを削除し、VLAN を、デフォルト MSTI である CIST に戻します。

次の例は、VLAN 200 を MSTI 3 にマッピングする方法を示しています。

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

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **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**	すべてのプライベート VLAN の関連プライマリ VLAN と同じ MSTI にすべてのセカンダリ VLAN を自動的にマッピングします。

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

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

ルート ブリッジの設定

スイッチは、ルート ブリッジになるよう設定できます。

（注） 各 MSTI のルート ブリッジは、バックボーン スイッチまたはディストリビューション スイッチである必要があります。 アクセス スイッチは、スパニングツリーのプライマリ ルート ブリッジとして設定しないでください。

MSTI 0（または IST）でのみ使用可能な **diameter** キーワードを入力し、ネットワーク直径（ネットワーク内の任意の 2 つのエンド ステーション間での最大ホップ数）を指定します。 ネットワークの直径を指定すると、その直径のネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムをスイッチが自動的に設定するので、コンバージェンスの所要時間を大幅に短縮できます。 **hello** キーワードを入力すると、自動的に計算された hello タイムを上書きできます。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **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

	コマンドまたはアクション	目的
		は 7 です。 このキーワードは、MST インスタンス 0 にだけ使用できます。 • hello-time *seconds* には、ルート ブリッジによって生成された設定メッセージの間隔を秒単位で指定します。 有効な範囲は 1 ～ 10 秒で、デフォルトは 2 秒です。
ステップ 3	switch(config)# **no spanning-tree mst** *instance-id* **root**	（任意） スイッチのプライオリティ、範囲、hello タイムをデフォルト値に戻します。

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

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

セカンダリ ルート ブリッジの設定

このコマンドは、複数のスイッチに対して実行し、複数のバックアップルートブリッジを設定できます。 **spanning-tree mst root primary** コンフィギュレーション コマンドでプライマリ ルート ブリッジを設定したときに使用したものと同じネットワーク直径と hello タイムの値を入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]]	次のように、セカンダリ ルート ブリッジとしてスイッチを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 有効な範囲は 1 ～ 4094 です。 • diameter *net-diameter* には、2 つのエンド ステーション間にホップの最大数を設定します。 デフォルトは 7 です。 このキーワードは、MST インスタンス 0 にだけ使用できます。

	コマンドまたはアクション	目的
		• 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

	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。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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。

	コマンドまたはアクション	目的
		• *priority* の範囲は 0 ～ 224 で、32 ずつ増加します。デフォルトは 128 です。 値が小さいほど、プライオリティが高いことを示します。 プライオリティ値は、0、32、64、96、128、160、192、224 です。 システムでは、他のすべての値が拒否されます。

次の例は、イーサネット ポート 3/1 で MSTI 3 の MST インターフェイス ポート プライオリティを 64 に設定する方法を示しています。

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

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

ポート コストの設定

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

（注） MST はロング パスコスト計算方式を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **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。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。

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

次の例は、イーサネット ポート 3/1 で MSTI 4 の MST インターフェイス ポート コストを設定する方法を示しています。

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

スイッチのプライオリティの設定

MSTインスタンスのスイッチのプライオリティは、指定されたポートがルートブリッジとして選択されるように設定できます。

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

手順

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

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **spanning-tree mst** *instance-id* **priority** *priority-value*	次のように、スイッチのプライオリティを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。 有効な範囲は 1 ～ 4094 です。 • priority の範囲は 0 ～ 61440 で、4096 ずつ増加します。 デフォルト値は 32768 です。 小さい値を設定すると、スイッチがルート スイッチとして選択される可能性が高くなります。 プライオリティ値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。 システムでは、他のすべての値が拒否されます。

次の例は、MSTI 5 のブリッジのプライオリティを 4096 に設定する方法を示しています。

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

hello タイムの設定

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

（注） このコマンドの使用には注意してください。 ほとんどの場合、hello タイムを変更するには、**spanning-tree mst** *instance-id* **root primary** および **spanning-tree mst** *instance-id* **root secondary** コンフィギュレーション コマンドの使用を推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree mst hello-time** *seconds*	すべての MST インスタンスについて、hello タイムを設定します。 hello タイムは、ルート ブリッジが設定メッセージを生成する間隔です。 これらのメッセー

	コマンドまたはアクション	目的
		ジは、スイッチがアクティブであることを意味します。 *seconds* の範囲は 1 ～ 10 で、デフォルトは 2 秒です。

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

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

転送遅延時間の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree mst forward-time** *seconds*	すべての MST インスタンスについて、転送時間を設定します。 転送遅延は、スパニングツリーブロッキング ステートとラーニング ステートからフォワーディング ステートに変更する前に、ポートが待つ秒数です。 *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
```

最大エージング タイムの設定

最大エージング 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エージング タイマーを設定できます（最大エージング タイムは IST にのみ適用されます）。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **spanning-tree mst max-age** *seconds*	すべての MST インスタンスについて、最大エージング タイムを設定します。 最大エージング タイムは、スイッチが、再設定を試行する前に、スパニングツリー設定メッセージの受信を待つ秒数です。 *seconds* の範囲は 6 ～ 40 で、デフォルトは 20 秒です。

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

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

最大ホップ カウントの設定

MST では、IST リージョナル ルートへのパス コストと、IP の存続可能時間（TTL）メカニズムに類似したホップ カウント メカニズムが使用されます。 リージョン内の最大ホップを設定し、それを、そのリージョンにある IST とすべての MST インスタンスに適用できます。 ホップ カウントを設定すると、メッセージ エージ情報を設定するのと同様の結果が得られます（再構成の開始時期を決定します）。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **spanning-tree mst max-hops** *hop-count*	BPDU を廃棄してポート用に保持していた情報を期限切れにするまでの、リージョンでのホップ数を設定します。 *hop-count* の範囲は 1 ～ 255 で、デフォルト値は 20 ホップです。

次の例は、最大ホップ カウントを 40 に設定する方法を示しています。

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

PVST シミュレーションのグローバル設定

この自動機能は、グローバルまたはポートごとにブロックできます。 グローバルコマンドを入力すると、インターフェイス コマンド モードの実行中に、スイッチ全体の PVST シミュレーション設定を変更できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no 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。 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。

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

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

ポートごとの PVST シミュレーションの設定

MST は、Rapid PVST+ とシームレスに相互動作します。 ただし、デフォルト STP モードとして MST が実行されていないスイッチへの誤った接続を防ぐため、この自動機能をディセーブルにする必要が生じる場合があります。 Rapid PVST+ シミュレーションをディセーブルにした場合、MST がイネーブルなポートが Rapid PVST+ がイネーブルなポートに接続されていることが検出されると、MST がイネーブルなポートは、ブロッキング ステートに移行します。 このポートは、BPDU の受信が停止されるまで、一貫性のないステートのままになり、それから、ポートは、通常の STP 送信プロセスに戻ります。

この自動機能は、グローバルまたはポートごとにブロックできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {{*type slot*/*port*} | {**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。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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+ のシームレスな相互運用を再びイネーブルにします。
ステップ 5	switch(config-if)# **no spanning-tree mst simulate pvst**	インターフェイスを、**spanning-tree mst simulate pvst global** コマンドを使用して、設定したスイッチ全体で MST と Rapid PVST+ との間で相互動作するよう設定します。

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

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

リンク タイプの設定

Rapid の接続性（802.1w 規格）は、ポイントツーポイントのリンク上でのみ確立されます。 リンク タイプは、デフォルトでは、インターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続であると見なされ、半二重ポートは共有接続であると見なされます。

リモート スイッチの 1 つのポートに、ポイントツーポイントで物理的に接続されている半二重リンクがある場合、リンク タイプのデフォルト設定を上書きし、高速移行をイネーブルにできます。

リンクを共有に設定すると、STP は 802.1D に戻されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 （注） これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/QSFP-module/port* になります。
ステップ 3	switch(config-if)# **spanning-tree link-type** {**auto** | **point-to-point** | **shared**}	リンク タイプを、ポイントツーポイントまたは共有に設定します。 システムでは、スイッチ接続からデフォルト値を読み込みます。 半二重リンクは共有で、全二重リンクはポイントツーポイントです。 リンク タイプが共有の場合、STP は 802.1D に戻ります。 デフォルトは auto で、インターフェイスのデュプレックス設定に基づいてリンク タイプが設定されます。

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

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

プロトコルの再開

MST ブリッジでは、レガシー BPDU または異なるリージョンに関連付けられている MST BPDU を受信するときに、ポートがリージョンの境界にあることを検出できます。 ただし、STP プロトコルの移行では、レガシー スイッチが指定スイッチではない場合、IEEE 802.1D のみが実行されているレガシー スイッチが、リンクから削除されたかどうかを認識できません。 スイッチ全体または指定したインターフェイスでプロトコル ネゴシエーションを再開する（強制的に隣接スイッチと再ネゴシエーションさせる）には、このコマンドを入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **clear spanning-tree detected-protocol** [**interface** *interface* [*interface-num* | *port-channel*]]	スイッチ全体または指定したインターフェイスで、MST を再開します。

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

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

MST の設定の確認

MST の設定情報を表示するには、次のコマンドを使用します。

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

次に、現在の MST 設定を表示する方法を示します。

```
switch# show spanning-tree mst configuration
% Switch is not in mst mode
Name      [mist-attempt]
Revision  1     Instances configured 2
Instance  Vlans mapped
--------  -------------------------------------------------------------------
0         1-12,14-41,43-4094
1         13,42
```

第 8 章

STP 拡張機能の設定

この章の内容は、次のとおりです。

- STP 拡張機能, 121 ページ

STP 拡張機能

シスコでは、スパニングツリー プロトコル（STP）に、収束をより効率的に行うための拡張機能を追加しました。 場合によっては、同様の機能が IEEE 802.1w 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、RPVST+ およびマルチ スパニングツリー プロトコル（MST）と組み合わせて使用できます。

使用可能な拡張機能には、スパニングツリー ポート タイプ、Bridge Assurance、Bridge Protocol Data Units（BPDU：ブリッジ プロトコル データ ユニット）ガード、BPDU フィルタリング、ループ ガード、ルート ガードがあります。 これらの機能の大部分は、グローバルに、または指定インターフェイスに適用できます。

（注） このマニュアルでは、IEEE 802.1w および IEEE 802.1s を指す用語として、「スパニングツリー」を使用します。 IEEE 802.1D STP について説明している箇所では、802.1D と明記します。

STP 拡張機能について

STP ポート タイプの概要

スパニングツリー ポートは、エッジ ポート、ネットワーク ポート、または標準ポートとして構成できます。 ポートは、ある一時点において、これらのうちいずれか 1 つの状態をとります。 デフォルトのスパニングツリー ポート タイプは「標準」です。 インターフェイスが接続されてい

るデバイスのタイプによって、スパニングツリーポートを上記いずれかのポートタイプに設定できます。

スパニングツリー エッジ ポート

エッジ ポートは、ホストに接続されるポートであり、アクセス ポートとトランク ポートのどちらにもなります。 エッジ ポート インターフェイスは、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します （この直接移行動作は、以前は、シスコ独自の機能 PortFast として設定していました）。

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

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

スパニングツリー ネットワーク ポート

ネットワーク ポートは、スイッチまたはブリッジだけに接続されます。 Bridge Assurance がグローバルにイネーブルになっているときに、ネットワーク ポートとしてポートを設定すると、そのポート上で Bridge Assurance がイネーブルになります。

（注） ホストまたは他のエッジ デバイスに接続されているポートを誤ってスパニングツリー ネットワーク ポートとして設定すると、それらのポートは自動的にブロッキング ステートに移行します。

スパニングツリー標準ポート

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

デフォルトのスパニングツリー インターフェイスは標準ポートです。

Bridge Assurance の概要

Bridge Assurance を使用すると、ネットワーク内でブリッジング ループの原因となる問題の発生を防ぐことができます。 具体的には、単方向リンク障害や、スパニングツリーアルゴリズムを実行しなくなってもデータ トラフィックの転送を続けているデバイスなどからネットワークを保護できます。

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

Bridge Assurance はデフォルトでイネーブルになっており、グローバル単位でだけディセーブルにできます。 また、Bridge Assurance をイネーブルにできるのは、ポイントツーポイント リンクに接続されたスパニングツリー ネットワーク ポートだけです。 Bridge Assurance は必ず、リンクの両端でイネーブルにする必要があります。

Bridge Assurance をイネーブルにすると、BPDU が hello タイムごとに、動作中のすべてのネットワーク ポート（代替ポートとバックアップ ポートを含む）に送出されます。 所定の期間 BPDU を受信しないポートは、ブロッキング ステートに移行し、ルート ポートの決定に使用されなくなります。 BPDU を再度受信するようになると、そのポートで通常のスパニングツリー状態遷移が再開されます。

BPDU ガードの概要

BPDU ガードをイネーブルにすると、BPDU を受信したときにそのインターフェイスがシャットダウンされます。

BPDU ガードはインターフェイス レベルで設定できます。 BPDU ガードをインターフェイス レベルで設定すると、そのポートはポート タイプ設定にかかわらず BPDU を受信するとすぐにシャットダウンされます。

BPDU ガードをグローバル単位で設定すると、動作中のスパニングツリー エッジ ポート上だけで有効となります。 正しい設定では、LAN エッジ インターフェイスは BPDU を受信しません。エッジ インターフェイスが BPDU を受信すると、無効な設定（未認証のホストまたはスイッチへの接続など）を知らせるシグナルが送信されます。 BPDU ガードをグローバル単位でイネーブルにすると、BPDU を受信したすべてのスパニングツリー エッジ ポートがシャットダウンされます。

BPDU ガードは、無効な設定があると確実に応答を返します。無効な設定をした場合は、当該 LAN インターフェイスを手動でサービス状態に戻す必要があるからです。

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

BPDU フィルタリングの概要

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

グローバルに設定された BPDU フィルタリングは、動作中のすべてのスパニングツリー エッジ ポートに適用されます。エッジポートはホストだけに接続してください。ホストでは通常、BPDU は破棄されます。 動作中のスパニングツリー エッジ ポートが BPDU を受信すると、ただちに標

準のスパニングツリー ポート タイプに戻り、通常のポート状態遷移が行われます。 その場合、当該ポートで BPDU フィルタリングはディセーブルとなり、スパニングツリーによって、同ポートでの BPDU の送信が再開されます。

BPDU フィルタリングは、インターフェイスごとに設定することもできます。 BPDU フィルタリングを特定のポートに明示的に設定すると、そのポートは BPDU を送出しなくなり、受信した BPDU をすべてドロップします。 特定のインターフェイスを設定することによって、個々のポート上のグローバルな BPDU フィルタリングの設定を実質的に上書きできます。 このようにインターフェイスに対して実行された BPDU フィルタリングは、そのインターフェイスがトランキングであるか否かに関係なく、インターフェイス全体に適用されます。

注意 BPDU フィルタリングをインターフェイスごとに設定するときは注意が必要です。 ホストに接続されていないポートに BPDU フィルタリングを明示的に設定すると、ブリッジング ループに陥る可能性があります。 というのは、そうしたポートは受信した BPDU をすべて無視して、フォワーディング ステートに移行するからです。

ポートがデフォルトで BPDU フィルタリングに設定されていなければ、エッジ設定によって BPDU フィルタリングが影響を受けることはありません。 次の表に、すべての BPDU フィルタリングの組み合わせを示します。

表 *6*： *BPDU* フィルタリングの設定

ポート単位の BPDU フィルタリングの設定	グローバルな BPDU フィルタリングの設定	STP エッジ ポート設定	BPDU フィルタリングの状態
デフォルト	イネーブル	イネーブル	イネーブル。ポートは最低 10 個の BPDU を送信します。 このポートは、BPDU を受信すると、スパニングツリー標準ポート状態に戻り、BPDU フィルタリングはディセーブルになります。
デフォルト	イネーブル	ディセーブル	ディセーブル
デフォルト	ディセーブル	イネーブルまたはディセーブル	ディセーブル
ディセーブル	イネーブルまたはディセーブル	イネーブルまたはディセーブル	ディセーブル

ポート単位の BPDU フィルタリングの設定	グローバルな BPDU フィルタリングの設定	STP エッジ ポート設定	BPDU フィルタリングの状態
イネーブル	イネーブルまたはディセーブル	イネーブルまたはディセーブル	イネーブル **注意** BPDU は一切送信されず、受信された場合、これは通常の STP の動作をトリガーしないため、慎重に使用します。

ループ ガードの概要

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

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

STP ループは、冗長なトポロジにおいてブロッキング ポートが誤ってフォワーディング ステートに移行すると発生します。 こうした移行は通常、物理的に冗長なトポロジ内のポートの 1 つ（ブロッキング ポートとは限らない）が BPDU の受信を停止すると起こります。

ループ ガードは、デバイスがポイントツーポイント リンクによって接続されているスイッチドネットワークだけで役立ちます。 ポイントツーポイント リンクでは、下位 BPDU を送信するか、リンクをダウンしない限り、代表ブリッジは消えることはありません。

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

ループ ガードを使用して、ルート ポートまたは代替/バックアップ ループ ポートが BPDU を受信するかどうかを確認できます。 BPDU を受信しないポートを検出すると、ループ ガードは、そのポートを不整合状態（ブロッキング ステート）に移行します。このポートは、再度 BPDU の受信を開始するまで、ブロッキング ステートのままです。 不整合状態のポートは BPDU を送信しません。 このようなポートが BPDU を再度受信すると、ループ ガードはそのループ不整合状態を解除し、STP によってそのポート状態が確定されます。こうしたリカバリは自動的に行われます。

ループ ガードは障害を分離し、STP は障害のあるリンクやブリッジを含まない安定したトポロジに収束できます。 ループ ガードをディセーブルにすると、すべてのループ不整合ポートはリスニング ステートに移行します。

ループ ガードはポート単位でイネーブルにできます。 ループ ガードを特定のポートでイネーブルにすると、そのポートが属するすべてのアクティブ インスタンスまたは Virtual LAN（VLAN：仮想 LAN）にループ ガードが自動的に適用されます。 ループ ガードをディセーブルにすると、指定ポートでディセーブルになります。

ルート ガードの概要

特定のポートでルート ガードをイネーブルにすると、そのポートはルート ポートになることが禁じられます。 受信した BPDU によって STP コンバージェンスが実行され、指定ポートがルート ポートになると、そのポートはルート不整合（ブロッキング）状態になります。 このポートが優位 BPDU の送信を停止すると、ブロッキングが再度解除されます。 次に、STP によって、フォワーディング ステートに移行します。 このようにポートのリカバリは自動的に行われます。

特定のインターフェイスでルート ガードをイネーブルにすると、そのインターフェイスが属するすべての VLAN にルート ガード機能が適用されます。

ルート ガードを使用すると、ネットワーク内にルート ブリッジを強制的に配置できます。 ルート ガードは、ルート ガードがイネーブルにされたポートを指定ポートに選出します。 通常、ルート ブリッジのポートはすべて指定ポートとなります（ただし、ルート ブリッジの 2 つ以上のポートが接続されている場合はその限りではありません）。 ルート ブリッジは、ルート ガードがイネーブルにされたポートで上位 BPDU を受信すると、そのポートをルート不整合 STP 状態に移行します。 このようにして、ルート ガードはルート ブリッジを強制的に配置します。

ルート ガードをグローバルには設定できません。

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

STP 拡張機能の設定

STP 拡張機能の設定における注意事項

STP 拡張機能を設定する場合は、次の注意事項に従ってください。

- ホストに接続されたすべてのアクセス ポートとトランク ポートをエッジ ポートとして設定します。
- Bridge Assurance は、ポイントツーポイントのスパニングツリー ネットワーク ポート上だけで実行されます。 この機能は、リンクの両端で設定する必要があります。
- ループ ガードは、スパニングツリー エッジ ポートでは動作しません。
- ポイントツーポイント リンクに接続していないポートでループ ガードをイネーブルにはできません。
- ルート ガードがイネーブルになっている場合、ループ ガードをイネーブルにはできません。

スパニングツリー ポート タイプのグローバルな設定

スパニングツリーポートタイプの割り当ては、そのポートが接続されているデバイスのタイプによって次のように決まります。

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

ポートタイプは、グローバル単位でもインターフェイス単位でも設定できます。デフォルトのスパニングツリー ポート タイプは「標準」です。

はじめる前に

STP が設定されていること。

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

	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)# **spanning-tree port type edge default**	すべてのインターフェイスをエッジ ポートとして設定します。 このコマンドの使用は、すべてのポートがホスト/サーバに接続されていることが前提になります。 エッジポートは、リンク アップすると、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。 デフォルトのスパニングツリー ポート タイプは「標準」です。
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。 このコマンドの使用は、すべてのポートがスイッチまたはブリッジに接続されていることが前提になります。 Bridge Assurance をイネーブルにすると、各ネットワーク ポート上で Bridge Assurance が自動的に実行されます。 デフォルトのスパニングツリー ポートタイプは「標準」です。 （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。

	コマンドまたはアクション	目的

次に、ホストに接続されたアクセス ポートおよびトランク ポートをすべて、スパニングツリー エッジ ポートとして設定する例を示します。

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

次に、スイッチまたはブリッジに接続されたポートをすべて、スパニングツリー ネットワーク ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# spanning-tree port type network default
```

指定インターフェイスでのスパニングツリー エッジ ポートの設定

指定インターフェイスにスパニングツリーエッジポートを設定できます。 スパニングツリーエッジ ポートとして設定されたインターフェイスは、リンク アップ時に、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。

このコマンドには次の 4 つの状態があります。

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

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

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

はじめる前に

STP が設定されていること。

インターフェイスがホストに接続されていること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	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。 （注） これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/QSFP-module/port* になります。
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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** type slot/port	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。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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

	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)# **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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	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。 （注） これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/QSFP-module/port* になります。
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

	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)# **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上で BPDU フィルタリングを明示的に設定した場合、ポートは受信したすべての BPDU を無視してフォワーディング ステートになるので、ブリッジング ループが発生する可能性があります。

このコマンドを入力すると、指定インターフェイスのポート設定が上書きされます。

このコマンドには次の 3 つの状態があります。

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

（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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	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。 （注）　これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/QSFP-module/port* になります。
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。

	コマンドまたはアクション	目的
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

	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)# **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

	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。

	コマンドまたはアクション	目的
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。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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、次のコマンドを使用します。

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

第 9 章

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，139 ページ
- インターフェイス LLDP の設定，141 ページ

グローバル LLDP コマンドの設定

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

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

スイッチは、次の必須の管理 LLDP TLV をサポートします。

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

Data Center Bridging Exchange Protocol（DCBXP）は LLDP を拡張したものです。 ピア間でのノード パラメータのアナウンス、交換、およびネゴシエートに使用されます。 DCBXP パラメータは

特定の DCBXP TLV にパッケージ化されます。 この TLV は、受信した LLDP パケットに確認応答を提供するように設計されています。

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

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **lldp** {**holdtime** *seconds* | **reinit** *seconds* | **timer** *seconds* | **tlv-select** {**dcbxp** | **management-address** | **port-description** | **port-vlan** | **system-capabilities** | **system-description** | **system-name**}}	LLDP オプションを設定します。 **holdtime** オプションを使用して、デバイスが受信したLLDP情報を廃棄するまでの保存時間（10～255秒）を設定します。 デフォルト値は 120 秒です。 **reinit** オプションを使用して、任意のインターフェイスで LLDP 初期化を実行するまでの待機時間（1 ～ 10 秒）を設定します。 デフォルト値は 2 秒です。 **timer** オプションを使用して、LLDP パケットを送信するレート（5 ～ 254 秒）を設定します。 デフォルト値は 30 秒です。 **tlv-select** オプションを使用して、タイプ、長さ、値（TLV）を指定します。 デフォルトではすべての TLV の送受信がイネーブルになります。 **dcbxp** オプションを使用して、データセンターイーサネット パラメータ交換（DCBXP）TLV メッセージを指定します。 **managment-address** オプションを使用して、管理アドレス TLV メッセージを指定します。 **port-description** オプションを使用して、ポート記述 TLV メッセージを指定します。 **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。

	コマンドまたはアクション	目的
		system-description オプションを使用して、システム記述 TLV メッセージを指定します。 **system-name** オプションを使用して、システム名 TLV メッセージを指定します。
ステップ 3	switch(config)# **no lldp** {**holdtime** | **reinit** | **timer**}	LLDP 値をデフォルトにリセットします。
ステップ 4	（任意）switch# **show lldp**	LLDP 設定を表示します。

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

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

次に、LLDP による管理アドレス TLV の送受信をイネーブルにする例を示します。

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

インターフェイス LLDP の設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	変更するインターフェイスを選択します。 （注） これが 10G ブレークアウト ポートの場合、*slot/port* 構文は *slot/QSFP-module/port* になります。
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	(オプション)switch# **show lldp** {**interface** | **neighbors** [**detail** |	LLDP 設定を表示します。

	コマンドまたはアクション	目的
	interface | **system-detail**] | **timers** | **traffic**}	

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 ネイバーの情報とシステム詳細を表示する例を示します。

```
switch# sh lldp neighbors system-detail
Capability codes:
 (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
 (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID Local Intf Chassis ID PortID Hold-time Capability

switch-2  Eth1/7  0005.73b7.37ce Eth1/7  120 B
switch-3  Eth/9   0005.73b7.37d0 Eth1/9  120 B
switch-4  Eth1/10 0005.73b7.37d1 Eth1/10 120 B
Total entries displayed: 3
```

次に、LLDP タイマーの情報を表示する例を示します。

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

次に、LLDP カウンタを表示する例を示します。

```
switch# show lldp traffic
LLDP traffic statistics:

    Total frames out: 8464
    Total Entries aged: 6
    Total frames in: 6342
    Total frames received in error: 2
    Total frames discarded: 2
    Total TLVs unrecognized: 0
```

第 10 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 アドレスに関する情報，145 ページ
- MAC アドレスの設定，146 ページ
- MAC アドレスの設定の確認，147 ページ

MAC アドレスに関する情報

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

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

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

MAC アドレスの設定

スタティック MAC アドレスの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **mac-address-table static** *mac_address* **vlan** *vlan-id* {**drop** | **interface** {*type slot*/*port*} | **port-channel** *number*} [**auto-learn**]	MACアドレステーブルに追加するスタティックアドレスを指定します。 **auto-learn** オプションをイネーブルにすると、同じ MAC アドレスが別のポート上で見つかった場合には、スイッチがエントリを更新します。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config)# **no mac address-table static** *mac_address* **vlan** *vlan-id*	（任意） MACアドレステーブルからスタティックエントリを削除します。 **mac-address-table static** コマンドを使用して、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 1/4
switch(config) #
```

MAC テーブルのエージング タイムの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **mac-address-table aging-time** *seconds* [**vlan** *vlan_id*]	エントリが無効になって、MAC アドレス テーブルから破棄されるまでの時間を指定します。 *seconds* の範囲は 0 ～ 1000000 です。 デフォルトは 1800 秒です。 0 を入力すると、MAC エージングがディセーブルになります。 VLAN を指定しなかった場合、エージングの指定がすべての VLAN に適用されます。

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

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

MAC テーブルからのダイナミック アドレスのクリア

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。

MAC アドレスの設定の確認

設定を確認するには、次のいずれかのコマンドを使用します。

表 7：*MAC* アドレス設定の確認コマンド

コマンド	目的
show mac-address-table aging-time	スイッチ内で定義されているすべての VLAN の MAC アドレスのエージング タイムを表示します。
show mac-address-table	MAC アドレス テーブルの内容を表示します。 （注） IGMP スヌーピングによって学習された MAC アドレスは表示されません。
show mac address-table loop-detect	現在設定されているアクションを表示します。

次に、MAC アドレス テーブルを表示する例を示します。

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

次に、現在のエージング タイムを表示する例を示します。

```
switch# show mac-address-table aging-time
Vlan  Aging Time
----- ----------
1     1800
13    1800
42    1800
```

次に、現在設定されているアクションを表示する例を示します。

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

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

第 11 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，149 ページ
- IGMP スヌーピング パラメータの設定，152 ページ
- IGMP スヌーピングの設定確認，156 ページ

IGMP スヌーピングの情報

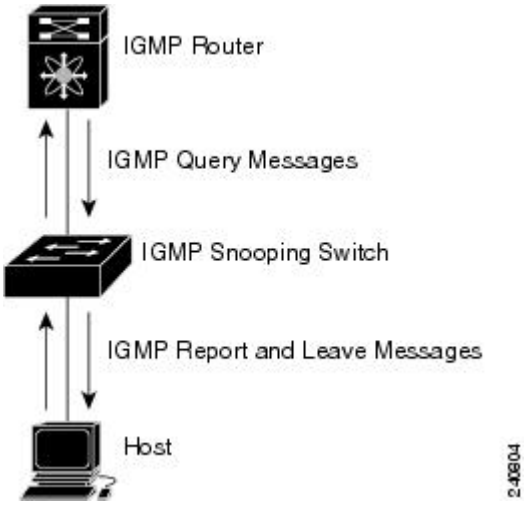
IGMP スヌーピング ソフトウェアは、VLAN 内の IGMP プロトコル メッセージを調べて、このトラフィックの受信に関連のあるホストまたはその他のデバイスに接続されているのはどのインターフェイスかを検出します。 IGMP スヌーピングは、インターフェイス情報を使用して、マルチアクセス LAN 環境での帯域幅消費を減らすことができ、これによって VLAN 全体のフラッディングを防ぎます。 IGMP スヌーピング機能は、どのポートがマルチキャスト対応ルータに接続されているかを追跡して、IGMP メンバーシップ レポートの転送管理を支援します。 トポロジの変更通知には、IGMP スヌーピング 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

（注） IGMP スヌーピングは、すべてのイーサネット インターフェイスでサポートされます。 スヌーピングという用語が使用されるのは、レイヤ 3 コントロール プレーン パケットが代行受信され、レイヤ 2 の転送決定に影響を与えるためです。

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

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

図 *18*： ***IGMP*** スヌーピング スイッチ



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

IGMPv1 および IGMPv2

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

各 VLAN スイッチ ポートに接続されているホストが 1 つしかない場合は、IGMPv2 の高速脱退機能を設定できます。 高速脱退機能を使用すると、最終メンバ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。 プロキシ機能により、ダウンストリーム ホストが送信するメンバーシップ レポートからグループ ステートが構築され、アップストリーム クエリアからのクエリーに応答するためにメンバーシップ レポートが生成されます。

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。

現在のところ、スイッチ クエリアと IGMP スヌーピング クエリアに対して同じ SVI IP アドレスを設定できます。 そうすると、両方のクエリアが同時にアクティブになって、両方が一般的なクエリーを定期的に VLAN に送信するようになります。 これを回避するには、IGMP スヌーピング クエリアとスイッチ クエリアで別々の IP アドレスを使用してください。

IGMP 転送

Cisco Nexus デバイスは、（S,G）/（*,G）IP アドレスに基づくスヌーピングをサポートしています。 Cisco Nexus デバイスにはマルチキャスト MAC のエイリアシングは適用されず、スヌーピングされたエントリは MAC テーブルではなく FIB テーブルにプログラミングされます。

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（S,G）または（*,G）グループの情報を更新し、そのグループのマルチキャスト トラフィックの受信に関心のあるホストだけが、転送テーブルに指定されるようにします。 ルータが VLAN からレポートを受信しなかった場合、その VLAN 用のグループは IGMP キャッシュから削除されます。

IGMP スヌーピング パラメータの設定

IGMP スヌーピング プロセスの動作を管理するには、次の表で説明する、省略可能な IGMP スヌーピング パラメータを設定します。

表 *8*：*IGMP* スヌーピング パラメータ

パラメータ	説明
IGMP スヌーピング	VLAN ごとに IGMP スヌーピングをイネーブルにします。 デフォルトはイネーブルです。 （注） グローバルな設定がディセーブルになっている場合は、すべての VLAN が、イネーブルかどうかに関係なくディセーブルと見なされます。
明示的な追跡	各ポートに接続されたそれぞれのホストから送信される IGMPv3 メンバーシップ レポートを、VLAN 別に追跡します。 デフォルトはイネーブルです。

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

パラメータ	説明
マルチキャスト ルータ vpc-peer-link	仮想ポートチャネル（vPC）ピア リンクへのスタティック接続を設定します。 デフォルトでは、vPC ピア リンクは、マルチキャストルータ ポートと見なされ、マルチキャスト パケットは、各レシーバ VLAN のピア リンクに送信されます。 孤立ポートを持つ各レシーバ VLAN に vPC ピア リンク上でマルチキャスト トラフィックを送信するには、**no ip igmp snooping mrouter vpc-peer-link** コマンドを使用します。 **no ip igmp snooping mrouter vpc-peer-link** コマンドを使用する場合、VLANに孤立ポートがない限り、マルチキャスト トラフィックは、送信元 VLAN とレシーバ VLAN のピア リンクに送信されません。 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。
スタティック グループ	VLAN に属するインターフェイスを、マルチキャスト グループのスタティック メンバとして設定します。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **ip igmp snooping**	IGMPスヌーピングをグローバルにイネーブルにします。デフォルトはイネーブルです。 （注） グローバルな設定がディセーブルになっている場合は、すべての VLAN が、イネーブルかどうかに関係なくディセーブルと見なされます。
ステップ 3	switch(config)# **vlan configuration** *vlan-id*	VLAN コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	switch(config-vlan)# **ip igmp snooping**	現在の VLAN に対して IGMP スヌーピングをイネーブルにします。 デフォルトはイネーブルです。 （注） IGMP スヌーピングがグローバルにイネーブルになっている場合は、このコマンドは必要ありません。
ステップ 5	switch(config-vlan)# **ip igmp snooping explicit-tracking**	各ポートに接続されたそれぞれのホストから送信される IGMPv3 メンバーシップ レポートを、VLAN 別に追跡します。 デフォルトは、すべての VLAN でイネーブルです。
ステップ 6	switch(config-vlan)# **ip igmp snooping fast-leave**	IGMPv2 プロトコルのホスト レポート抑制メカニズムのために、明示的に追跡できない IGMPv2 ホストをサポートします。 高速脱退がイネーブルの場合、IGMP ソフトウェアは、各 VLAN ポートに接続されたホストが 1 つだけであると見なします。 デフォルトは、すべての VLAN でディセーブルです。
ステップ 7	switch(config-vlan)# **ip igmp snooping last-member-query-interval** *seconds*	いずれのホストからも IGMP クエリー メッセージへの応答がないまま、最終メンバのクエリー インターバルの期限が切れた場合に、対応する VLAN ポートからグループを削除します。 有効範囲は 1 ～ 25 秒です。 デフォルトは 1 秒です。
ステップ 8	switch(config-vlan)# **ip igmp snooping querier** *IP-address*	マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、スヌーピング クエリアを設定します。 IP アドレスは、メッセージの送信元として使用します。 デフォルトはディセーブルです。
ステップ 9	switch(config-vlan)# **ip igmp snooping report-suppression**	マルチキャスト対応ルータに送信されるメンバーシップ レポート トラフィックを制限します。 レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。 デフォルトはイネーブルです。
ステップ 10	switch(config-vlan)# **ip igmp snooping mrouter interface** *interface*	マルチキャスト ルータへのスタティックな接続を設定します。 ルータと接続するインターフェイスが、選択した VLAN に含まれている必要があります。 インターフェイスは、タイプと番号で指定できます。
ステップ 11	switch(config-vlan)# **ip igmp snooping mrouter vpc-peer-link**	仮想ポート チャネル（vPC）ピア リンクへのスタティック接続を設定します。 デフォルトでは、vPC ピア リンクはマルチキャスト ルータ ポートと見なされ、マルチ

	コマンドまたはアクション	目的
		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。 孤立ポートを持つ各レシーバ VLAN に vPC ピア リンク上でマルチキャスト トラフィックを送信するには、**no ip igmp snooping mrouter vpc-peer-link** コマンドを使用します。 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 configuration 5
switch(config-vlan)# ip igmp snooping last-member-query-interval 3
switch(config-vlan)# ip igmp snooping querier 172.20.52.106
switch(config-vlan)# ip igmp snooping explicit-tracking
switch(config-vlan)# ip igmp snooping fast-leave
switch(config-vlan)# ip igmp snooping report-suppression
switch(config-vlan)# ip igmp snooping mrouter interface ethernet 1/10
switch(config-vlan)# ip igmp snooping 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、次のコマンドを使用します。

コマンド	説明
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。
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。

コマンド	説明
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。
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。
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: 192.0.2.1, version: 3
  Querier interval: 125 secs
  Querier last member query interval: 10 secs
  Querier robustness: 2
  Switch-querier enabled, address 192.0.2.1, currently running
  Explicit tracking enabled
  Fast leave enabled
  Report suppression enabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 1
  Number of groups: 1
```

第 12 章

MVR の設定

この章の内容は、次のとおりです。

- MVR について，159 ページ
- MVR のライセンス要件，160 ページ
- MVR に関する注意事項と制約事項，161 ページ
- デフォルトの MVR 設定，161 ページ
- MVR の設定，162 ページ
- MVR 設定の確認，165 ページ

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。 ルータは、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 の静的設定のいずれかを使用して、ホストが加入した MVR ポートに対してのみ転送します。 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、仮想ポート チャネル（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** コマンドは、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不要です。 ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 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。
- Flex Link ポートでの MVR の設定はサポートされません。
- 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。

（注） インサービス ソフトウェア アップグレード（ISSU）時には、join がアップストリーム ルータに転送されないため、MVR レシーバ ポートの MVR IGMP メンバーシップがタイムアウトする可能性があります。 タイムアウトを避けるためには、ISSUに対応するようにアップストリーム ルータのクエリア タイマーまたはネットワーク クエリアを増加させる必要があります。

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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **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	switch(config)# [**no**] **mvr-vlan** *vlan-id*	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	switch(config)# [**no**] **mvr-group** *addr*[/*mask*] [**count** *groups*] [**vlan** *vlan-id*]	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。 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。

	コマンドまたはアクション	目的
ステップ 5	switch(config)# **end**	（任意） 特権 EXEC モードに戻ります。
ステップ 6	switch# **clear mvr counters** [**source-ports** | **receiver-ports**]	（任意） MVR IGMP パケット カウンタをクリアします。
ステップ 7	switch# **show mvr**	（任意） グローバル MVR 設定を表示します。
ステップ 8	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次の例は、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 192.0.2.1 count 4
switch(config-mvr)# mvr-group 192.0.2.240/28 vlan 101
switch(config-mvr)# mvr-group 192.0.2.6 vlan 340
switch(config-mvr)# end
switch# show mvr
MVR Status           : enabled
Global MVR VLAN      : 100
Number of MVR VLANs  : 3
switch# copy running-config startup-config
```

MVR インターフェイスの設定

手順

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

	コマンドまたはアクション	目的
	channel-number | **vethernet** *number*}	（注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 4	[**no**] **mvr-type** {**source** | **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*	（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*]	（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。

	コマンドまたはアクション	目的
		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**	（任意） 特権 EXEC モードに戻ります。
ステップ 8	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

次の例は、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と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*}	指定されたインターフェイスの MVR の設定を表示します。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
show mvr members [**count**]	すべての MVR メンバーの数と詳細を表示します。

コマンド	説明
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。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。

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 13 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，169 ページ
- トラフィック ストーム制御の注意事項と制約事項，171 ページ
- トラフィック ストーム制御の設定，172 ページ
- トラフィック ストーム制御の設定の確認，172 ページ
- トラフィック ストーム制御の設定例，173 ページ
- デフォルトのトラフィック ストームの設定，173 ページ

トラフィック ストーム制御の概要

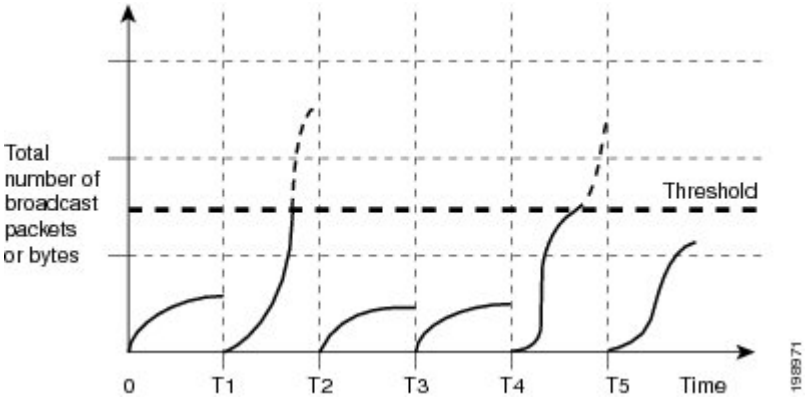
トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。 トラフィック ストーム制御機能を使用すると、ブロードキャスト、マルチキャスト、または未知のユニキャスト トラフィック ストームによって、イーサネット インターフェイス経由の通信が妨害されるのを防ぐことができます。

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、または未知のユニキャストの着信トラフィックのレベルを 10 ミリ秒間隔で監視できます。 この間、トラフィック レベル（ポートの使用可能合計帯域幅に対するパーセンテージ）が、設定したトラフィック ストーム制御レベルと比較されます。 入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。

次の図に、指定したタイム インターバル期間中におけるイーサネット インターフェイス上のブロードキャスト トラフィック パターンを示します。 この例では、トラフィック ストーム制御が

T1 と T2 時間の間、および T4 と T5 時間の間で発生します。 これらの間隔中に、ブロードキャスト トラフィックの量が設定済みのしきい値を超過したためです。

図 *19* : ブロードキャストの抑制



トラフィック ストーム制御のしきい値とタイム インターバルを使用することで、トラフィック ストーム制御アルゴリズムは、さまざまなレベルの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。

トラフィック ストーム制御は、ハードウェアに実装されています。 トラフィック ストーム制御回路は、イーサネットインターフェイス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/ブロードキャストであることを判断し、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超過したブロードキャスト トラフィックがドロップされます。
- マルチキャスト トラフィック ストーム制御をイネーブルにした場合、マルチキャスト トラフィックが 10 マイクロ秒のインターバル以内にしきい値レベルを超えると、トラフィック ストーム制御により、そのインターバルが終了するまですべての超過したマルチキャスト トラフィックがドロップされます。
- ブロードキャストおよびマルチキャスト トラフィック ストーム制御をイネーブルにした場合、ブロードキャスト トラフィックが 10 マイクロ秒のインターバル以内にしきい値レベルを超えると、トラフィックストーム制御により、そのインターバルが終了するまですべての超過したブロードキャスト トラフィックがドロップされます。

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

デフォルトで、Cisco NX-OS は、トラフィックが設定済みレベルを超えても是正のための処理を行いません。

トラフィック ストーム制御の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。
- スイッチをファブリック エクステンダ（FEX）に接続するファブリック ポートまたはファブリック ポート チャネルでのトラフィック ストーム制御を設定できます。 FEX で設定したストーム制御は、その FEX 上のすべてのポートに着信する集約トラフィックに適用されます。

（注） NIF ストーム制御機能は、FEX ファブリック ポートに着信するすべてのトラフィックに適用されます。 VNTAG ヘッダー付きで FEX ファブリック ポートに着信するトラフィックには、元のトラフィックに追加の 6 バイトが追加されます。 これらの追加の 6 バイトのオーバーヘッドが原因で、ストーム制御ポリサーがトラフィックをポリシングするレートは、HIF ポートに入るオリジナル トラフィックのパケット サイズに応じてスキューされます。 小さいパケット サイズの場合、大きいパケット サイズに比べてスキューが大きくなります。

- レベルをインターフェイスの帯域幅全体に対する割合として指定します。
  - レベルの指定範囲は 0 ～ 100 です。
  - 任意で、レベルの小数部を 0 ～ 99 の範囲で指定できます。
  - 100% は、トラフィック ストーム制御がないことを意味します。
  - 0.0% は、すべてのトラフィックを抑制します。
- ストーム制御ドロップが個別にカウントされることを防ぐ、ローカル リンクおよびハードウェアの制約事項があります。 代わりに、ストーム制御ドロップは discards カウンタの他のドロップとともにカウントされます。
- ハードウェアの制限およびサイズの異なるパケットがカウントされる方式のため、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。

- HIF 範囲に対するストーム制御の適用は推奨されません。 ハードウェア リソースのアベイラビリティによって、範囲内の 1 つ以上のインターフェイスの設定が失敗することがあります。 コマンドの結果は、場合によっては部分的に成功します。

トラフィック ストーム制御の設定

制御対象のトラフィックが使用できる、利用可能な合計帯域幅に対するパーセンテージを設定できます。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {**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。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
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、ポート チャネル 122 および 123 のトラフィック ストーム制御を設定する例を示します。

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

トラフィック ストーム制御の設定の確認

トラフィック ストーム制御の設定情報を表示するには、次のコマンドを使用します:

コマンド	目的
show interface [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control**	インターフェイスのトラフィック 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。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
show running-config interface	トラフィック ストーム制御の設定を表示します。

（注） ストームイベントがポートで発生し、パケットがストーム制御設定によって廃棄される場合、ストーム イベントが開始したことを示すために syslog メッセージが生成されます。 追加の syslog メッセージは、ストーム イベントが終了し、パケットがドロップされなくなった場合に生成されます。

トラフィック ストーム制御の設定例

次に、トラフィック ストーム制御の設定例を示します。

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

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

デフォルトのトラフィック ストームの設定

次の表に、トラフィック ストーム制御パラメータのデフォルト設定を示します。

表 *9*：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

パラメータ	デフォルト
しきい値パーセンテージ	100

第 14 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。

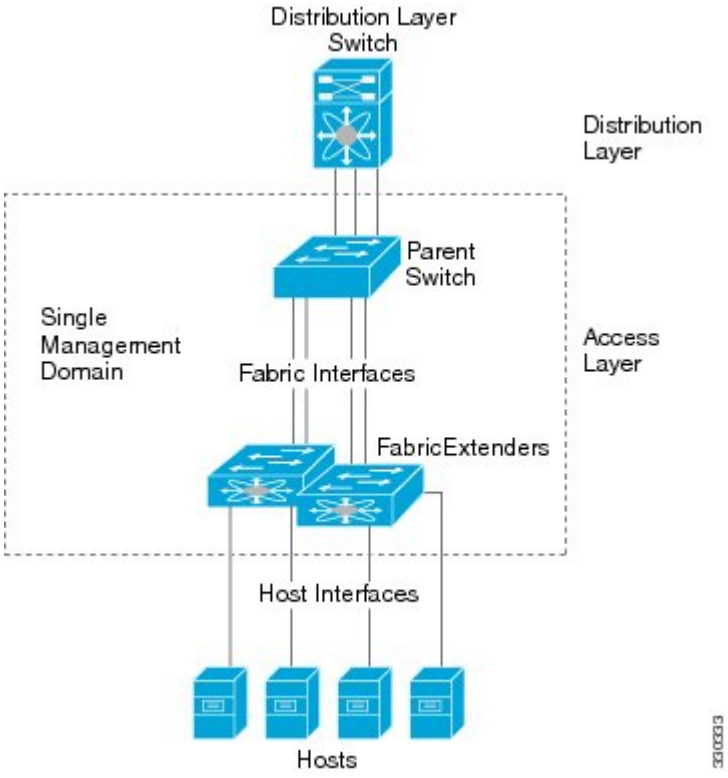
- Cisco Nexus 2000 シリーズ ファブリック エクステンダについて，176 ページ
- ファブリック エクステンダの用語，177 ページ
- ファブリック エクステンダの機能，177 ページ
- オーバーサブスクリプション，184 ページ
- 管理モデル，185 ページ
- フォワーディング モデル，186 ページ
- 接続モデル，187 ページ
- ポート番号の表記法，190 ページ
- ファブリック エクステンダのイメージ管理，190 ページ
- ファブリック エクステンダのハードウェア，191 ページ
- ファブリック インターフェイスへのファブリック エクステンダの関連付け，192 ページ
- ファブリック エクステンダ グローバル機能の設定，196 ページ
- 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，199 ページ
- リンクの再配布，200 ページ
- ファブリック エクステンダの設定の確認，202 ページ
- シャーシ管理情報の確認，205 ページ
- Cisco Nexus N2248TP-E ファブリック エクステンダの設定，210 ページ
- Cisco Nexus N2248PQ ファブリック エクステンダの設定，214 ページ

Cisco Nexus 2000 シリーズ ファブリック エクステンダについて

Cisco Nexus 2000 シリーズ ファブリック エクステンダ（別名 FEX）は、Cisco Nexus シリーズ デバイスと連携してサーバ集約のために高密度、低コストの接続を実現する、スケーラブルかつ柔軟性の高いサーバ ネットワーキング ソリューションです。 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、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 Quality of Service（QoS）設定パラメータを含め、親デバイスと同じ機能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 *20*： 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。

- ポートチャネルの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 チャネルのホスト インターフェイス：サーバまたはホスト システムとの接続に使用するポート チャネルのホスト 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 または（BPDU フィルタをイネーブルにした）vPC などの、スパニングツリーに依存していないリンク冗長性メカニズムを使用するすべてのエッジ 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。 ループを排除するためにスパニングツリーが使用されていないため、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 フリー トポロジを使用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, （123 ページ）を参照してください。

ホスト ポート チャネル

次のファブリック エクステンダは、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ています。 1 つのポート チャネルには、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、リンク アグリゲーション制御プロトコル（LACP）の有無にかかわらず設定できます。

- Cisco Nexus 2248TP
- Cisco Nexus 2232PP

- Cisco Nexus 2224TP
- Cisco Nexus 2248PQ
- Cisco Nexus B22 Fabric Extender for Fujitsu（N2K-B22FTS-P）
- Cisco Nexus B22 Fabric Extender for Dell（N2K-B22DELL-P）
- Cisco Nexus B22 Fabric Extender for HP（N2K-B22HP-P）
- Cisco Nexus B22 Fabric Extender for IBM（N2K-B22IBM-P）

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 のメンバーになれます。

- ホスト インターフェイスは、隔離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

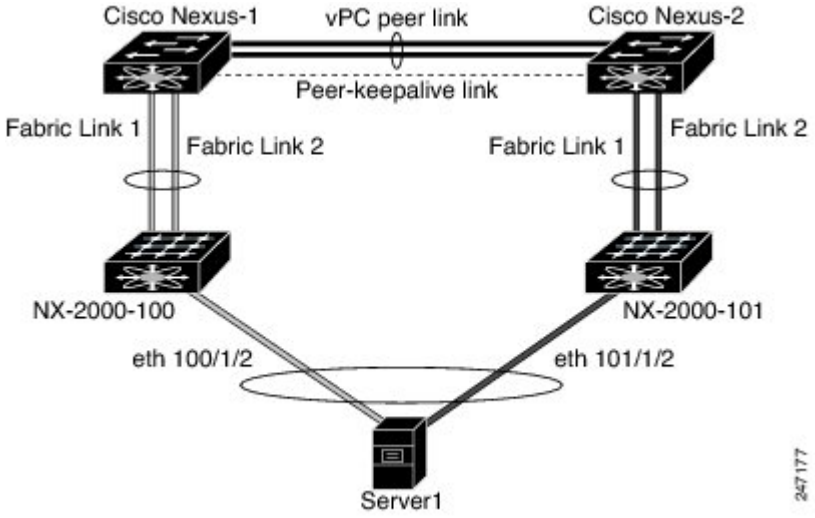
仮想ポート チャネル（vPC）を使用して、Cisco Nexus ファブリック エクステンダが親スイッチのペアに接続されているトポロジやファブリック エクステンダのペアが 1 つの親スイッチに接続されているトポロジを設定できます。 vPC では、マルチパス接続を提供できます。この接続を使用すると、ネットワーク上のノード間に冗長性を作成できます。

（注） 同じ Cisco Nexus デバイスに接続された 2 つの FEX 間のポート チャネルはサポートされません。 同じ Cisco Nexus デバイスに接続されたとき、仮想ポート チャネル（vPC）は 2 つの異なる FEX にまたがることはできません。

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。

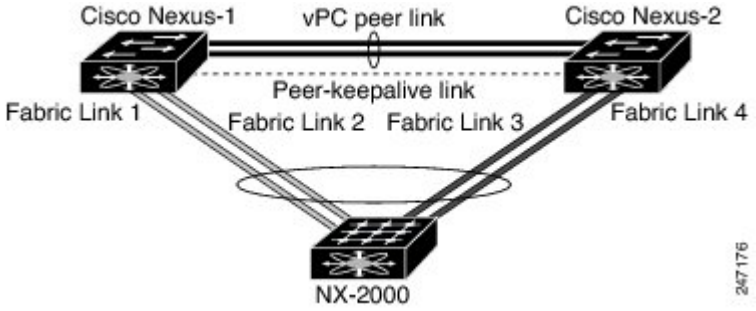
- 親スイッチは、ファブリック エクステンダにシングルホーム接続されます。その後、ファブリック エクステンダは、デュアル インターフェイスを持つサーバに接続されます（次の図を参照）。

図 *21*：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 *22*：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。

（注） 同じ Cisco Nexus デバイスに接続された 2 つのファブリック エクステンダ間のポート チャネルはサポートされません。vPC は、同じ物理 Cisco Nexus デバイスに接続された 2 つの異なるファブリック エクステンダにまたがることはできません。

Fibre Channel over Ethernet（FCoE）のサポート

Cisco Nexus 2232PP および Cisco Nexus 2248PQ 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、『Fibre Channel over Ethernet Configuration Guide』を参照してください。（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 プレーンの負荷を軽減するために、Cisco NX-OS では ファブリック エクステンダ CPU にリンク レベルのプロトコル処理をオフロードすることができます。 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）および Data Center Bridging Exchange（DCBX）
- Cisco Discovery Protocol（CDP）
- リンク アグリゲーション制御プロトコル（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 Quality of Service（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。

LCC および Quality of Service の詳細については、デバイスの『Quality of Service Configuration Guide』を参照してください。

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、親 Cisco Nexus シリーズ 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、デバイスの『Security Configuration Guide』を参照してください。

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 エクステンダおよびその親スイッチは、宛先マルチキャスト MAC アドレスだけに基づいて、IGMPv3 スヌーピングをサポートします。 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、『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』も参照してください。

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 インターフェイスを、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することができます。 ファブリック エクステンダ ポートを SPAN 宛先として設定することはできません。 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を分離することはできません。

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、入力モニタリングと出力モニタリングが設定されている場合、パケットが 2 回表示されることがあります（1 回めは Rx が設定されているインターフェイスのパケット入力、2 回めは Tx が設定されているインターフェイスのパケット出力）。

SPAN の詳細については、デバイスの『System Management Configuration Guide』を参照してください。

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。

（注） 2248PQ の場合は、すべてのファブリック インターフェイスを 1 つのファブリック ポート チャネルにまとめる必要があります。 これらは、個別のポートとして親スイッチとの接続に使用することはできません。

PFC の詳細については、デバイスの『Quality of Service Configuration Guide』を参照してください。

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。 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。 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とき、Cisco Nexus 2148T に同様の設定が提供されます。

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 2248PQ ファブリック エクステンダには、16 個の 10 ギガビット イーサネット ファブリック インターフェイスと 48 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 2248PQ の最大オーバーサブスクリプション比率は 3:1 です。

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 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。 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。 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 G-BASE-T（10 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、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 2224TP 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。

Cisco Nexus B22 Fabric Extender for HP（NB22HP）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 16 の 1G/10 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。 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。 静的ピン接続およびポート チャネル モードがサポートされています。 すべてのホストインターフェイスがすべてのファブリックインターフェイスにトラフィックを送信する場合、Cisco Nexus B22 Fabric Extender for HP（N2K-B22HP-P）の最大オーバーサブスクリプション比は 2:1 です。

Cisco Nexus B22 Fabric Extender for Fujitsu（NB22FTS）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 16 の 10 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。 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。 静的ピン接続およびポート チャネル モードがサポートされています。 すべてのホスト インターフェイスがすべてのファブリック インターフェイスにトラフィックを送信する場合、Cisco Nexus B22 Fabric Extender for Fujitsu（N2K-B22FTS-P）の最大オーバーサブスクリプション比は 2:1 です。

Cisco Nexus B22 Fabric Extender for Dell（NB22DELL）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 16 の 1G/10 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。 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。 静的ピン接続およびポート チャネル モードがサポートされています。 すべてのホスト インターフェイスがすべてのファブリック インターフェイスにトラフィックを送信する場合、Cisco Nexus B22 Fabric Extender for Dell（N2K-B22DELL-P）の最大オーバーサブスクリプション比は 2:1 です。

Cisco Nexus B22 Fabric Extender for IBM（NB22IBM）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 14 個の 1G/10 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。 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。 静的ピン接続およびポート チャネル モードがサポートされています。 すべてのホスト インターフェイスがすべてのファブリック インターフェイスにトラフィックを送信する場合、Cisco Nexus B22 Fabric Extender for IBM（N2K-B22IBM-P）の最大オーバーサブスクリプション比は 2:1 です。

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で ファブリック エクステンダを検出します。

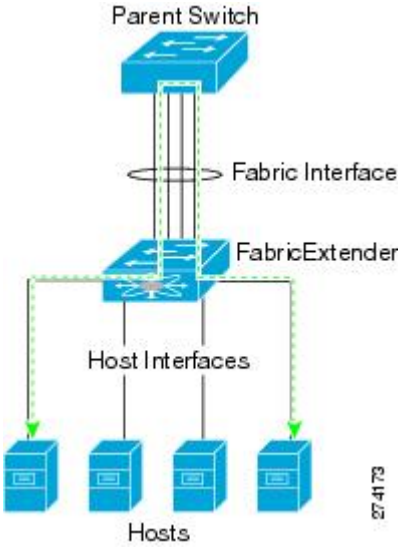
ファブリック エクステンダが検出され、親スイッチに正常に関連付けられていると、次の操作が実行されます。

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 *23*： 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 エクステンダと親 Cisco Nexus シリーズ 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。その結果、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した場合、そのインターフェイスはBPDUが受信された時点で errdisable ステートになります。

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は 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。

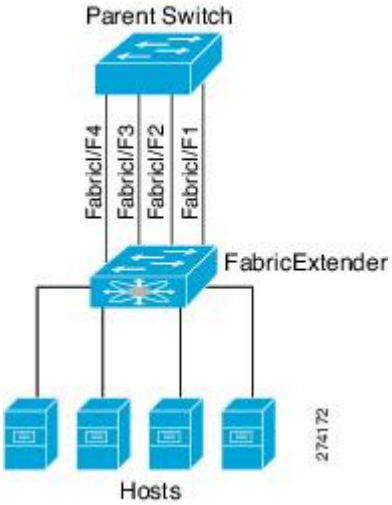
（注） Cisco Nexus 2248PQ ファブリック エクステンダは、静的ピン接続ファブリック インターフェイス接続をサポートしていません。

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 *24*：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。

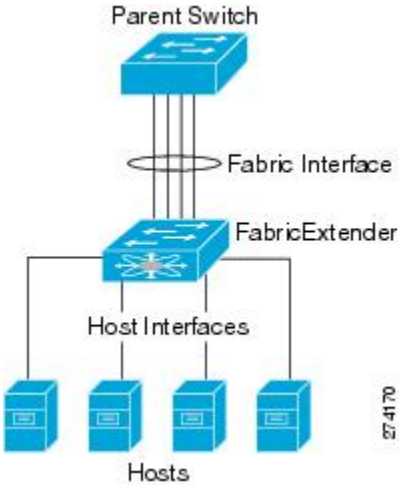
リブート後にも決定論的で固定的な関連付けを維持するために、ピン接続を手動で再配布できます。

（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、次の図に示すように、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 *25*： 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 インターフェイスは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*/*QSFP-module*/*port*

値は次のとおりです。

- *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。
- *QSFP* モジュールは 10G ブレークアウト ラインカード拡張モジュール（LEM）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 エクステンダのイメージ管理

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 8 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 2224TP 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 2248PQ 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 48 個の 10 ギガビット イーサネット ホスト インターフェイスと、4 つの QSFP インターフェイス アダプタに対応する 16 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 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。

- Cisco Nexus B22 Fabric Extender for HP（NB22HP）には、16 個の 1G/10 ギガビット 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。 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。
- Cisco Nexus B22 Fabric Extender for Fujitsu（NB22FTS）には、16 個の 10 ギガビット イーサネット ホスト インターフェイスが搭載されています。 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。
- Cisco Nexus B22 Fabric Extender for Dell（NB22DELL）には、16 個の 1G/10 ギガビット 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。 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。
- Cisco Nexus B22 Fabric Extender for IBM（NB22IBM）には、14 個の 1G/10 ギガビット 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。 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。

ファブリックインターフェイスへのファブリックエクステンダの関連付け

FEXは、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番号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。

イーサネット インターフェイスへのファブリック エクステンダの関連付け

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

	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。
		（注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。

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。

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 番号を関連付けます。 FEX 番号の範囲は 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関連付けを表示します。

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関連付ける例を示します。

```
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関連付け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
```

ポート チャネルへのファブリック エクステンダの関連付け

はじめる前に

ファブリック エクステンダ機能をイネーブルにしていることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**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** *channel*
	
	例：
	`switch(config)# interface port-channel 4`
	`switch(config-if)#`
		ポート チャネルを設定することを指定します。

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 番号を関連付けます。 範囲は 101 ～ 199 です。

	コマンドまたはアクション	目的
ステップ 5	**show interface port-channel** *channel* **fex-intf** 例： `switch# show interface port-channel 4 fex-intf`	（任意） ポートチャネルインターフェイスへのファブリックエクステンダの関連付けを表示します。

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関連付ける例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/28
switch(config-if)# channel-group 4
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# interface ethernet 1/29
switch(config-if)# channel-group 4
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# interface ethernet 1/30
switch(config-if)# channel-group 4
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# interface ethernet 1/31
switch(config-if)# channel-group 4
switch(config-if)# no shutdown
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 ベスト プラクティスとして、物理インターフェイスからではなく、ポート チャネル インターフェイスからのみ **fex associate** コマンドを入力します。

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 に関連付けようとすると、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 シリーズ デバイスはそのリンク上の 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）で入力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関連付け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のファブリックエクステンダの関連付けの解除

はじめる前に

ファブリック エクステンダ機能をイネーブルにしていることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**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* | **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 チャネルを指定できます。
		（注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。

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 グローバル機能の設定

ファブリック エクステンダのグローバル機能を設定できます。

はじめる前に

ファブリック エクステンダ機能セットをイネーブルにしていることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**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** *FEX-number*
	
	例：
	`switch(config)# fex 101`
	`switch(config-fex)#`
		指定したファブリック エクステンダの FEX コンフィギュレーション 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 番号です。 FEX 番号が 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 • N2224TP：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 および N2232TM：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

	コマンドまたはアクション	目的
		• 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 Base-T/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 • N2248PQ：48 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 16 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 • NB22HP：16 個の 1 G/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 • NB22FTS：16 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 • NB22DELL：16 個の 1 G/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 • NB22IBM：14 個の 1 G/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 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 のタイプを削除します。 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おり、親スイッチのバイナリ設定に保存された設定済みタイプが一致していなければ、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。

	コマンドまたはアクション	目的
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。 1 ポート チャネル接続は 1 つだけ存在できます。 **注意** **pinning max-links** コマンドでアップリンクの数を変更すると、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 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** コマンドでアップリンクの数を変更すると、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にだけ、スイッチでは、対応するシャーシIDを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** 指定されたファブリック エクステンダに一致しないシリアル番号を設定すると、ファブリック エクステンダが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

	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。
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。

（注） Cisco Nexus 2248PQ ファブリック エクステンダは、静的ピン接続ファブリック インターフェイス接続をサポートしていません。

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 ポートを中断します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	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* 番号の範囲は 100 ～ 199 です。

ファブリック エクステンダの設定の確認

ファブリック エクステンダの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、次のコマンドを使用します。

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	デバイスの機能セットの状態を表示します。

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、親スイッチのインターフェイスに接続されている SFP+ トランシーバのファブリック エクステンダアップリンクの 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 SFP+ トランシーバのファブリック エクステンダアップリンクの SFP+ トランシーバおよび DOM の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、次のいずれかを使用します。

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        --         ok
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 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）
- 入力方向のキュー制限（FEX グローバル レベルおよびインターフェイス レベル）
- 出力方向のキュー制限（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 25392KB 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

	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 のコンフィギュレーション モードを開始します。
		
		chassis_id 値の範囲は 100 ～ 199 です。

	コマンドまたはアクション	目的
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 ～ 25392 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。

次に、共有バッファを設定する例を示します。

```
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 レベルでのキュー制限の設定

キュー制限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 キュー制限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

	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 のコンフィギュレーション モードを開始します。
		chassis_id 値の範囲は 100 ～ 199 です。

	コマンドまたはアクション	目的
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）のデフォルトのキュー制限は 4 MB です。 （注） **hardware N2248TP-E queue-limit** コマンドでは、デフォルトの tx キュー制限を指定します。 • 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 キュー制限を指定します。

次に、キュー制限を設定する例を示します。

```
switch# configure terminal
switch(config)# fex 100
switch(config-fex)# hardware N2248TP-E queue-limit 83000 tx
switch(config-fex)#
```

ポート レベルでのキュー制限の設定

ポート レベルでキュー制限を設定することで、グローバル レベル設定を上書きできます。

また、ポート レベルでキュー制限をディセーブルにすることもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 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。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。

	コマンドまたはアクション	目的
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）のデフォルトのキュー制限は 4 MB です。 • rx（入力）のデフォルトのキュー制限は 1 MB です。

次に、キュー制限を設定する例を示します。

```
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

	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 のコンフィギュレーション 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*	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。

	コマンドまたはアクション	目的
	例： `switch(config-fex)# hardware N2248TP-E uplink-pause-no-drop distance 3000`	（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。

次に、アップリンク距離を設定する例を示します。

```
switch# configure terminal
switch(config)# fex 100
switch(config-fex)# hardware N2248TP-E uplink-pause-no-drop distance 3000
switch(config-fex)#
```

Cisco Nexus N2248PQ ファブリック エクステンダの設定

Cisco Nexus 2248PQ 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）
- ロードバランシング キュー（FEX グローバル 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 16 MB 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 10240 KB です。

（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

	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 のコンフィギュレーション 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 N2248PQ shared-buffer-size** *buffer-size* 例： `switch(config-fex)# hardware N2248PQ shared-buffer-size 8096`	共有バッファ サイズ（KB）を指定します。 *buffer-size* 値の範囲は 3072 KB ～ 10240 KB です。 （注） **hardware N2248PQ shared-buffer-size** コマンドでは、デフォルトの共有バッファ サイズ 10240 KB を指定します。

次に、共有バッファを設定する例を示します。

```
switch# configure terminal
switch(config)# fex 100
switch(config-fex)# hardware N2248PQ shared-buffer-size 8096
switch(config-fex)#
```

アップリンク距離の設定

Cisco Nexus N2248PQ 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

	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 のコンフィギュレーション 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 N2248PQ uplink-pause-no-drop distance** *distance-value* 例： `switch(config-fex)# hardware N2248PQ 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 N2248PQ 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。

次に、アップリンク距離を設定する例を示します。

```
switch# configure terminal
switch(config)# fex 100
switch(config-fex)# hardware N2248PQ uplink-pause-no-drop distance 3000
switch(config-fex)#
```

低速ドレインの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **fex** *chassis_id*	指定された FEX のコンフィギュレーション 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	switch(config-fex)# **hardware** *fex* **slow-port-error-disable-time** *val*	FEX および時間しきい値を指定します。

	コマンドまたはアクション	目的
		fex 値は設定された FEX の PID です。 *val* の範囲は 200 ～ 1000 ミリ秒です。 デフォルト値は 1000 ミリ秒です。

次に、N2232P FEX での低速ドレイン機能を設定する例を示します。

```
switch# configure terminal
switch(config)# fex N2232P
switch(config-fex)# hardware N2232P slow-port-error-disable-time 500
```

FEX グローバル レベルでのロードバランシング キュー

Cisco Nexus 2248PQ は、8 つのロード バランシング キューを提供します。 これらのロード バランシング キューは、ポート輻輳を解決するように設計されています。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	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 のコンフィギュレーション 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 N2248PQ uplink-load-balance-mode** 例： `switch(config-fex)# hardware N2248PQ uplink-load-balance-mode`	ロード バランシング キューを FEX グローバル レベルでイネーブルまたはディセーブルにします。

次に、ロード バランシング キューを設定する例を示します。

```
switch# configure terminal
switch(config)# fex 100
switch(config-fex)# hardware N2248PQ uplink-load-balance-mode
switch(config-fex)#
```

第 15 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，219 ページ
- VM-FEX のライセンス要件，222 ページ
- VM-FEX のデフォルト設定，222 ページ
- VM-FEX の設定，222 ページ
- VM-FEX 設定の確認，233 ページ

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、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 ファブリック エクステンダによってサポートされます。

VM-FEX および AFEX では、FEX はファブリック PO に接続されていて、個別リンクではない必要があります。

スイッチ

VM-FEX は、Cisco Nexus デバイス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	Cisco Nexus デバイスごとに 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 です。 ライセンス付き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。

手順

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, （224 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, （225 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, （229 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, （233 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：グローバル コンフィギュレーション 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：グローバル コンフィギュレーション 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, （230 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, （232 ページ）および vCenter Server への接続の確認, （235 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, （233 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

	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	**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。
ステップ 3	**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**	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**	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**	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**	（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。

	コマンドまたはアクション	目的
ステップ 8	**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**	（任意） 特権 EXEC モードに戻ります。
ステップ 10	**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**	（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

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、固定スタティック vEthernet インターフェイスを作成できます。 固定スタティック インターフェイスの設定の詳細については、デバイスの『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次の手順を同じ設定で実行できます。

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

	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	**interface ethernet** *slot/port*	最初のイーサネット ポートのインターフェイス コンフィギュレーション モードを開始します。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	**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**	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*	2 番めのイーサネット ポートのインターフェイス コンフィギュレーション モードを開始します。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 6	**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**	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*	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コンフィギュレーションモードを開始します。
ステップ 9	**bind interface ethernet** *slot/port* **channel** *channel-number*	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。

	コマンドまたはアクション	目的
		（注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 10	**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*	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コンフィギュレーションモードを開始します。
ステップ 12	**bind interface ethernet** *slot/port* **channel** *channel-number*	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） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 13	**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*	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コンフィギュレーションモードを開始します。
ステップ 15	**bind interface ethernet** *slot/port* **channel** *channel-number*	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） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 16	**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*	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コンフィギュレーションモードを開始します。
ステップ 18	**bind interface ethernet** *slot/port* **channel** *channel-number*	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） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。

	コマンドまたはアクション	目的
ステップ 19	**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*	最初のイーサネット ポートのコンフィギュレーション モードを開始します。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 21	**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*	2 番目のイーサネット ポートのコンフィギュレーション モードを開始します。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 23	**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

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できます。 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次の手順を同じ設定で実行できます。

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

	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	**port-profile type vethernet** *profilename*	指定されたポート プロファイルのコンフィギュレーションモードを開始し、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**	（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。
ステップ 4	**switchport access vlan** *vlan-id*	（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*}	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。

	コマンドまたはアクション	目的
ステップ 6	**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**	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)#
```

vCenter Server への SVS 接続の設定

スイッチから vCenter Server への安全な接続を設定できます。

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

	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	**svs connection** *svs-name*	スイッチから vCenter Server への SVS 接続のコンフィギュレーション 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**	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。

	コマンドまたはアクション	目的
ステップ 4	**vmware dvs datacenter-name** *dc-name*	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*	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**}] • **remote hostname** *host-name* [**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。
ステップ 7	**install certificate** {**bootflash:**[//*server*/] | **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*	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_6004_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

スイッチから vCenter Server への接続をアクティブ化できます。

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

	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	**svs connection** *svs-name*	スイッチから vCenter Server への SVS 接続のコンフィギュレーション モードをイネーブルにして開始します。
ステップ 3	[**no**] **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、次のコマンドを使用します。

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。

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

	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	**show svs connections** [*svs-name*]	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_6004_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 6.0.2 build-388657


Peer Info:
----------
    hostname: -
    ip address: -
    vrf:
    protocol: -
    extension key: Cisco_Nexus_6004_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)#
```

第 16 章

MAC/ARP ハードウェア リソース カービング テンプレートの設定

この章の内容は、次のとおりです。

- MAC/ARP ハードウェア リソース カービング テンプレートについて，237 ページ
- MAC/ARP ハードウェア リソース テンプレートの設定，238 ページ
- デフォルト テンプレートの適用，239 ページ
- MAC/ARP ハードウェア リソース カービング テンプレート設定の確認，240 ページ

MAC/ARP ハードウェア リソース カービング テンプレートについて

Cisco Nexus デバイスでは、IPv4/IPv6 および unicast/multicast エントリは同じテーブルを共有します。 さらに、同じテーブルが、ステーション テーブル管理（STM）とホスト ルート テーブル（HRT）で共有されます。 STM は、MAC エントリを保持するホスト テーブルの一部です。 HRT は、ARP、IPv6 ND、および /32 ホスト ルートを保持するホスト テーブルの一部です。 STM/HRT テンプレート プロファイル機能は、Cisco Nexus デバイスに固有です。 この機能は、要件ごとに STM および HRT テーブルのサイズをカービングするための柔軟性を提供します。 合計テーブル サイズは 256k です。 次の 4 種類の定義済みテンプレートのいずれかを適用できます。

テンプレート プロファイル	仕様
hrt-128-stm-128	HRT サイズ：128k、STM サイズ：128k（デフォルト サイズ）
hrt-96-stm-160	HRT サイズ：96k、STM サイズ：160k
hrt-64-stm-192	HRT サイズ：64k、STM サイズ：192k

テンプレート プロファイル	仕様
hrt-32-stm-224	HRT サイズ：32k、STM サイズ：224k

（注） hrt-96-stm-160 および hrt-32-stm-224 テンプレート プロファイルは、IPv6 エントリが存在する場合は推奨されません。 これは、この 2 つのプロファイルを使用すると、HRT テーブルで奇数の SRAM が使用可能になるためです。 IPv6 エントリを挿入すると、連続する 2 つの SRAM 内に空き領域が必要になります。

推奨される設定値の最大 ARP 割合は 50% です。 推奨される設定値の最大 MAC 割合は 90% です。 たとえば、プロファイルが hrt-96-stm-160 に設定される場合、スイッチが使用できる最大 ARP エントリには 96k の 50%（48k）が推奨されます。

テンプレート プロファイルを適用または適用解除するときは、新しく適用されるテンプレートまたはデフォルト テンプレートをアクティブにするために、**copy running-config startup-config** コマンドを入力してスイッチをリロードする必要があります。 これらのコマンドはスイッチ単位です。そのため、vPC ピア スイッチに対して明示的に設定する必要があります。

MAC/ARP ハードウェア リソース テンプレートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **hardware profile route resource service-template** *template-name*	指定された事前定義テンプレートをコミットします。 4 種類の定義済みの stm/hrt テンプレートがあります。 • hrt-128-stm-128 デフォルト値 • hrt-96-stm-160 • hrt-64-stm-192 • hrt-32-stm-224 このコマンドを入力すると、適用される stm/hrt テンプレートがスイッチのリロード時にアクティブ化されることを通知するメッセージが表示されます。

	コマンドまたはアクション	目的
		リブート時に、この定義済みテンプレートが適用されます。 このコマンドが複数回発効された場合は、最新の stm/hrt テンプレートが適用されます。
ステップ 3	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、hrt-96-stm-160 テンプレートを設定する例を示します。

```
switch# configure terminal
switch(config)# hardware profile route resource service-template hrt-96-stm-160
switch(config)# copy running-config startup-config
```

次の作業

スイッチをリロードします。

デフォルト テンプレートの適用

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no hardware profile route resource service-template**	デフォルトのテンプレートを適用します。
ステップ 3	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次の例では、デフォルト テンプレートを設定する方法を示します。

```
switch# configure terminal
switch(config)# no hardware profile route resource service-template
switch(config)# copy running-config startup-config
```

次の作業

スイッチをリブートすると、デフォルト テンプレート（hrt-128-stm-128）が適用されます。

MAC/ARP ハードウェア リソース カービング テンプレート設定の確認

MAC/ARP ハードウェア リソース カービング テンプレート設定情報を表示するには、次のコマンドのいずれかを入力します。

コマンド	目的
show hardware profile route resource template	デフォルトを含む既存のテンプレートをすべて表示します。
show hardware profile route resource template *template-name*	特定の事前定義されたテンプレートの詳細を表示します。
show hardware profile route resource template default	デフォルトテンプレートの詳細を表示します。
show running-config hardware profile route resource template	テンプレートマネージャに関連する実行設定情報を表示します。 現在適用されているデフォルト以外の stm/hrt テンプレートを表示します。デフォルト テンプレートが適用されている場合、ここには何も表示されません。
show startup-config hardware profile route resource template	テンプレート マネージャに関連するスタートアップ設定情報を表示します。 **copy running-config startup-config** コマンドを入力すると、現在適用されているデフォルト以外の stm/hrt テンプレートが表示されます。 デフォルトテンプレートが適用されている場合は何も表示されません。

第 17 章

VN-Segment の設定

この章の内容は、次のとおりです。

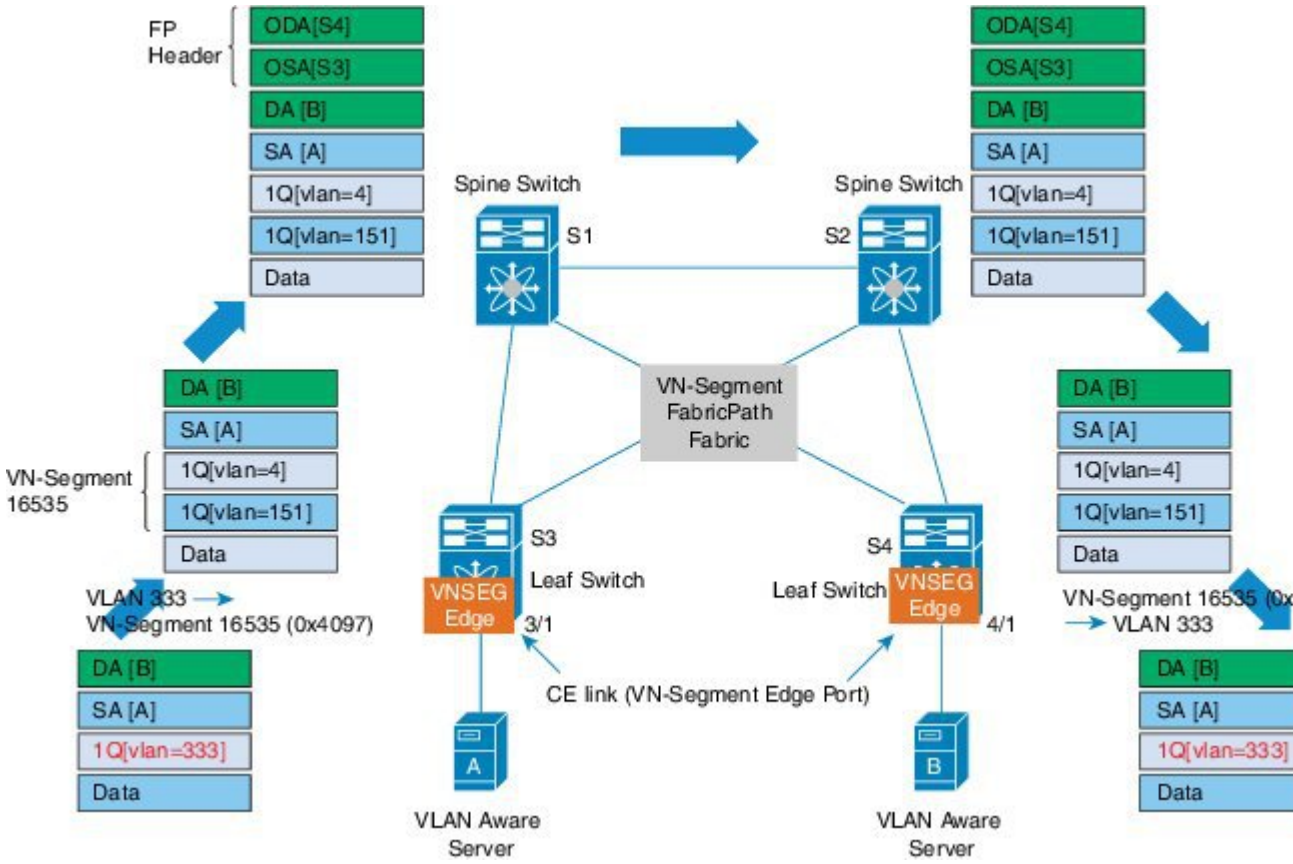
- VN-Segment について，241 ページ
- VN-Segment の注意事項と制約事項，243 ページ
- VN-Segment のイネーブル化，244 ページ
- VLAN 用の VN-Segment の設定，244 ページ
- Configure Sync での VLAN 用の VN-Segment の設定，245 ページ
- トランジット モードでの VN-Segment の設定，246 ページ
- 非トランジット モードでの VN-Segment の設定，247 ページ
- VN-Segment のディセーブル化，247 ページ
- VN-Segment 設定の確認，248 ページ

VN-Segment について

VN-Segment 機能は、従来の 802.1Q VLAN タグに代わる、回線上でパケットに「タグ付け」する新しい方法を定義したものです。 この機能では、仮想ネットワーク識別子（VNI）と呼ばれる 24 ビットのタグが使用されます。 CE リンク（アクセスとトランク）が従来の VLAN タグ付き/タグなしフレームを伝送します。 これらは VN-Segment エッジ ポートです。

FabricPath リンク（**switchport mode fabricpath**）が、VNI が定義された VLAN 用の VN-Segment タグ付きフレームを伝送します。 これらは VN-Segment コア ポートです。

図 *26*：***VN-Segment*** および ***FabricPath***



上の図に、代表的な Cisco FabricPath ネットワークを示します。 スイッチ S1 と S2 はスパイン スイッチです。 スイッチ S3 と S4 は、リーフ スイッチで、FabricPath インターフェイス経由でスパインに接続されます。 VN-Segment 機能はすべてのリーフ スイッチでイネーブルにされます。

!!!!! PD チームはスパイン設定を明確にする必要があります

!!!!! お客様が "vni" コマンドと

!!!!! "fabricpath mode transit" コマンドのどちらを使用するかを判断するにはどうしたらいいですか。

サーバ A はリーフ スイッチ S3 に接続され、サーバ B は通常のレイヤ 2 トランク/アクセス ポートを介してリーフ スイッチ S4 に接続されます。 これらのインターフェイスは、"VNSeg エッジ" ポートとも呼ばれます。 サーバは、従来の .1Q タグ付きまたはタグなしフレームを送受信します。 サーバ上の新しい設定は必要ありません。 スパインが VN-Segment タグ付きフレームを目的のリーフに転送します。

サーバ A とサーバ B は同じレイヤ 2 フラッド ドメイン内に存在しているものとします。

リーフ スイッチでは、VLAN 333 が使用可能な VN-Segment ID 16535 にマッピングされます。 この VN-Segment ID が FabricPath ネットワーク上で VLAN 333 を識別します。

一般的なパケット フローを以下に示します。

1. VLAN 333 でタグ付けされたサーバ A からサーバ B へのデータ パケットが S3 の VNSEG ポートで受信されます。
2. S3 がパケット ルックアップを実行して、スパイン宛ての FabricPath ポートにパケットを送出します。 スイッチ S3 は VLAN に対応した VN-Segment ID を使用します。
3. S1 と S2 が目的のリーフ宛ての FabricPath 転送を実行します。
4. S4 が VN-Segment ID タグ付きパケットを受信して、パケット ルックアップを実行します。 パケット宛先ポートが VNSEG エッジポートとして特定されたら、S4 はパケット内の VN-Segment ID に対応する VLAN ID を使用して、パケットを送信します。

（注） VN-Segment ID と VLAN のマッピングが存在しない場合は、パケットがドロップされます。

5. サーバ B がサーバ A から .1Q データ パケットを受信します。

サーバ B からサーバ A へのデータ パケットでも同じプロセスが実行されます。

VN-Segment の注意事項と制約事項

VN-Segment には、次の注意事項と制限事項があります。

- VN-Segment タグは FabricPath（FP）リンクを出力するトラフィックにのみ追加されます。
- データ転送動作は VLAN と同じです。
- デバイスは、適切なハードウェア サポートを伴う VN-Segment 対応のものでなければなりません。
- リーフ スイッチを VN-Segment 用に設定する必要があります。
- 仮想ネットワーク識別子（VNI）は VLAN ID ではなく、ネットワーク グローバル ID です。
- リーフ スイッチあたり最大 4K の VN-Segment とグローバル VLAN がサポートされます。 4K VLAN だけが存在します。
- ハードウェアとソフトウェアの制限により、ファブリック上でリーフごとにマッピングが異なる（最大 50K のテナントのサポートまで）可能性があります。
- イメージの互換性チェックに失敗した場合は、ISSD が拒否されます。
- 正しいトラフィック フローを実現するためには、vPC+ ピア スイッチ上の VLAN-to-VN-Segment マッピングが一貫している必要があります。 vPC タイプ 1 整合性チェックを通して、マッピングが不整合な vPC ピア スイッチ上の VLAN が停止されます。

VN-Segment のイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **install feature-set fabricpath**	スイッチで FabricPath フィーチャ セットをインストールします。
ステップ 3	switch(config)# **feature-set fabricpath**	スイッチで FabricPath フィーチャ セットをイネーブルにします。
ステップ 4	switch(config)# **feature vn-segment-vlan-based**	スイッチの VN-Segment 機能をイネーブルにします。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次の例では、VN-Segment をイネーブルにする方法を示します。

```
switch# configure terminal
switch(config)# install feature-set fabricpath
switch(config)# feature-set fabricpath
switch(config)# feature vn-segment-vlan-based

switch(config)# copy running-config startup-config
```

VLAN 用の VN-Segment の設定

はじめる前に

VN-Segment 機能をイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **vlan** *vlan-id*	VLAN を作成します。
ステップ 3	switch(config-vlan)# **mode fabricpath**	VLAN を FabricPath VLAN として設定します。 VLAN 用の VN-Segment は、リーフ上で FabricPath モードで設定する必要があります。
ステップ 4	switch(config-vlan)# **vn-segment** *segmentation-id*	ネットワーク グローバル ID を定義します。 *segmentation-id* の範囲は 4096 ～ 16,773,119 です。
ステップ 5	switch(config-vlan)# **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。

次に、VN-Segment を VLAN 用に設定する例を示します。

```
switch# configure terminal
switch(config)# vlan 100
switch(config-vlan)# mode fabricpath
switch(config-vlan)# vn-segment 4096
```

Configure Sync での VLAN 用の VN-Segment の設定

VPC 用の **configure sync** コマンドを使用して、VN-Segment を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure sync**	設定同期モードを開始します。
ステップ 2	switch(config-sync)# **switch-profile test**	所定の設定を含むスイッチ プロファイルを作成します。
ステップ 3	switch(config-sync-sp)# **vlan** *vlan-id*	VLAN を作成します。
ステップ 4	switch(config-sync-sp-vlan)# **vn-segment** *segmentation-id*	ネットワーク グローバル ID を定義します。 *segmentation-id* の範囲は 4096 ～ 16,773,119 です。

	コマンドまたはアクション	目的
ステップ 5	switch(config-sync-sp-vlan)# **commit**	（任意） 設定をピア スイッチと同期させてから、ローカルに適用します。
ステップ 6	switch(config-sync-sp-vlan)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、VN-Segment を設定同期モードで VLAN 用に設定する例を示します。

```
switch# configure sync
switch(config-sync)# switch-profile test
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# vlan 3500
switch(config-sync-sp-vlan)# vn-segment 40001
switch(config-sync-sp-vlan)#
```

トランジット モードでの VN-Segment の設定

はじめる前に

FabricPath フィーチャ セットをイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# **fabricpath mode transit**	トランジット モードをイネーブルにします。 設定を保存して、スパインをリロードする必要があります。 （注） vn-segment-vlan-based が設定されている場合は、相互排他的であるという理由でこのコマンドが拒否されます。

次に、トランジット モードで VN-Segment を設定する例を示します。

```
switch# configure terminal
switch(config)# fabricpath mode transit
Enabling transit mode. Please save configuration and reload.
```

次の作業

モードのステータスを表示するには、**show fabricpath mode** コマンドを入力します。

非トランジット モードでの VN-Segment の設定

スパインを非トランジット モードでイネーブルにするには、スパインに対して **feature vn-segment-vlan-based** コマンドを入力する必要があります。

はじめる前に

FabricPath フィーチャ セットをイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# **feature vn-segment-vlan-based**	VLAN ベースの VN-Segment をイネーブルにします。
ステップ 3	switch(config)# **vni** *vni-id*	*vni-id* の範囲は 4096 ～ 16,773,119 です。

次に、VN-Segment を非トランジット モードで設定する例を示します。

```
switch# configure terminal
switch(config)# feature vn-segment-vlan-based
switch(config)# vni 16896
```

VN-Segment のディセーブル化

はじめる前に

この機能をディセーブルにする前に、VN-Segment 設定を手動で削除する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no feature vn-segment-vlan-based**	VN-Segment をディセーブルにします。
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

	コマンドまたはアクション	目的
		レーションにコピーして、変更を永続的に保存します。

次に、VN-Segment をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature vn-segment-vlan-based
```

VN-Segment 設定の確認

VN-セグメントの設定情報を表示するには、次のコマンドを使用します:

コマンド	目的
show vlan id *vland-id-list* **vn-segment**	指定された VLAN リストの設定済みの VLAN-to-VN-Segment マッピングを表示します。
show vpc consistency-parameters global	VPC スイッチごとの VLAN 数と VN-Segment マッピングに関する情報を表示します。この情報は不整合の特定に役立ちます。
show vpc consistency-parameters vlans	VLAN 設定と VN-Segment 設定の不整合を特定するための情報を表示します。

索 引

数字

1000 Base-T イーサネット インターフェイス 191
100 Base-T イーサネット インターフェイス 191
10 ギガビット イーサネット インターフェイス 191
802.1Q VLAN 33, 46
　設定 46
　プライベート VLAN 33

A

ACL のサポート 182

B

BPDU ガード 123, 178, 186

C

CDP 178, 181
Cisco Discovery Protocol。参照先： CDP
Cisco Nexus 2148T 191
Cisco Nexus 2224PP 191
Cisco Nexus 2232PP 191
Cisco Nexus 2248TP 191
Cisco Nexus B22 Fabric Extender for IBM（NB22IBM） 191
Cisco Nexus B22 Fabric Extender for DELL（NB22DELL） 191
Cisco Nexus B22 Fabric Extender for Fujitsu（NB22FTS） 191
Cisco Nexus B22 Fabric Extender for HP（NB22HP） 191
CIST リージョナル ルート 94
CIST ルート 96
CoS 181

D

Data Center Bridging Exchange。参照先： DCBX
DCBX 181
DOM 183
drop キュー 181

E

Enhanced vPC 49, 50, 51, 52, 53, 54, 55, 56, 57, 58
　インターフェイス整合性の確認 57
　概要 49
　共通のポート チャネル番号の確認 56
　サポートされているプラットフォーム 50
　サポートされるトポロジ 50
　失敗応答 51
　スケーラビリティ 51
　設定の概要 53
　設定の確認 54
　設定例 58
　ポート チャネル番号の確認 55
　ライセンス 52

F

FEX-number 190
FEX トランク ポート 31
　PVLAN 31

I

ICMPv2 150
IEEE 802.1p 181
IEEE 802.1w 91
IEEE 802.3x 181

IGMP 152
スヌーピング パラメータ、設定 152
IGMPv1 150
IGMPv3 151
IGMP スヌーピング 151, 160, 182
MVR との相互運用性 160
問い合わせ 151

L

LACP 181
LAN インターフェイス 41
イーサネット アクセス ポート 41
LLDP 181

M

MAC アドレス 146
スタティック、設定 146
MAC アドレス設定 147
確認 147
MAC アドレス リダクション 63
MAC テーブル 146, 147
エージング タイム、設定 146
ダイナミック アドレスのクリア 147
max-links の中断 187
MST 95, 104
CIST リージョナル ルート 95
デフォルト値に設定 104
MSTP 91, 92, 94, 95, 96, 97, 104
CIST、説明 94
CIST リージョナル ルート 94
CIST ルート 96
CST 94
定義 94
リージョン間の動作 94
IEEE 802.1s 95
用語 95
IST 94
リージョン内の動作 94
MST リージョン 91, 92, 94, 96
CIST 94
サポートされるスパニングツリーインスタンス 92
説明 91
ホップ カウント メカニズム 96
VLAN から MST インスタンスへのマッピング 104
MSTP *(続き)*
境界ポート 97
説明 97
MTU 181
MVR 159, 160, 161, 162, 163, 165
IGMP スヌーピングとの相互運用性 160
vPC スヌーピングとの相互運用性 160
インターフェイスの設定 163
概要 159
グローバル パラメータの設定 162
設定の確認 165
注意事項と制約事項 161
デフォルト設定 161
ライセンス 160

N

no-drop キュー 181

P

PFC 183
pinning max-links 196
PortFast BPDU フィルタリング 123
PVLAN 31
FEX トランク ポート 31

Q

QoS 181
QoS 出力ポリシー 181
QoS ブロードキャスト クラス 181
QoS マルチキャスト クラス 181
Quality of Service。参照先： QoS
queue-limit 211, 212
グローバル レベル 211
ポート レベル 212

R

Rapid PVST+ 80
設定 80
Rapid PVST+ の設定 90
確認 90
Rapid PVST のプライオリティ 86

RSTP 67, 71, 76, 91
BPDU 76
処理 76
アクティブ トポロジ 71
高速コンバージェンス 67
ポイントツーポイント リンク 67
ルート ポート 67
指定スイッチ、定義済み 71
指定ポート、定義済み 71
提案合意ハンドシェイク プロセス 67
ルート ポート、定義済み 71

S

SFP+ 191
SFP+ インターフェイス アダプタ 191
SFP+ 検証 183
show diagnostics 205
show environment 205
show fex 202
show inventory 205
show modules 205
show SPROM 205
show transceiver status 202
Small Form-Factor Pluggable トランシーバ 191
SPAN 送信元ポート 182
SPAN の制約事項 182
STP 67, 73, 74, 121, 122
PortFast 67, 122
エッジ ポート 67, 122
概要 73, 74
ディセーブル ステート 74
フォワーディング ステート 74
ブロッキング ステート 73
ラーニング ステート 74
標準ポート 122
ネットワーク ポート 122
ポート タイプ 121
STP の概要 62
STP ブリッジ ID 63
STP ルート ガード 126

V

VLAN 7, 11, 12, 14, 33
拡張範囲 7
設定 12
VLAN *(続き)*
プライベート 33
変更 11
ポートの追加 14
予約範囲 7
VLAN の設定 16
確認 16
VLAN の予約された範囲 11
変更 11
VLAN 予約範囲 7
VM-FEX 219, 220, 222, 224, 225, 229, 230, 233, 235
vCenter 接続の確認 235
vCenter への接続 230
インターフェイス ステータスの確認 233
概要 219
機能のイネーブル化 224
固定スタティック インターフェイスの設定 225
コンポーネント 219
設定手順 222
デフォルト設定 222
ポート プロファイルの設定 229
用語 220
ライセンス 222
vPC 49, 160
MVR との相互運用性 160
拡張 49
vPC トポロジ 179

あ

アクセス VLAN 39
説明 39
アクティブ-アクティブ vPC トポロジ 179
アップリンク距離 213, 215
設定 213, 215

い

イーサネット インターフェイス 191
イーサネットのファブリック インターフェイス 177
イメージの管理 190

え

エージング タイム、設定 146
MAC テーブル 146
エッジ ポート（PortFast） 178

お

オーバーサブスクライブ比率 184
オーバーサブスクリプション 184

か

拡張範囲 VLAN 7
確認 16, 90
Rapid PVST+ の設定 90
VLAN の設定 16

き

共有バッファ 210, 214
設定 210, 214

く

クラスごとのフロー制御 181

こ

高速スパニングツリー プロトコル 91
コミュニティ VLAN 18, 20
コミュニティ ポート 19

さ

サービス クラス。参照先： CoS
最大伝送単位。参照先： MTU

し

シャーシ ID 190
シャーシ コンフィギュレーション モード 196
ジャンボ フレーム 181
手動での再配布 187
情報 237
MAC/ARP ハードウェア リソース カービング テンプレート 237
シリアル番号 196
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 179

す

スイッチポート fex-fabric モード 183
スイッチポートで保存される設定 183
スタティック MAC アドレス、設定 146
スヌーピング パラメータ、設定 152
IGMP 152

せ

静的ピン接続 187
セカンダリ VLAN 18
設定 12, 29, 30, 216, 238, 246
MAC/ARP ハードウェア リソース カービング テンプレート 238
VLAN 12
低速ドレイン 216
独立トランク ポート 30
トランジット モードの VN-Segment 246
無差別トランク ポート 29
設定データ 185
説明 39, 196
アクセス VLAN 39

た

ダイナミック アドレスのクリア 147
MAC テーブル 147
タイプ 196

て

デジタル オプティカル モニタリング。参照先： DOM
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 179

と

独立 VLAN 18, 20
独立ポート 19
トラフィック ストーム 171
　制御なし 171

ね

ネイティブ 802.1Q VLAN 46
　設定 46

は

バージョンの互換性 190
パケット数 178

ひ

ビーコン LED 199

ふ

ファブリック インターフェイス 177
ファブリック インターフェイスの表示 201
ファブリック インターフェイス ポート チャネル 189
ファブリック エクステンダの関連付け 192
フェールオーバー ロード バランシング 189
プライオリティ フロー制御。参照先： PFC
プライベート VLAN 18, 19, 20, 22, 23, 33, 179
　802.1Q VLAN 33
　エンド ステーションからのアクセス 23
　コミュニティ VLAN 18, 20
　セカンダリ VLAN 18
　独立 VLAN 18, 20
　独立トランク 22
　プライマリ VLAN 18
　ポート 19
　　コミュニティ 19
　　独立 19
　　無差別 19
　無差別トランク 22
プライマリ VLAN 18
ブリッジ ID 63
ブロードキャスト ストーム 169
ブロッキング ステート、STP 73

ほ

ポート 14
　VLAN への追加 14
ポート チャネル 189
ポート チャネルのファブリック インターフェイス 177, 183
ポート チャネル ホスト インターフェイス 177, 178
ポート番号 190
ホスト インターフェイス 177
ホスト インターフェイスの再配布 201
ホスト インターフェイスの自動ネゴシエーション 181
ホスト インターフェイスのフロー制御のデフォルト 181
ホスト インターフェイスのリンク レベル フロー制御 181
ホスト ポート 19
　種類 19

ま

マルチキャスト ストーム 169
マルチキャスト レプリケーション 186

む

無差別ポート 19

ゆ

ユニキャスト ストーム 169

ら

ライセンス 52, 160, 222
　Enhanced vPC 52
　MVR 160
　VM-FEX 222

り

リンク アグリケーション制御プロトコル。参照先： LACP

リンク障害 76, 97
　単一方向の検出 76, 97
リンク層検出プロトコル。参照先： LLDP

る

ルート ガード 126
ループバック アドレスの範囲 185
ループバック アドレスの割り当て 185

れ

レイヤ 2 スイッチング 1
　イーサネット スイッチング 1

ろ

ローカル スイッチング 186
ロードバランシング キュー 217
　グローバル レベル 217
ロケータ LED 199