Cisco IOS XE Everest 16.6.x （Catalyst 9500 スイッチ） レイヤ 2 およびレイヤ 3 コンフィギュレーション ガイド

初版：2017 年 7 月 31 日

最終更新：2017 年 11 月 3 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/

目 次

第 1 章 スパニングツリー プロトコルの設定 1

STP の制約事項 1

スパニング ツリー プロトコルに関する情報 2

Spanning Tree Protocol; スパニングツリー プロトコル 2

スパニングツリー トポロジと BPDU 3

ブリッジ ID、デバイス プライオリティ、および拡張システム ID 4

ポート プライオリティとパス コスト 5

スパニングツリー インターフェイス ステート 6

デバイス またはポートがルート デバイスまたはルート ポートになる仕組み 9

スパニングツリーおよび冗長接続 10

スパニングツリー アドレスの管理 10

接続を維持するためのエージング タイムの短縮 10

スパニングツリー モードおよびプロトコル 11

サポートされるスパニングツリー インスタンス 12

スパニングツリーの相互運用性と下位互換性 12

STP および IEEE 802.1Q トランク 13

VLAN ブリッジ スパニングツリー 13

スパニング ツリーとデバイス スタック 13

スパニングツリー機能のデフォルト設定 14

スパニングツリー機能の設定方法 15

スパニングツリー モードの変更（CLI） 15

スパニング ツリーのディセーブル化（CLI） 17

ルート デバイスの設定（CLI） 18

セカンダリ ルート デバイスの設定（CLI） 19

ポート プライオリティの設定（CLI） 21
パス コストの設定（CLI） 22
VLAN のデバイス プライオリティの設定（CLI） 24
hello タイムの設定（CLI） 25
VLAN の転送遅延時間の設定（CLI） 26
VLAN の最大エージング タイムの設定（CLI） 26
転送保留カウントの設定（CLI） 27
スパニングツリー ステータスのモニタリング 28
スパニング ツリー プロトコルに関する追加情報 29
STP の機能情報 30

第 2 章 複数のスパニング ツリー プロトコルの設定 31
機能情報の確認 31
MSTP の前提条件 31
MSTP の制約事項 32
MSTP について 33
MSTP の設定 33
MSTP 設定時の注意事項 33
ルート スイッチ 34
MST リージョン 35
IST、CIST、CST 36
MST リージョン内の動作 36
MST リージョン間の動作 37
IEEE 802.1s の用語 38
MST リージョンの図 38
ホップ カウント（Hop Count） 39
境界ポート 40
IEEE 802.1s の実装 41
ポートの役割名の変更 41
レガシーおよび規格デバイスの相互運用 41
単一方向リンク障害の検出 42

MSTP およびデバイス スタック 42
IEEE 802.1D STP との相互運用性 43
RSTP 概要 43
ポートの役割およびアクティブ トポロジ 43
高速コンバージェンス 45
ポート ロールの同期 46
ブリッジ プロトコル データ ユニットの形式および処理 47
トポロジの変更 48
プロトコル移行プロセス 49
MSTP のデフォルト設定 50
MSTP 機能の設定方法 50
MST リージョン設定の指定と MSTP のイネーブル化（CLI） 50
ルート デバイスの設定（CLI） 53
セカンダリ ルート デバイスの設定（CLI） 54
ポート プライオリティの設定（CLI） 55
パス コストの設定（CLI） 57
デバイス プライオリティの設定（CLI） 59
hello タイムの設定（CLI） 61
転送遅延時間の設定（CLI） 62
最大エージング タイムの設定（CLI） 63
最大ホップ カウントの設定（CLI） 63
高速移行を確実にするためのリンク タイプの指定（CLI） 64
ネイバー タイプの設定（CLI） 66
プロトコルの移行プロセスの再開（CLI） 67
MSTP に関する追加情報 68
MSTP の機能情報 69

第 3 章 オプションのスパニングツリー機能の設定 71
オプションのスパニングツリー機能について 71
PortFast 71
BPDU ガード 72

BPDU フィルタリング 72
UplinkFast 73
Cross-Stack UplinkFast 75
クロススタック UplinkFast の動作 75
高速コンバージェンスを発生させるイベント 77
BackboneFast 78
EtherChannel ガード 80
ルート ガード 81
ループ ガード 82
オプションのスパニングツリー機能の設定方法 82
PortFast のイネーブル化（CLI） 82
BPDU ガードのイネーブル化（CLI） 84
BPDU フィルタリングのイネーブル化（CLI） 86
冗長リンクで使用するための UplinkFast のイネーブル化（CLI） 87
UplinkFast のディセーブル化（CLI） 89
BackboneFast をイネーブル化（CLI） 90
EtherChannel ガードのイネーブル化（CLI） 91
ルート ガードのイネーブル化（CLI） 92
ループ ガードのイネーブル化（CLI） 93
スパニングツリー ステータスのモニタリング 94
オプションのスパニング ツリー機能に関する追加情報 95
オプションのスパニングツリー機能の機能情報 96

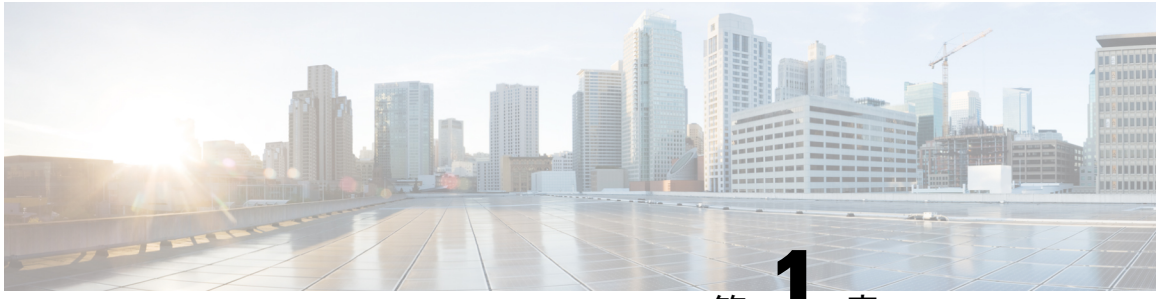
第 4 章
EtherChannel の設定 97
機能情報の確認 97
EtherChannel の制約事項 97
EtherChannel について 98
EtherChannel の概要 98
チャネル グループおよびポートチャネル インターフェイス 98
Port Aggregation Protocol; ポート集約プロトコル 100
PAgP モード 100

PAgP 学習方式およびプライオリティ 101
PAgP と他の機能との相互作用 102
リンク アグリケーション制御プロトコル 103
LACP モード 103
LACP とリンクの冗長性 104
LACP と他の機能との相互作用 105
EtherChannel の On モード 105
ロードバランシングおよび転送方式 105
MAC アドレス転送 106
IP アドレス転送 106
ロードバランシングの利点 107
EtherChannel およびデバイス スタック 108
デバイス スタックおよび PAgP 108
デバイス スタックおよび LACP 108
EtherChannel のデフォルト設定 109
EtherChannel 設定時の注意事項 110
レイヤ 2 EtherChannel 設定時の注意事項 111
レイヤ 3 EtherChannel 設定時の注意事項 112
Auto-LAG 112
Auto-LAG 設定時の注意事項 113
EtherChannel の設定方法 113
レイヤ 2 EtherChannel の設定 （CLI） 113
レイヤ 3 EtherChannel の設定 （CLI） 116
EtherChannel ロードバランシングの設定（CLI） 119
EtherChannel 拡張ロードバランシングの設定（CLI） 121
PAgP 学習方式およびプライオリティの設定 （CLI） 122
LACP ホット スタンバイ ポートの設定 123
LACP 最大バンドル機能の設定（CLI） 124
LACP ポートチャネル スタンドアロン ディセーブルの設定 125
LACP ポート チャネルの最小リンク機能の設定（CLI） 126
LACP システム プライオリティの設定（CLI） 127

LACP ポート プライオリティの設定（CLI） 128
LACP 高速レート タイマーの設定 129
グローバルな Auto-LAG の設定 131
ポート インターフェイスでの Auto-LAG の設定 132
Auto-LAG での持続性の設定 133
EtherChannel、PAgP、および LACP ステータスのモニタ 133
EtherChannel の設定例 134
レイヤ 2 EtherChannel の設定：例 134
レイヤ 3 EtherChannel の設定：例 135
LACP ホット スタンバイ ポートの設定：例 136
Auto-LAG の設定：例 136
EtherChannels の追加リファレンス 137
EtherChannels の機能情報 138

第 5 章 単方向リンク検出の設定 139
機能情報の確認 139
UDLD 設定の制約事項 139
UDLD について 140
動作モード 140
通常モード 140
Aggressive Mode 141
単一方向リンクの検出方法 141
ネイバー データベース メンテナンス 142
イベントドリブン検出およびエコー 142
UDLD リセット オプション 142
UDLD のデフォルト設定 143
UDLD の設定方法 143
UDLD のグローバルなイネーブル化（CLI） 143
インターフェイスでの UDLD のイネーブル化（CLI） 145
UDLD のモニタおよびメンテナンス 146
UDLD の追加リファレンス 146

UDLD の機能情報 147



第 1 章

スパニングツリー プロトコルの設定

- STP の制約事項 （1 ページ）
- スパニング ツリー プロトコルに関する情報 （2 ページ）
- スパニングツリー機能の設定方法 （15 ページ）
- スパニングツリー ステータスのモニタリング （28 ページ）
- スパニング ツリー プロトコルに関する追加情報 （29 ページ）
- STP の機能情報 （30 ページ）

STP の制約事項

- ルート デバイスとしてデバイスを設定しようとする場合、ルート デバイスにするために必要な値が 1 未満だと、失敗します。
- ネットワークが、拡張システム ID をサポートするデバイスとサポートしないものの両方で構成されている場合、拡張システム ID をサポートするデバイスがルート デバイスになる可能性は低くなります。古いソフトウェアを実行している接続デバイスの優先度より VLAN 番号が大きい場合は常に、拡張システム ID によってデバイス 優先度の値が増加します。
- 各スパニングツリー インスタンスのルート デバイスは、バックボーンまたはディストリビューション デバイスでなければなりません。アクセス デバイスをスパニングツリー プライマリ ルートとして設定しないでください。

関連トピック

ルート デバイスの設定（CLI） （18 ページ）

ブリッジ ID、デバイス プライオリティ、および拡張システム ID

スパニングツリー トポロジと BPDU （3 ページ）

接続を維持するためのエージング タイムの短縮 （10 ページ）

スパニング ツリー プロトコルに関する情報

Spanning Tree Protocol; スパニングツリー プロトコル

スパニングツリープロトコル（STP）は、ネットワーク内のループを回避しながらパスを冗長化するためのレイヤ2リンク管理プロトコルです。レイヤ2イーサネット ネットワークが正常に動作するには、任意の2つのステーション間で存在できるアクティブ パスは1つだけです。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、ネットワークにループが生じます。このループがネットワークに発生すると、エンドステーションにメッセージが重複して到着する可能性があります。デバイスは、複数のレイヤ 2 インターフェイスのエンド ステーション MAC アドレスを学習する可能性もあります。このような状況によって、ネットワークが不安定になります。スパニングツリーの動作は透過的であり、エンドステーション側で、単一LAN セグメントに接続されているのか、複数セグメントからなるスイッチド LAN に接続されているのかを検出することはできません。

STPは、スパニングツリーアルゴリズムを使用し、スパニングツリーのルートとして冗長接続ネットワーク内のデバイスを1つ選択します。アルゴリズムは、次に基づき、各ポートに役割を割り当て、スイッチド レイヤ 2 ネットワークを介して最良のループフリー パスを算出します。 アクティブ トポロジでのポートの役割：

- ルート：スパニングツリー トポロジに対して選定される転送ポート
- 指定：各スイッチド LAN セグメントに対して選定される転送ポート
- 代替：スパニングツリーのルート ブリッジへの代替パスとなるブロック ポート
- バックアップ：ループバック コンフィギュレーションのブロック ポート

すべてのポートに役割が指定されているデバイス、またはバックアップの役割が指定されているスイッチはルート デバイスです。 少なくとも *1* つのポートに役割が指定されているデバイスは、指定デバイスを意味します。

冗長データ パスはスパニングツリーによって、強制的にスタンバイ（ブロックされた）ステートにされます。スパニングツリーのネットワーク セグメントでエラーが発生したときに冗長パスが存在する場合は、スパニングツリー アルゴリズムがスパニングツリー トポロジを再計算し、スタンバイ パスをアクティブにします。デバイスは、スパニングツリーフレーム（ブリッジ プロトコル データ ユニット（BPDU）と呼ばれる）を定期間隔で送受信します。デバイスはこのフレームを転送しませんが、このフレームを使用してループフリーパスを構築します。BPDU には、デバイスおよび MAC アドレス、デバイスの優先順位、ポートの優先順位、およびパス コストを含む、送信側デバイスとそのポートに関する情報が含まれます。スパニングツリーはこの情報を使用して、スイッチド ネットワーク用のルート デバイスおよびルート ポートを選定し、さらに、各スイッチド セグメントのルート ポートおよび指定ポートを選定します。

デバイスの 2 つのポートがループの一部である場合、 spanning-tree および、パス コスト設定は、どのポートがフォワーディング ステートになるか、およびどのポートがブロッキング ス

テートになるかを制御します。スパニングツリー ポート プライオリティ値は、ネットワーク トポロジにおけるポートの位置とともに、トラフィック転送におけるポートの位置がどれだけ適切であるかを表します。事前定義済みの コスト値は、メディア速度を表します。

（注） デフォルトではデバイスは、Small Form-Factor Pluggable（SFP）モジュールを備えていないインターフェイスにだけ、（接続が稼働していることを確認するために）キープアライブ メッセージを送信します。[**no**] **keepalive** インターフェイス コンフィギュレーション コマンドをキーワードなしで入力すると、インターフェイスのデフォルトを変更できます。

スパニングツリー トポロジと BPDU

スイッチド ネットワーク内の安定したアクティブ スパニングツリー トポロジは、次の要素によって制御されます。

- デバイス上の各 VLAN に関連付けられた一意のブリッジ ID（デバイス優先度および MAC アドレス）。デバイス スタックでは、ある特定のスパニングツリー インスタンスに対して、すべてのデバイスが同一のブリッジ ID を使用します。
- ルート デバイスに対するスパニングツリー パス コスト。
- 各レイヤ 2 インターフェイスに対応付けられたポート ID（ポート プライオリティおよび MAC アドレス）。

ネットワーク内のデバイスに電源が入ると、各機能はルートデバイスとして機能します。各デバイスは、そのすべてのポートからコンフィギュレーション BPDU を送信します。BPDU によって通信が行われ、スパニングツリートポロジが計算されます。各設定BPDUには、次の情報が含まれています。

- 送信デバイスがルート デバイスとして識別するデバイスの一意のブリッジ ID
- ルートまでのスパニングツリー パス コスト
- 送信デバイスのブリッジ ID
- メッセージ エージ
- 送信側インターフェイス ID
- hello タイマー、転送遅延タイマー、および max-age プロトコル タイマーの値

デバイスは、優位な情報（より小さいブリッジ ID、より低いパス コストなど）が含まれているコンフィギュレーション BPDU を受信すると、そのポートに対する情報を保存します。この BPDU をデバイスのルート ポート上で受信した場合、そのデバイスが指定デバイスとなっているすべての接続 LAN に、更新したメッセージを付けて BPDU を転送します。

デバイスは、そのポートに現在保存されている情報よりも下位の情報を含むコンフィギュレーション BPDU を受信した場合は、その BPDU を廃棄します。デバイスが下位 BPDU を受信した LAN の指定デバイスである場合、そのポートに保存されている最新情報を含む BPDU をそ

の LAN に送信します。このようにして下位情報は廃棄され、優位情報がネットワークで伝播されます。

BPDU の交換によって、次の処理が行われます。

- ネットワーク内の 1 つのデバイスがとして選択されます。ルート デバイス（スイッチド ネットワークのスパニングツリー トポロジーの論理的な中心）。箇条書きの項目の下の図を参照してください。

  VLAN ごとに、デバイス優先度が最も高い（最も小さい数字の優先順位の値）デバイスがルート デバイスとして選択されます。すべてのデバイスがデフォルトの優先度（32768）で設定されている場合、VLAN 内で MAC アドレスの最も小さいデバイスがルート デバイスになります。デバイスの優先順位の値は、ブリッジ ID の最上位ビットを占めます。

- デバイスごとに（ルートデバイスを除く）、ルート ポートが 1 つ選択されます。このポートは、デバイスからルートデバイスにパケットを転送するときに最適パス（最小コスト）を提供します。

- ルート デバイスへの最短距離は、パス コストに基づいてデバイスごとに計算されます。

- LAN セグメントごとに指定デバイスが選択されます。指定デバイスは、その LAN からルート デバイスにパケットを転送するときの最小パス コストを提供します。DP は、指定デバイスが LAN に接続されているポートです。

スイッチド ネットワーク上のいずれの地点からもルート デバイスに到達する場合に必要のないパスはすべて、スパニングツリー ブロッキング モードになります。

関連トピック

ルート デバイスの設定（CLI） （18 ページ）
STP の制約事項 （1 ページ）

ブリッジ ID、デバイス プライオリティ、および拡張システム ID

IEEE 802.1D 標準では、それぞれのデバイスに固有の ルートデバイスの選択を制御するブリッジ識別子（ブリッジ ID）が必要です。各 VLAN は PVST+ と Rapid PVST+ によって異なる論理ブリッジと見なされるので、同一のデバイスは設定された各 VLAN とは異なるブリッジ ID を保有している必要があります。デバイス上の各 VLAN には一意の 8 バイト ブリッジ ID が設定されます。上位の 2 バイトはデバイス プライオリティに使用され、残りの 6 バイトがデバイスの MAC アドレスから取得されます。

従来はデバイス プライオリティに使用されていた 2 バイトが、4 ビットのプライオリティ値と 12 ビットの拡張システム ID 値（VLAN ID と同じ）に割り当てられています。

表 *1*：デバイス プライオリティ値および拡張システム *ID*

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

スパニングツリーは、ブリッジ ID を VLAN ごとに一意にするために、拡張システム ID、デバイス プライオリティ、および割り当てられたスパニングツリー MAC アドレスを使用します。

拡張システム ID のサポートにより、ルート デバイス、セカンダリ ルート デバイス、および VLAN のデバイス プライオリティの手動での設定方法に影響が生じます。たとえば、デバイスのプライオリティ値を変更すると、デバイスがルートデバイスとして選定される可能性も変更されることになります。大きい値を設定すると可能性が低下し、値が小さいと可能性が増大します。

ポート プライオリティとパス コスト

ループが発生した場合、スパニングツリーはポートプライオリティを使用して、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。最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）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に同じプライオリティ値が与えられている場合、スパニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

スパニングツリー 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に基づきます。ループが発生した場合、スパニングツリー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。最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択される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。すべてのインターフェイスに同じコスト値が与えられている場合、スパニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

デバイスがデバイス スタックのメンバーの場合は、最初に選択させたいインターフェイスには小さいコスト値を与え、最後に選択させたいインターフェイスには（ポートプライオリティを調整せずに）大きいコスト値を与えます。詳細については、関連項目を参照してください。

関連トピック

ポート プライオリティの設定（CLI） （21 ページ）
パス コストの設定（CLI） （22 ページ）

スパニングツリー インターフェイス ステート

プロトコル情報がスイッチド LAN を通過するとき、伝播遅延が生じることがあります。その結果、スイッチド ネットワークのさまざまな時点および場所でトポロジーの変化が発生します。インターフェイスがスパニングツリートポロジに含まれていない状態からフォワーディング ステートに直接移行すると、一時的にデータ ループが形成されることがあります。インターフェイスは新しいトポロジ情報がスイッチド LAN 上で伝播されるまで待機し、フレーム転送を開始する必要があります。インターフェイスはさらに、古いトポロジで使用されていた転送フレームのフレーム存続時間を満了させることも必要です。

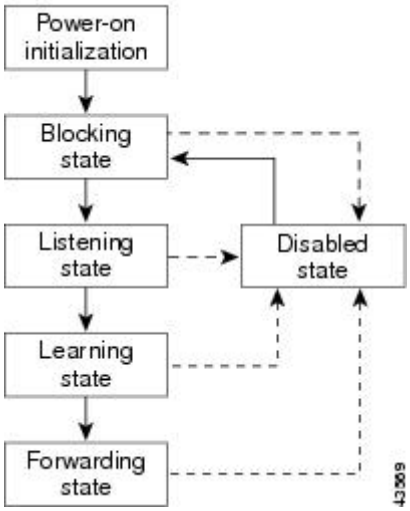
スパニングツリーを使用しているデバイスの各レイヤ2インターフェイスは、次のいずれかのステートになります。

- ブロッキング：インターフェイスはフレーム転送に関与しません。
- リスニング：インターフェイスをフレーム転送に関与させることをスパニングツリーが決定した場合、ブロッキング ステートから最初に移行するステートです。
- ラーニング：インターフェイスはフレーム転送に関与する準備をしている状態です。
- フォワーディング：インターフェイスはフレームを転送します。
- ディセーブル：インターフェイスはスパニングツリーに含まれません。シャットダウンポートであるか、ポート上にリンクがないか、またはポート上でスパニングツリーインスタンスが稼働していないためです。

インターフェイスは次のように、ステートを移行します。

- 初期化からブロッキング
- ブロッキングからリスニングまたはディセーブル
- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

図 *1*: スパニングツリー インターフェイス ステート



インターフェイスはこれらのステート間を移動します。

デフォルト設定では、デバイスを起動するとスパニングツリーが有効になります。その後、デバイスの各インターフェイス、VLAN、ネットワークがブロッキング ステートからリスニングおよびラーニングという移行ステートを通過します。スパニングツリーは、フォワーディング ステートまたはブロッキング ステートで各インターフェイスを安定させます。

スパニングツリー アルゴリズムがレイヤ 2 インターフェイスをフォワーディング ステートにする場合、次のプロセスが発生します。

1. スパニングツリーがインターフェイスをブロッキング ステートに移行させるプロトコル情報を待つ間、インターフェイスはリスニング ステートになります。
2. スパニングツリーは転送遅延タイマーの満了を待ち、インターフェイスをラーニング ステートに移行させ、転送遅延タイマーをリセットします。
3. ラーニング ステートの間、デバイスが転送データベースのエンド ステーションの位置情報を学習しているとき、インターフェイスはフレーム転送をブロックし続けます。
4. 転送遅延タイマーが満了すると、スパニングツリーはインターフェイスをフォワーディング ステートに移行させ、このときラーニングとフレーム転送の両方が可能になります。

ブロッキング ステート

ブロッキング ステートのレイヤ2インターフェイスはフレームの転送に関与しません。初期化後、デバイスの各インターフェイスにBPDUが送信されます。デバイスは最初、他のデバイスとBPDUを交換するまで、ルートとして動作します。この交換により、ネットワーク内でどのデバイスがルートまたはルートデバイスになるかが確立されます。ネットワーク内にデバイスが1つしかない場合は交換は行われず、転送遅延タイマーが満了し、インターフェイスがリスニング ステートになります。インターフェイスはデバイスの初期化後、必ずブロッキング ステートになります。

ブロッキング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

リスニング ステート

リスニング ステートは、ブロッキング ステートを経て、レイヤ 2 インターフェイスが最初に移行するステートです。インターフェイスがリスニング ステートになるのは、スパニングツリーによってそのインターフェイスのフレーム転送への関与が決定された場合です。

リスニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

ラーニング ステート

ラーニング ステートのレイヤ2インターフェイスは、フレームの転送に関与できるように準備します。インターフェイスはリスニング ステートからラーニング ステートに移行します。

ラーニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習します。
- BPDU を受信します。

フォワーディング ステート

フォワーディング ステートのレイヤ2インターフェイスは、フレームを転送します。インターフェイスはラーニング ステートからフォワーディング ステートに移行します。

フォワーディング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上でフレームを受信して転送します。
- 他のインターフェイスからスイッチングされたフレームを転送します。
- アドレスを学習します。
- BPDU を受信します。

ディセーブル ステート

ブロッキング ステートのレイヤ2インターフェイスは、フレームの転送やスパニングツリーに関与しません。ディセーブル ステートのインターフェイスは動作不能です。

ディセーブル インターフェイスは、次の機能を実行します。

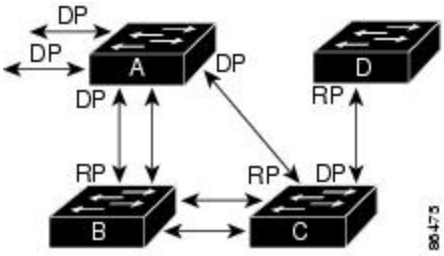
- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信しません。

デバイス またはポートがルート デバイスまたはルート ポートになる仕組み

ネットワーク上のすべてのデバイスがデフォルトのスパニングツリー設定で有効になっている場合、最小の MAC アドレスを持つデバイスがルート デバイスになります。

図 *2:* スパニングツリー トポロジ

デバイス A はルート デバイスとして選択されます。すべてのデバイスのデバイスの優先度がデフォルト（32768）に設定されており、デバイス A の MAC アドレスが最も小さいためです。ただし、トラフィック パターン、転送インターフェイスの数、またはリンク タイプによっては、デバイス A が最適なルート デバイスとは限りません。ルート デバイスになるように、最適なデバイスの優先度を引き上げる（数値を引き下げる）と、スパニングツリーの再計算が強制的に行われ、最適なデバイスをルートとした新しいトポロジが形成されます。



RP = Root Port
DP = Designated Port

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、ルート ポートよりプライオリティの高いインターフェイスに高速リンクを接続すると、ルート ポートが変更される可能性があります。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、デバイス B のあるポートがギガビット イーサネット リンクで、デバイス上の別のポート（10/100 リンク）がルート ポートであると仮定します。ネットワーク トラフィックはギガビット イーサネット リンクに流す方が効率的です。ギガビット イーサネット ポートのスパニングツリー ポート プライオリティをルート ポートより高くする（数値を小さくする）と、ギガビット イーサネット ポートが新しいルート ポートになります。

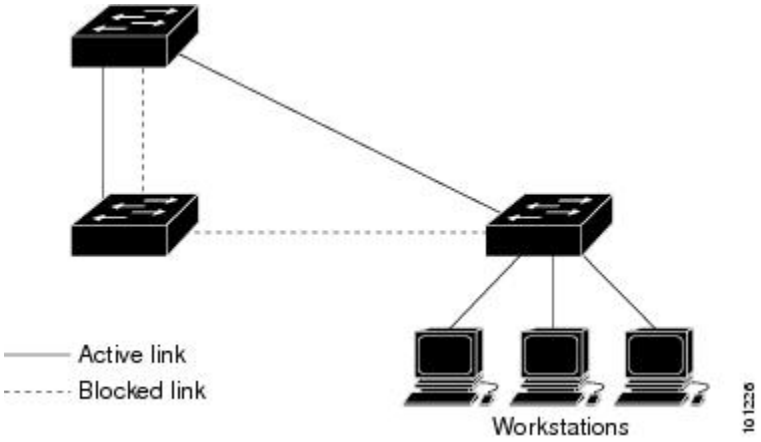
関連トピック

ポート プライオリティの設定（CLI）　（21 ページ）

スパニングツリーおよび冗長接続

図 *3:* スパニングツリーおよび冗長接続

2 つのデバイス インターフェイスを別の 1 台のデバイス、または 2 台の異なるデバイスに接続することにより、スパニングツリーを使用して冗長バックボーンを作成できます。スパニングツリーは一方のインターフェイスを自動的にディセーブルにし、他方でエラーが発生した場合にはそのディセーブルにしていた方をイネーブルにします。一方のリンクが高速で、他方が低速の場合、必ず、低速の方のリンクがディセーブルになります。速度が同じ場合、ポート優先度とポート ID が加算され、最大値を持つリンクがスパニングツリーによって無効にされます。



EtherChannel グループを使用して、デバイス間に冗長リンクを設定することもできます。

スパニングツリー アドレスの管理

IEEE 802.1D では、各種ブリッジ プロトコルに使用させるために、0x00180C2000000 ～ 0x0180C2000010 の範囲で 17 のマルチキャスト アドレスが規定されています。これらのアドレスは削除できないスタティック アドレスです。

スパニングツリー ステートに関係なく、スタック内の各デバイスは 0x0180C2000000 ～ 0x0180C2000000 のアドレス宛てのパケットを受信しますが、転送は行いません。

スパニングツリーがイネーブルの場合、デバイスまたはスタック内の各デバイスの CPU は 0x0180C2000000 および 0x0180C2000010 宛てのパケットを受信します。スパニングツリーがディセーブルの場合は、デバイスまたはスタック内の各デバイスは、それらのパケットを不明のマルチキャスト アドレスとして転送します。

接続を維持するためのエージング タイムの短縮

ダイナミック アドレスのエージング タイムはデフォルトで 5 分です。これは、**mac address-table aging-time** グローバル コンフィギュレーション コマンドのデフォルトの設定です。ただし、スパニングツリーの再構成により、多数のステーションの位置が変更されることがあります。このようなステーションは、再構成中、5 分以上にわたって到達できないことがあるので、ア

ドレステーブルからステーションアドレスを削除し、改めて学習できるように、アドレスエージング タイムが短縮されます。スパニングツリー再構成時に短縮されるエージング タイムは、転送遅延パラメータ値（**spanning-tree vlan** *vlan-id* **forward-time** *seconds* グローバル コンフィギュレーション コマンド）と同じです。

各 VLAN はそれぞれ独立したスパニングツリー インスタンスであるため、デバイスは VLAN 単位でエージング タイムを短縮します。ある VLAN でスパニングツリーの再構成が行われると、その VLAN で学習されたダイナミック アドレスがエージング タイム短縮の対象になります。他の VLAN のダイナミック アドレスは影響を受けず、デバイスで設定されたエージング間隔がそのまま保持されます。

関連トピック

ルート デバイスの設定（CLI）　（18 ページ）
STP の制約事項　（1 ページ）

スパニングツリー モードおよびプロトコル

このデバイスでサポートされるモードおよびプロトコルは、次のとおりです。

- PVST+：このスパニングツリー モードは、IEEE 802.1D 標準およびシスコ独自の拡張機能に準拠します。PVST+ はデバイス上の各 VLAN でサポートされる最大数まで動作し、各 VLAN にネットワーク上でのループフリー パスを提供します。

  PVST+ は、対象となる VLAN にレイヤ 2 ロード バランシングを提供します。ネットワーク上の VLAN を使用してさまざまな論理トポロジを作成し、特定のリンクに偏らないようにすべてのリンクを使用できるようにします。VLAN 上の PVST+ インスタンスごとに、それぞれ 1 つのルート デバイスがあります。このルート デバイスは、その VLAN に対応するスパニングツリー情報を、ネットワーク上の他のすべてのデバイスに伝送します。このプロセスにより、各デバイスがネットワークに関する共通の情報を持つため、ネットワーク トポロジが確実に維持されます。

- Rapid PVST+：Rapid PVST+ はデバイス上のデフォルトの STP モードです。このスパニングツリー モードは、IEEE 802.1w 標準に準拠した高速コンバージェンスを使用する以外は PVST+ と同じです。。高速コンバージェンスを行うため、Rapid PVST+ はトポロジ変更を受信すると、ポート単位でダイナミックに学習した MAC アドレス エントリをただちに削除します。このような場合、PVST+ では、ダイナミックに学習した MAC アドレス エントリには短いエージング タイムが使用されます。

  Rapid PVST+ は PVST+ と同じ設定を使用しているので（特に明記する場合を除く）、デバイスで必要なことは最小限の追加設定のみです。Rapid PVST+ の利点は、大規模な PVST+ のインストール ベースを Rapid PVST+ に移行する際に、複雑なマルチ スパニングツリー プロトコル（MSTP）設定の学習やネットワーク再設定の必要がないことです。Rapid PVST+ モードでは、各 VLAN は独自のスパニングツリー インスタンスを最大数実行します。

- MSTP：このスパニングツリー モードは IEEE 802.1s 標準に準拠しています。複数の VLAN を同一のスパニングツリー インスタンスにマッピングし、多数の VLAN をサポートする場合に必要となるスパニングツリーインスタンスの数を減らすことができます。MSTP は Rapid Spanning-Tree Protocol（RSTP）（IEEE 802.1w 準拠）上で実行され、転送遅延を解消し、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行するこ

とにより、スパニングツリーの高速コンバージェンスを可能にします。デバイス スタックでは、クロススタック高速移行（CSRT）機能が RSTP と同じ機能を実行します。RSTP または CSRT を使用しなければ、MSTP は稼働できません。

関連トピック

スパニングツリー モードの変更（CLI） （15 ページ）

サポートされるスパニングツリー インスタンス

PVST+ または Rapid PVST+ モードでは、デバイスまたはデバイス スタックは最大 128 のスパニングツリー インスタンスをサポートします。

MSTP モードでは、デバイスまたはデバイス スタックは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。

関連トピック

スパニング ツリーのディセーブル化（CLI） （17 ページ）
スパニングツリー機能のデフォルト設定 （14 ページ）
MSTP のデフォルト設定 （50 ページ）

スパニングツリーの相互運用性と下位互換性

MSTP および PVST+ が混在したネットワークでは、Common Spanning-Tree（CST）のルートは MST バックボーンの内側に配置する必要があり、PVST+ デバイスを複数の MST リージョンに接続することはできません。

ネットワーク内に Rapid PVST+ を実行しているデバイスと PVST+ を実行しているデバイスが存在する場合、Rapid PVST+ デバイスと PVST+ デバイスを別のスパニングツリー インスタンスに設定することを推奨します。Rapid PVST+ スパニングツリー インスタンスでは、ルートデバイスは Rapid PVST+ デバイスでなければなりません。PVST+ インスタンスでは、ルートデバイスは PVST+ デバイスでなければなりません。PVST+ デバイスはネットワークのエッジに配置する必要があります。

すべてのスタック メンバーが、同じバージョンのスパニングツリーを実行します（すべて PVST+、すべて Rapid PVST+、またはすべて MSTP）。

表 *2 : PVST+、MSTP、Rapid PVST+* の相互運用性と互換性

	PVST+	**MSTP**	**Rapid PVST+**
PVST+	○	あり（制限あり）	あり（PVST+に戻る）
MSTP	あり（制限あり）	○	あり（PVST+に戻る）
Rapid PVST+	あり（PVST+に戻る）	あり（PVST+に戻る）	○

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI） （50 ページ）
MSTP 設定時の注意事項 （33 ページ）

MST リージョン （35 ページ）

STP および IEEE 802.1Q トランク

VLAN トランクに関する IEEE 802.1Q 規格は、ネットワークのスパニングツリー ストラテジに一定の制限を設けています。この規格では、トランク上で使用できるすべての VLAN に対して、1 つのスパニングツリー インスタンスしか認められません。ただし、IEEE 802.1Q トランクを介して接続される Cisco デバイスのネットワークにおいて、デバイスはトランク上で許容される VLAN ごとに 1 つのスパニングツリー インスタンスを維持します。

IEEE 802.1Q トランクを介して Cisco デバイスを他社製のデバイスに接続する場合、Cisco デバイスは PVST+ を使用してスパニングツリーの相互運用性を実現します。Rapid PVST+ がイネーブルの場合、デバイスは PVST+ ではなく Rapid PVST+ を使用します。デバイスは、トランクの IEEE 802.1Q VLAN のスパニングツリー インスタンスと他社の IEEE 802.1Q デバイスのスパニングツリー インスタンスを結合します。

ただし、PVST+ または Rapid PVST+ の情報はすべて、他社製の IEEE 802.1Q デバイスからなるクラウドにより分離された Cisco デバイスによって維持されます。Cisco デバイスを分離する他社製の IEEE 802.1Q クラウドは、デバイス間の単一トランク リンクとして扱われます。

PVST+ は IEEE 802.1Q トランクで自動的に有効になるので、ユーザ側で設定する必要はありません。アクセス ポートおよび ISL（スイッチ間リンク）トランク ポートでの外部スパニングツリーの動作は、PVST+ の影響を受けません。

VLAN ブリッジ スパニングツリー

シスコ VLAN ブリッジ スパニングツリーは、フォールバック ブリッジング機能（ブリッジ グループ）で使用し、DECnet などの IP 以外のプロトコルを 2 つ以上の VLAN ブリッジ ドメインまたはルーテッドポート間で伝送します。VLAN ブリッジ スパニングツリーにより、ブリッジ グループは個々の VLAN スパニングツリーの上部にスパニングツリーを形成できるので、VLAN 間で複数の接続がある場合に、ループが形成されないようにします。また、ブリッジングされている VLAN からの個々のスパニングツリーが単一のスパニングツリーに縮小しないようにする働きもします。

VLAN ブリッジ スパニングツリーをサポートするには、一部のスパニングツリー タイマーを増やします。フォールバック ブリッジング機能を使用するには、デバイスでネットワーク アドバンテージ ライセンスを有効にする必要があります。

スパニング ツリーとデバイス スタック

デバイス スタックが PVST+ または Rapid PVST+ モードで動作している場合：

- デバイス スタックは、ネットワークのその他の部分に対しては単一のスパニングツリー ノードに見え、すべてのスタック メンバーが与えられたスパニングツリーに同一のブリッジ ID を使用します。ブリッジ ID は、アクティブ スイッチの MAC アドレスから取得されます。
- 新しいデバイスがスタックに加わると、そのスイッチは、アクティブ スイッチのブリッジ ID を自分のブリッジ ID として設定します。新しく追加されたデバイスの ID が最も小さ

く、ルート パス コストがすべてのスタック メンバー間で同じ場合は、新しく追加されたデバイスがスタック ルートになります。

- スタック メンバがスタックから除外されると、スタック内でスパニングツリーの再コンバージェンスが発生します（スタック外で発生する場合もあります）。残っているスタック メンバのうち最も低いスタック ポート ID を持つスタック メンバが、スタック ルートになります。
- デバイス スタックがスパニング ツリー ルートで、アクティブ スイッチで障害が発生した、またはスタックから外れた場合、スタンバイ スイッチが新しいアクティブ スイッチになり、ブリッジ ID は同じままで、スパニング ツリーの再コンバージェンスが発生する可能性があります。
- デバイス スタック外にあるネイバー デバイスに障害が発生したか、またはその電源が停止した場合、通常のスパニングツリー処理が発生します。スパニングツリーの再コンバージェンスは、アクティブなトポロジ内のデバイスが失われたことにより発生する場合もあります。
- デバイス スタック外にある新しい デバイスがネットワークに追加された場合、通常のスパニングツリー処理が発生します。スパニングツリーの再コンバージェンスは、ネットワークにデバイスが追加されたことにより発生する場合もあります。

スパニングツリー機能のデフォルト設定

表 *3:* スパニングツリー機能のデフォルト設定

機能	デフォルト設定
イネーブル ステート	VLAN 1 上でイネーブル
スパニングツリー モード	Rapid PVST+（PVST+ と MSTP はディセーブル）
デバイス priority	32768
スパニングツリー ポート プライオリティ（インターフェイス単位で設定可能）	128
スパニングツリー ポート コスト（インターフェイス単位で設定可能）	1000 Mb/s：4 100 Mb/s：19 10 Mb/s：100
スパニングツリー VLAN ポート プライオリティ（VLAN 単位で設定可能）	128

機能	デフォルト設定
スパニングツリー VLAN ポート コスト（VLAN 単位で設定可能）	1000 Mb/s：4 100 Mb/s：19 10 Mb/s：100
スパニングツリー タイマー	hello タイム：2 秒 転送遅延時間：15 秒 最大エージング タイム：20 秒 転送保留カウント：6 BPDU

（注） Cisco IOS Release 15.2(4)E 以降では、デフォルトの STP モードは Rapid PVST+ です。

関連トピック

スパニング ツリーのディセーブル化（CLI） （17 ページ）
サポートされるスパニングツリー インスタンス （12 ページ）

スパニングツリー機能の設定方法

スパニングツリー モードの変更（CLI）

スイッチは次の 3 つのスパニングツリー モードをサポートします。Per-VLAN Spanning-Tree Plus（PVST+）、Rapid PVST+、またはマルチ スパニングツリープロトコル（MSTP）。デフォルトでは、デバイスは Rapid PVST+ プロトコルを実行します。

デフォルト モード以外のモードをイネーブルにする場合、この手順は必須です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例：	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
	`Device# configure terminal`	
ステップ 3	**spanning-tree mode {pvst | mst | rapid-pvst}** 例： `Device(config)# spanning-tree mode pvst`	スパニングツリーモードを設定します。 すべてのスタック メンバーは、同じバージョンのスパニング ツリーを実行します。 • PVST+ をイネーブルにするには、**pvst** を選択します。 • MSTP をイネーブルにするには、**mst** を選択します。 • **rapid-pvst** を選択して、Rapid PVST+ をイネーブルにします。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet1/0/1`	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。有効なインターフェイスとしては、物理ポート、VLAN、ポート チャネルなどがあります。VLAN ID の範囲は 1 ～ 4094 です。指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 5	**spanning-tree link-type point-to-point** 例： `Device(config-if)# spanning-tree link-type point-to-point`	このポートのリンク タイプがポイントツーポイントであることを指定します。 このポート（ローカル ポート）をポイントツーポイント リンクでリモート ポートと接続し、ローカル ポートが指定ポートになると、デバイスはリモート ポートとネゴシエーションし、ローカル ポートをフォワーディング ステートにすばやく変更します。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**clear spanning-tree detected-protocols** 例：	デバイス上のいずれかのポートが IEEE 802.1D レガシー デバイス上のポートに接続されている場合は、このコマンドに

	コマンドまたはアクション	目的
	`Device# clear spanning-tree detected-protocols`	よりデバイス全体のプロトコル移行プロセスを再開します。 このステップは、このデバイスで Rapid PVST+ が稼働していることを指定デバイスが検出する場合のオプションです。

関連トピック

スパニングツリー モードおよびプロトコル （11 ページ）

スパニング ツリーのディセーブル化（CLI）

スパニングツリーはデフォルトで、VLAN 1 およびスパニングツリー限度を上限として新しく作成されたすべての VLAN 上でイネーブルです。スパニングツリーをディセーブルにするのは、ネットワーク トポロジにループがないことが確実な場合だけにしてください。

注意 スパニングツリーがディセーブルでありながら、トポロジにループが存在していると、余分なトラフィックが発生し、パケットの重複が無限に繰り返されることによって、ネットワークのパフォーマンスが大幅に低下します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**no spanning-tree vlan** *vlan-id* 例： `Device(config)# no spanning-tree vlan 300`	*vlan-id* に指定できる範囲は 1 ～ 4094 です。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

サポートされるスパニングツリー インスタンス （12 ページ）
スパニングツリー機能のデフォルト設定 （14 ページ）

ルート デバイスの設定（CLI）

特定の VLAN でデバイスをルートとして設定するには、**spanning-tree vlan** *vlan-id***root** グローバル コンフィギュレーション コマンドを使用して、デバイス プライオリティをデフォルト値（32768）から、それより大幅に小さい値に変更します。このコマンドを入力すると、ソフトウェアが各 VLAN について、ルート デバイスのデバイス プライオリティを確認します。拡張システム ID をサポートするため、デバイスは指定された VLAN の自身のプライオリティを 24576 に設定します。この値によって、このデバイスを指定された VLAN のルートに設定できます。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間の最大デバイス ホップ カウント）を指定するには、**diameter** キーワードを使用します。ネットワーク直径を指定すると、デバイスはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に設定します。その結果、コンバージェンスに要する時間が大幅に短縮されます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree vlan** *vlan-id***root primary** [**diameter** *net-diameter* 例： `Device(config)# spanning-tree vlan 20-24 root primary diameter 4`	指定された VLAN のルートになるように、デバイスを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • （オプション）**diameter** *net-diameter* には、任意の 2 つのエンド ステーション間の最大デバイス数を指定します。範囲は 2 ～ 7 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

次のタスク

デバイスをルート デバイスに設定した後に、hello タイム、転送遅延時間、最大エージング タイムを、**spanning-tree vlan** *vlan-id***hello-time**、**spanning-tree vlan** *vlan-id***forward-time**、および **spanning-tree vlan** *vlan-id***max-age** グローバル コンフィギュレーション コマンドを使用して手動で設定することは推奨しません。

関連トピック

ブリッジ ID、デバイス プライオリティ、および拡張システム ID
スパニングツリー トポロジと BPDU （3 ページ）
接続を維持するためのエージング タイムの短縮 （10 ページ）
STP の制約事項 （1 ページ）

セカンダリ ルート デバイスの設定（CLI）

デバイスをセカンダリ ルートとして設定すると、デバイス プライオリティがデフォルト値（32768）から 28672 に変更されます。このプライオリティでは、デバイスがプライマリ ルート デバイスが失敗した場合の、指定された VLAN のルートデバイスになる可能性があります。ここでは、その他のネットワーク デバイスが、デフォルトのデバイス プライオリティの 32768 を使用しているためにルート デバイスになる可能性が低いことが前提となっています。

このコマンドを複数のデバイスに対して実行すると、複数のバックアップ ルート デバイスを設定できます。**spanning-tree vlan** *vlan-id***root primary** グローバル コンフィギュレーション コ

マンドでプライマリ ルート デバイスを設定したときと同じネットワーク直径および hello タイム値を使用してください。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree vlan** *vlan-id***root secondary** [**diameter** *net-diameter* 例： `Device(config)# spanning-tree vlan 20-24 root secondary diameter 4`	指定された VLAN のセカンダリ ルートになるように、デバイスを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • （オプション）**diameter** *net-diameter* には、任意の 2 つのエンド ステーション間の最大デバイス数を指定します。指定できる範囲は 2 ～ 7 です。 プライマリ ルート デバイスを設定したときと同じネットワーク直径を使用してください。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ポート プライオリティの設定（CLI）

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	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。 有効なインターフェイスは、物理ポートおよびポートチャネル論理インターフェイス（**port-channel** *port-channel-number*）です。
ステップ 4	**spanning-tree port-priority** *[プライオリティ（priority）]* 例： `Device(config-if)# spanning-tree port-priority 0`	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* に指定できる範囲は 0 ～ 240 で、16 ずつ増加します。デフォルトは 128 です。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。その他の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。
ステップ 5	**spanning-treevlan** *vlan-id* **port-priority** *priority* 例： `Device(config-if)# spanning-tree vlan 20-25 port-priority 0`	VLAN のポート プライオリティを設定します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。

	コマンドまたはアクション	目的
		• *priority* に指定できる範囲は 0 ～ 240 で、16 ずつ増加します。デフォルトは 128 です。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。その他の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

ポート プライオリティとパス コスト （5 ページ）
デバイス またはポートがルート デバイスまたはルート ポートになる仕組み （9 ページ）

パス コストの設定（CLI）

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	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。有効なインターフェイスは、物理ポートおよびポート チャネル論理インターフェイス

	コマンドまたはアクション	目的
		（**port-channel** *port-channel-number*）です。
ステップ 4	**spanning-tree cost** *cost* 例： `Device(config-if)# spanning-tree cost 250`	インターフェイスのコストを設定します。 ループが発生した場合、スパニングツリーはパスコストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 5	**spanning-tree vlan** *vlan-id***cost** *cost* 例： `Device(config-if)# spanning-tree vlan 10,12-15,20 cost 300`	VLAN のコストを設定します。 ループが発生した場合、スパニングツリーはパスコストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 • *vlan-id* には、VLAN ID 番号で識別された単一のVLAN、ハイフンで区切られた範囲のVLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は1～4094 です。 • *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

show spanning-treeinterface *interface-id* 特権 EXEC コマンドによって表示されるのは、リンクアップ動作可能状態のポートの情報だけです。そうでない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

関連トピック

ポート プライオリティとパス コスト （5 ページ）

VLAN のデバイス プライオリティの設定（CLI）

デバイス プライオリティを設定して、スタンドアロン デバイスまたはスタックにあるデバイスがルート デバイスとして選択される可能性を高めることができます。

（注） このコマンドの使用には注意してください。多くの場合、**spanning-tree vlan** *vlan-id***root primary** および **spanning-tree vlan** *vlan-id***root secondary** グローバル コンフィギュレーション コマンドを使用して、デバイスのプライオリティを変更することを推奨します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree vlan** *vlan-id***priority** *priority* 例： `Device(config)# spanning-tree vlan 20 priority 8192`	VLAN のデバイス プライオリティの設定 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *priority* の範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。この値が低いほど、デバイスがルート デバイスとして選択される可能性が高くなります。 有効なプライオリティ値は 4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、

	コマンドまたはアクション	目的
		57344、61440 です。その他の値はすべて拒否されます。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

hello タイムの設定（CLI）

hello タイムはルート デバイスによって設定メッセージが生成されて送信される時間の間隔です。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**spanning-tree vlan** *vlan-id* **hello-time** *seconds* 例： `Device(config)# spanning-tree vlan 20-24 hello-time 3`	VLAN の hello タイムを設定します。hello タイムはルート デバイスによって設定メッセージが生成されて送信される時間の間隔です。このメッセージは、デバイスが活動中であることを表します。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 3	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

VLAN の転送遅延時間の設定（CLI）

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree vlan** *vlan-id* **forward-time** *seconds* 例： `Device(config)# spanning-tree vlan 20,25 forward-time 18`	VLAN の転送時間を設定します。転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、インターフェイスが待機する秒数です。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 4 ～ 30 です。デフォルトは 15 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

VLAN の最大エージング タイムの設定（CLI）

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree vlan** *vlan-id* **max-age** *seconds* 例： `Device(config)# spanning-tree vlan 20 max-age 30`	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 タイムは、デバイスが再設定を試す前にスパニングツリー設定メッセージを受信せずに待機する秒数です。 • *vlan-id* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • *seconds* に指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

転送保留カウントの設定（CLI）

転送保留カウント値を変更することで、BPDU のバースト サイズを設定できます。

（注） このパラメータをより高い値に変更すると、（特に Rapid PVST+ モードで）CPU の使用率に大きく影響します。逆に、この値を低く設定すると、セッションによってはコンバージェンスを抑えることができます。この値は、デフォルト設定で使用することを推奨します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree transmit hold-count** *value* 例： `Device(config)# spanning-tree transmit hold-count 6`	1 秒間停止する前に送信できる BPDU 数を設定します。 *value* に指定できる範囲は 1 ～ 20 です。デフォルト値は 6 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

スパニングツリー ステータスのモニタリング

表 *4:* スパニングツリー ステータス表示用のコマンド

show spanning-tree active	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree vlan *vlan-id*	指定した VLAN のスパニング ツリー情報を表示します。
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree interface *interface-id* **portfast**	指定したインターフェイスのスパニングツリー portfast 情報を表示します。

show spanning-tree summary [**totals**]	インターフェイス ステートのサマリーを表示します。または STP ステート セクションのすべての行を表示します。

スパニングツリー カウンタをクリアするには、**clear spanning-tree** [**interface** *interface-id*] 特権 EXEC コマンドを使用します。

スパニング ツリー プロトコルに関する追加情報

関連資料

関連項目	参照先
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9500 Series Switches)* の「Layer 2/3 Commands」の項を参照してください

標準および RFC

標準/RFC	役職（Title）
なし	—

MIB

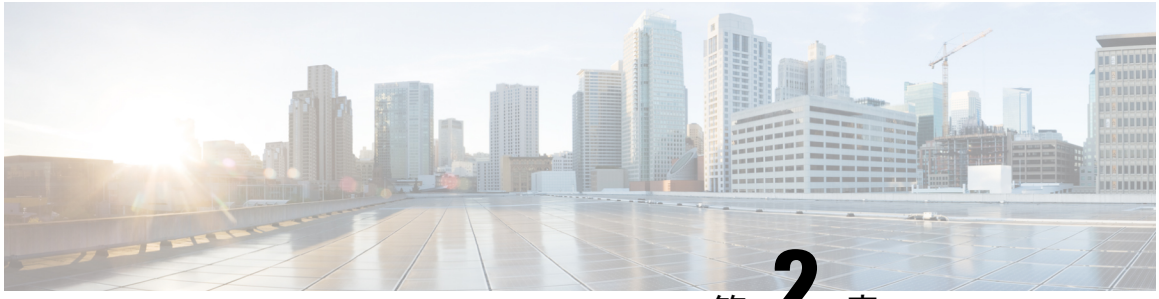
MIB	MIB リンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

STP の機能情報

リリース	変更箇所
Cisco IOS XE Everest 16.5.1a	この機能が導入されました。



第 2 章

複数のスパニング ツリー プロトコルの設定

- 機能情報の確認 （31 ページ）
- MSTP の前提条件 （31 ページ）
- MSTP の制約事項 （32 ページ）
- MSTP について （33 ページ）
- MSTP 機能の設定方法 （50 ページ）
- MSTP に関する追加情報 （68 ページ）
- MSTP の機能情報 （69 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびCisco ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

MSTP の前提条件

- 2 つ以上のデバイスを同じマルチスパニングツリー（MST）リージョンに設定するには、その 2 つに同じ VLAN/インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。
- ネットワーク内の冗長パスでロード バランシングを機能させるには、すべての VLAN/インスタンスマッピングの割り当てが一致している必要があります。一致していないと、すべてのトラフィックが 1 つのリンク上で伝送されます。

- Per-VLAN Spanning-Tree Plus（PVST+）と MST クラウドの間、または Rapid- PVST+ と MST クラウドの間でロードバランシングが機能するためには、すべての MST 境界ポートがフォワーディングでなければなりません。MST クラウドの内部スパニングツリー（IST）マスターが共通スパニング ツリー（CST）のルートである場合、MST 境界ポートはフォワーディングです。MST クラウドが複数の MST リージョンから構成されている場合、いずれかの MST リージョンに CST ルートを含める必要があり、その他すべての MST リージョンに、PVST+ クラウドまたは高速 PVST+ クラウドを通るパスよりも、MST クラウド内に含まれるルートへのパスが良くする必要があります。クラウド内のデバイスを手動で設定しなければならない場合もあります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI） （50 ページ）
MSTP 設定時の注意事項 （33 ページ）
MST リージョン （35 ページ）

MSTP の制約事項

- デバイス スタックは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。
- PVST+、Rapid PVST+、および MSTP はサポートされますが、アクティブにできるのは 1 つのバージョンだけです（たとえば、すべての VLAN で PVST+ を実行する、すべての VLAN で Rapid PVST+ を実行する、またはすべての VLAN で MSTP を実行します）。
- MST コンフィギュレーションの VLAN トランキング プロトコル（VTP）伝搬はサポートされません。ただし、コマンドライン インターフェイス（CLI）または簡易ネットワーク管理プロトコル（SNMP）サポートを通じて、MST リージョン内の各デバイスで MST コンフィギュレーション（リージョン名、リビジョン番号、および VLAN とインスタンスのマッピング）を手動で設定することは可能です。
- ネットワークを多数のリージョンに分割することは推奨できません。ただし、どうしても分割せざるを得ない場合は、スイッチド LAN をルータまたは非レイヤ 2 デバイスで相互接続された小規模な LAN に分割することを推奨します。
- リージョンは、同じ MST コンフィギュレーションを持つ 1 つまたは複数のメンバーで構成されます。リージョンの各メンバーは高速スパニングツリープロトコル（RSTP）ブリッジ プロトコル データ ユニット（BPDU）を処理する機能を備えている必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリー インスタンスの数は 65 までです。VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI） （50 ページ）
MSTP 設定時の注意事項 （33 ページ）
MST リージョン （35 ページ）

ルート デバイスの設定（CLI） （53 ページ）
ルート スイッチ （34 ページ）

MSTP について

MSTP の設定

高速コンバージェンスのために RSTP を使用する MSTP では、複数の VLAN をグループ化して同じスパニングツリーインスタンスにマッピングすることが可能で、多くのVLANをサポートするのに必要なスパニングツリー インスタンスの数を軽減できます。MSTP は、データ トラフィックに複数の転送パスを提供し、ロード バランシングを実現して、多数の VLAN をサポートするのに必要なスパニングツリーインスタンスの数を減らすことができます。MSTP を使用すると、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）は影響を受けないので、ネットワークのフォールトトレランスが向上します。

（注） マルチ スパニングツリー（MST）実装は IEEE 802.1s 標準に準拠しています。

MSTP を導入する場合、最も一般的なのは、レイヤ 2 スイッチド ネットワークのバックボーンおよびディストリビューション レイヤへの導入です。MSTP の導入により、サービス プロバイダー環境に求められる高可用性ネットワークを実現できます。

デバイスが MST モードの場合、IEEE 802.1w 準拠の RSTP が自動的にイネーブルになります。RSTP は、IEEE 802.1D の転送遅延を軽減し、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行する明示的なハンドシェイクによって、スパニングツリーの高速コンバージェンスを実現します。

MSTP と RSTP は、既存のシスコ独自の Multiple Instance STP（MISTP）、および既存の Cisco PVST+ と Rapid Per-VLAN Spanning-Tree plux（Rapid PVST+）を使用して、スパニングツリーの動作を改善し、（オリジナルの）IEEE 802.1D スパニング ツリーに準拠した機器との下位互換性を保持しています。

デバイス スタックは、ネットワークのその他の部分に対しては単一のスパニングツリー ノードに見え、すべてのスタック メンバーが同一のデバイス ID を使用します。

MSTP 設定時の注意事項

- **spanning-tree mode mst** グローバル コンフィギュレーション コマンドを使用して、MST をイネーブルにすると、RSTP が自動的にイネーブルになります。
- UplinkFast、BackboneFast、クロススタック UplinkFast の設定のガイドラインについては、関連項目のセクションの該当するセクションを参照してください。

- デバイスが MST モードの場合は、パス コスト値の計算に、ロング パス コスト計算方式（32 ビット）が使用されます。ロング パス コスト計算方式では、次のパス コスト値がサポートされます。

速度	パス コスト値
10 Mb/s	2,000,000
100 Mb/s	200,000
1 Gb/s	20,000
10 Gb/s	2,000
100 Gb/s	200

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）（50 ページ）
MSTP の前提条件（31 ページ）
MSTP の制約事項（32 ページ）
スパニングツリーの相互運用性と下位互換性（12 ページ）
オプションのスパニングツリー設定時の注意事項
BackboneFast（78 ページ）
UplinkFast（73 ページ）

ルート スイッチ

デバイスは、マッピングされている VLAN グループのスパニングツリー インスタンスを保持しています。デバイス ID は、デバイスのプライオリティおよびデバイスの MAC アドレスで構成されており、各インスタンスに関連付けられます。VLAN のグループでは、最小のデバイス ID をもつデバイスがルート デバイスになります。

デバイスをルートとして設定する場合は、デバイス プライオリティをデフォルト値（32768）からそれより大幅に低い値に変更し、デバイスが、指定したスパニング ツリー インスタンスのルート デバイスになるようにします。このコマンドを入力すると、デバイスはルート デバイスのデバイス プライオリティをチェックします。拡張システム ID をサポートしているため、24576 という値でデバイスが指定したスパニングツリー インスタンスのルートとなる場合、そのデバイスは指定したインスタンスに対する自身のプライオリティを 24576 に設定します。

指定されたインスタンスのルート デバイスに 24576 に満たないデバイス プライオリティが設定されている場合は、デバイスは自身のプライオリティを最小のデバイスプライオリティより 4096 だけ小さい値に設定します（4096 は 4 ビット デバイス プライオリティの最下位ビットの値です）。詳細については、関連項目の「ブリッジ ID、スイッチ プライオリティ、および拡張システム IDデバイス」リンクを参照してください。

ネットワークが、拡張システム ID をサポートするデバイスとサポートしないものの両方で構成されている場合、拡張システム ID をサポートするデバイスがルート デバイスになる可能性は低くなります。古いソフトウェアを実行している接続デバイスのプライオリティより VLAN 番号が大きい場合は常に、拡張システム ID によってスイッチ プライオリティ値が増加します。

各スパニングツリーインスタンスのルートデバイスは、バックボーンまたはディストリビューション デバイスでなければなりません。アクセス デバイスをスパニングツリー プライマリ ルートとして設定しないでください。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間の最大デバイス ホップ カウント）を指定するには、**diameter** キーワード（MST インスタンスが 0 の場合のみ使用できる）を指定します。ネットワーク直径を指定すると、デバイスはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に設定します。その結果、コンバージェンスに要する時間が大幅に短縮されます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

関連トピック

ルート デバイスの設定（CLI） （53 ページ）
MSTP の制約事項 （32 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID

MST リージョン

スイッチを MST インスタンスに加入させるには、同じ MST コンフィギュレーション情報を使用して矛盾のないようにスイッチを設定する必要があります。同じ MST 設定の相互接続スイッチの集まりによって MST リージョンが構成されます。

MST 設定では、それぞれのデバイスが属する MST リージョンが制御されます。この設定には、領域の名前、バージョン番号、MST VLAN とインスタンスの割り当てマップが含まれます。その中で MST リージョンの設定を指定することにより、リージョンのデバイスを設定します。MST インスタンスに VLAN をマッピングし、リージョン名を指定して、リビジョン番号を設定できます。手順と例については、関連項目の「MST リージョン設定の指定と MSTP のイネーブル化」リンクをクリックします。

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。さらに、各メンバは、RSTP ブリッジプロトコルデータ ユニット（BPDU）を処理できる必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリーインスタンスの数は 65 までです。インスタンスは、0 ～ 4094 の範囲の任意の番号で識別できます。VLAN には、一度に 1 つのスパニングツリーインスタンスのみ割り当てることができます。

関連トピック

MST リージョンの図 （38 ページ）
MST リージョン設定の指定と MSTP のイネーブル化（CLI） （50 ページ）
MSTP の前提条件 （31 ページ）

MSTP の制約事項 （32 ページ）
スパニングツリーの相互運用性と下位互換性 （12 ページ）
オプションのスパニングツリー設定時の注意事項
BackboneFast （78 ページ）
UplinkFast （73 ページ）

IST、CIST、CST

すべてのスパニングツリー インスタンスが独立している PVST+ および Rapid PVST+ とは異なり、MSTP は次の 2 つのタイプのスパニングツリーを確立して保持しています。

- Internal Spanning-Tree（IST）は、1 つの MST リージョン内で稼働するスパニングツリーです。

  各 MST リージョン内の MSTP は複数のスパニングツリー インスタンスを維持しています。インスタンス 0 は、リージョンの特殊なインスタンスで、IST と呼ばれています。その他すべての MSTI には、1 ～ 4094 の番号が付きます。

  IST は、BPDU を送受信する唯一のスパニングツリー インスタンスです。他のスパニングツリーの情報はすべて、MSTP BPDU 内にカプセル化されている M レコードに格納されています。MSTP BPDU はすべてのインスタンスの情報を伝送するので、複数のスパニングツリー インスタンスをサポートする処理が必要な BPDU の数を大幅に減少できます。

  同一リージョン内のすべての MST インスタンスは同じプロトコル タイマーを共有しますが、各 MST インスタンスは独自のトポロジ パラメータ（ルート デバイス ID、ルート パス コストなど）を持っています。デフォルトでは、すべての VLAN が IST に割り当てられます。

  MSTI はリージョンにローカルです。たとえばリージョン A およびリージョン B が相互接続されていても、リージョン A の MSTI 1 は、リージョン B の MSTI 1 に依存しません。

- Common and Internal Spanning-Tree（CIST）は、各 MST リージョン内の IST と、MST リージョンおよびシングル スパニングツリーを相互接続する Common Spanning-Tree（CST）の集合です。

  1 つのリージョン内で計算されたスパニングツリーは、スイッチド ドメイン全体を網羅する CST のサブツリーと見なされます。CIST は、IEEE 802.1w、IEEE 802.1s、および IEEE 802.1D 標準をサポートするスイッチ間で実行されるスパニングツリー アルゴリズムによって形成されます。MST リージョン内の CIST は、リージョン外の CST と同じです。

MST リージョン内の動作

IST は 1 つのリージョン内のすべての MSTP スイッチを接続します。IST が収束すると、IST のルートは、CIST リージョナル ルート（IEEE 802.1s 標準が実装される以前は *IST* マスターと呼ばれた）になります。これは、リージョン内で最も小さいデバイス ID、および CIST ルートに対するパス コストをもつデバイスです。ネットワークに領域が 1 つしかない場合、CIST リージョナル ルートは CIST ルートにもなります。CIST ルートがリージョンの外部にある場合、

リージョンの境界に位置する MSTP スイッチの 1 つが CIST リージョナル ルートとして選択されます。

MSTP デバイスは初期化時に、自身が CIST のルートおよび CIST リージョナル ルートであることを主張するために CIST ルートと CIST リージョナル ルートへのパス コストがいずれもゼロに設定された BPDU を送信します。デバイスはすべての MSTI を初期化し、そのすべてのルートであることを主張します。デバイスは、ポート用に現在保存されているものより上位の MST ルート情報（低いデバイス ID、低いパス コストなど）を受信した場合、CIST リージョナル ルートとしての主張を放棄します。

リージョンには、初期化中に多くのサブ リージョンが含まれて、それぞれに独自の CIST リージョナル ルートが含まれることがあります。スイッチは、優位の IST 情報を受信すると、古いサブリージョンを脱退して、真の CIST リージョナル ルートが含まれている新しいサブリージョンに加入します。真の CIST リージョナル ルートが含まれている以外のサブリージョンは、すべて縮小します。

正常な動作のためには、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。共通の CIST リージョナル ルートに収束する場合、そのリージョン内にある 2 つのスイッチは、1 つの MST インスタンスに対するポートの役割のみを同期させます。

関連トピック

MST リージョンの図 （38 ページ）

MST リージョン間の動作

ネットワーク内に複数のリージョンまたはレガシー IEEE 802.1D デバイスが混在している場合、MSTP は、ネットワーク内のすべての MST リージョンとすべてのレガシー STP デバイスから構成される CST を構築して保持します。MSTI は、リージョンの境界にある IST と組み合わさり、CST になります。

IST はリージョン内のすべての MSTP デバイスを接続し、スイッチド ドメイン全体を囲む CIST 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 デバイスおよび MST リージョンへの仮想デバイスとして認識されます。

CST インスタンスのみが BPDU を送受信し、MST インスタンスはスパニングツリー情報を BPDU に追加して隣接するデバイスと相互作用し、最終的なスパニングツリー トポロジを算出します。したがって、BPDU 伝送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 インスタンスだけで設定されますが、その影響はすべての MST インスタンスに及びます。スパニングツリー トポロジに関連するパラメータ（デバイス 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 MST インスタンスの両方で設定できます。

MSTP デバイスは、バージョン 3 RSTP BPDU または IEEE 802.1D STP BPDU を使用して、レガシー IEEE 802.1D デバイスと通信します。MSTP デバイスは、MSTP BPDU を使用して MSTP デバイスと通信します。

関連トピック

MST リージョンの図 （38 ページ）

IEEE 802.1s の用語

シスコの先行標準実装で使用される一部のMST命名規則は、一部の内部パラメータまたはリージョンパラメータを識別するように変更されました。これらのパラメータは、ネットワーク全体に関連している外部パラメータと違い、MST リージョン内でのみ影響があります。CIST はネットワーク全体を網羅するスパニングツリー インスタンスのため、CIST パラメータのみ、内部修飾子やリージョナル修飾子ではなく外部修飾子が必要です。

- CIST ルートは、ネットワーク全体を網羅する一意のインスタンスのためのルート デバイスです。
- CIST 外部ルート パス コストは、CIST ルートまでのコストです。このコストは MST 領域内で変化しません。MST リージョンは、CIST への単一デバイスと見なすことに注意してください。CIST 外部ルート パス コストは、これらの仮想デバイス、およびどのリージョンにも属さないデバイスの間で算出されるルート パス コストです。
- CIST リージョナル ルートは、準規格の実装で IST マスターと呼ばれていました。CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。CIST ルートがリージョン内にない場合、CIST リージョナル ルートは、リージョン内の CIST ルートに最も近いデバイスです。CIST リージョナル ルートは、IST のルート デバイスとして動作します。
- CIST 内部ルート パス コストは、領域内の CIST リージョナル ルートまでのコストです。このコストは、IST つまりインスタンス 0 だけに関連します。

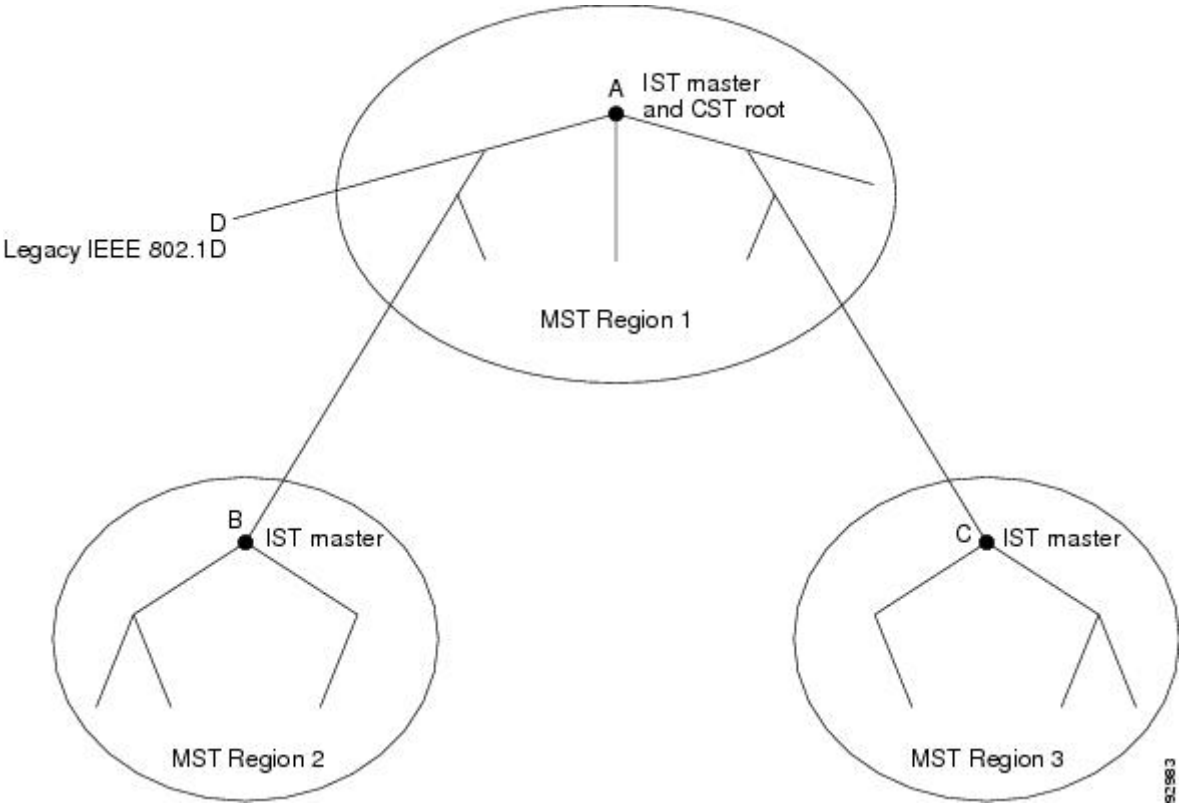
表 *5*: 準規格と規格の用語

IEEE 標準	シスコ先行標準	シスコ標準
CIST リージョナル ルート	IST マスター	CIST リージョナル ルート
CIST 内部ルート パス コスト	IST マスター パス コスト	CIST 内部パス コスト
CIST 外部ルート パス コスト	ルート パス コスト	ルート パス コスト
MSTI リージョナル ルート	インスタンス ルート	インスタンス ルート
MSTI 内部ルート パス コスト	ルート パス コスト	ルート パス コスト

MST リージョンの図

この図は、3 個の MST リージョンとレガシー IEEE 802.1D デバイス（D）を示しています。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。RSTPはすべてのリージョンで稼働しています。

図 *4 : MST* リージョン、*CIST* マスター、および *CST* ルート



関連トピック

MST リージョン （35 ページ）
MST リージョン内の動作 （36 ページ）
MST リージョン間の動作 （37 ページ）

ホップ カウント（Hop Count）

IST および MST インスタンスは、スパニングツリートポロジの計算に、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 タイムの情報を使用しません。その代わりに、IP Time To Live（TTL）メカニズムに似た、ルートまでのパス コストおよびホップ 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 カウントは、メッセージ エージ情報と同じ結果になります（再設定を開始）。インスタンスのルート デバイスは、コストが 0 でホップ カウントが最大値に設定されている BPDU（M レコード）を常に送信します。デバイスは、この BPDU を受信すると、受信した残りのホップ カウントから 1 を引き、生成する BPDU で残りのホップカウントとしてこの値を伝播します。カウントがゼロに達すると、デバイスは BPDU を廃棄し、ポート用に維持されている情報を期限切れにします。

BPDU の RSTP 部分に格納されているメッセージ有効期間と最大エージング タイムの情報は、リージョン全体で同じままであり、そのリージョンの境界に位置する指定ポートによって同じ値が伝播されます。

境界ポート

シスコ先行標準の実装では、境界ポートは、RSTP が稼働する単一のスパニングツリー リージョン、PVST+ または Rapid PVST+ が稼働する単一のスパニングツリー リージョン、または異なる MST コンフィギュレーションを持つ別の MST リージョンに MST リージョンを接続します。境界ポートは、LAN、単一のスパニングツリー デバイスまたは MST 設定が異なるデバイスの指定デバイスにも接続します。

IEEE 802.1s 標準では、境界ポートの定義はなくなりました。IEEE 802.1Q-2002 標準では、ポートが受信できる 2 種類のメッセージを識別します。

- 内部（同一リージョンから）
- 外部（別のリージョンから）

メッセージが内部の場合、CIST の部分は CIST によって受信されるので、各 MST インスタンスは個々の M レコードだけを受信します。

メッセージが外部である場合、CIST だけが受信します。CIST の役割がルートや代替ルートの場合、または外部 BPDU のトポロジが変更された場合は、MST インスタンスに影響する可能性があります。

MST リージョンには、デバイスおよび LAN の両方が含まれます。セグメントは、DP のリージョンに属します。そのため、セグメントの指定ポートではなく異なるリージョンにあるポートは境界ポートになります。この定義では、リージョン内部の 2 つのポートが、別のリージョンに属するポートとセグメントを共有し、内部メッセージおよび外部メッセージの両方を 1 つのポートで受信できるようになります。

シスコ先行標準の実装との主な違いは、STP 互換モードを使用している場合、指定ポートが境界ポートとして定義されない点です。

（注） レガシー STP デバイスがセグメントに存在する場合、メッセージは常に外部と見なされます。

シスコ先行標準の実装から他に変更された点は、送信デバイス ID を持つ RSTP またはレガシー IEEE 802.1Q デバイスの部分に、CIST リージョナル ルート デバイス ID フィールドが加えられたことです。リージョン全体は、一貫した送信者デバイス ID をネイバー デバイスに送信し、単一仮想デバイスのように動作します。この例では、A または B がセグメントに指定されているかどうかに関係なく、ルートの一貫した送信者デバイス ID が同じである BPDU をデバイス C が受信します。

IEEE 802.1s の実装

シスコの IEEE MST 標準の実装には、標準の要件を満たす機能だけでなく、すでに公開されている標準には含まれていない一部の（要望されている）先行標準の機能が含まれています。

ポートの役割名の変更

境界の役割は最終的に MST 標準に含まれませんでしたが、境界の概念自体はシスコの実装に投影されています。ただし、リージョン境界にある MST インスタンスのポートは、対応する CIST ポートのステートに必ずしも従うわけではありません。現在、2 つの境界の役割が存在しています。

- 境界ポートが CIST リージョナル ルートのルート ポートである場合：CIST インスタンスポートを提案されて同期中の場合、対応するすべての MSTI ポートの同期を取り終わった後であれば（その後フォワーディングします）、その場合のみ合意を返信してフォワーディング ステートに移行できます。MSTI ポートには、特別なマスターの役割があります。
- 境界ポートが CIST リージョナル ルートのルート ポートでない：MSTI ポートは、CIST ポートのステートおよび役割に従います。標準では提供される情報が少ないため、MSTI ポートが BPDU（M レコード）を受信しない場合、MSTI ポートが BPDU を代わりにブロックできる理由がわかりにくい場合があります。この場合、境界の役割自体は存在していませんが、**show** コマンドで見ると、出力される *type* カラムで、ポートが境界ポートとして認識されていることがわかります。

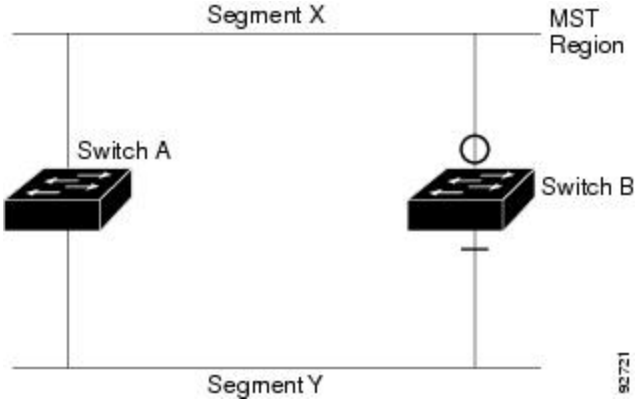
レガシーおよび規格デバイスの相互運用

準規格デバイスの自動検出はエラーになることがあるので、インターフェイス コンフィギュレーション コマンドを使用して準規格ポートを識別できます。デバイスの規格と準規格の間にリージョンを形成することはできませんが、CIST を使用して相互運用することができます。このような特別な方法を採用しても、失われる機能は、異なるインスタンス上のロードバランシングだけです。ポートが先行標準の BPDU を受信すると、CLI（コマンドライン インターフェイス）にはポートの設定に応じて異なるフラグが表示されます。デバイスが準規格BPDU送信用に設定されていないポートで準規格BPDUを初めて受信したときは、Syslogメッセージも表示されます。

図 *5*：規格および準規格のデバイスの相互運用

A が規格のデバイスで、B が準規格のデバイスとして、両方とも同じリージョンに設定されているとします。AはCISTのルートデバイスです。BのセグメントXにはルート ポート（BX）、セグメント Y には代替ポート（BY）があります。セグメント Y がフラップして BY のポートが代替になってから準規格 BPDU を 1 つ送信すると、AY は準規格デバイスが Y に接続されていることを検出できず、規格 BPDU の送信を続けます。ポート BY は境界に固定され、A と B との間でのロードランシングは不可能になります。セグメントXにも同じ問題がありますが、

B はトポロジの変更であれば送信する場合があります。



（注） 規格 MST 実装と準規格 MST 実装間の相互作用を最低限に抑えることを推奨します。

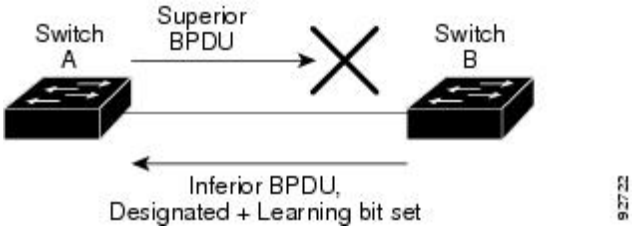
単一方向リンク障害の検出

IEEE MST 標準にはこの機能が存在していませんが、Cisco IOS Release には加えられています。ソフトウェアは、受信した BPDU でポートのロールおよびステートの一貫性をチェックし、ブリッジング ループの原因となることがある単方向リンク障害を検出します。

指定ポートは、矛盾を検出すると、その役割を維持しますが、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。

図 *6*: 単一方向リンク障害の検出

次の図に、ブリッジング ループの一般的な原因となる単方向リンク障害を示します。デバイス A はルート デバイスであり、デバイス B へのリンクで BPDU は失われます。RSTP および MST BPDU には、送信側ポートの役割とステートが含まれます。デバイス A はこの情報を使用し、ルータ A が送信する上位 BPDU にデバイス B が反応しないこと、およびデバイス B がルート デバイスではなく指定ブリッジであることを検出できます。この結果、デバイス 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。



MSTP およびデバイス スタック

デバイス スタックは、ネットワークのその他の部分に対しては単一のスパニングツリー ノードに見え、すべてのスタック メンバーが与えられたスパニングツリーに同一のブリッジ ID を使用します。ブリッジ ID は、アクティブ スイッチの MAC アドレスから取得されます。

スタックがネットワークのルートで、スタック内でルートの選択が行われていない場合は、アクティブ スイッチがスタック ルートになります。

デバイス スタックがスパニング ツリー ルートで、アクティブ スイッチで障害が発生した、またはスタックから外れた場合、スタンバイ スイッチが新しいアクティブ スイッチになり、ブリッジ ID は同じままで、スパニング ツリーの再コンバージェンスが発生する可能性があります。

MSTP をサポートしていないデバイスが、MSTP またはリバースをサポートしているデバイス スタックに追加されると、デバイスはバージョンが不一致の状態になります。可能な場合、デバイスは、デバイス スタックで実行中のソフトウェアと同じバージョンに自動的にアップグレードまたはダウングレードされます。

IEEE 802.1D STP との相互運用性

MSTP が稼働しているデバイスは、IEEE 802.1D 準拠のレガシー デバイスとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。このデバイスは、レガシー IEEE 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）を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。また、MSTP デバイスは、レガシー BPDU、別のリージョンに関連付けられている MSTP BPDU（バージョン 3）、または RSTP BPDU（バージョン 2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、デバイスが IEEE 802.1D BPDU を受信していない場合は、自動的に MSTP モードに戻りません。これはレガシー デバイスが指定デバイスでない限り、レガシー デバイスがリンクから削除されたかどうか検出できないためです。このデバイスが接続するデバイスがリージョンに加入していると、デバイスはポートに境界の役割を割り当て続ける場合があります。プロトコル移行プロセスを再開するには（強制的にネイバーデバイスと再びネゴシエーションするには）、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

リンク上のすべてのレガシーデバイスが RSTP デバイスであれば、これらのスイッチは、RSTP BPDU 同様に MSTP BPDU を処理できます。したがって、MSTP デバイスは、バージョン 0 コンフィギュレーションと TCN BPDU またはバージョン 3 MSTP BPDU のいずれかを境界ポートで送信します。境界ポートは、LAN、単一スパニングツリー デバイスまたは MST 設定が異なるデバイスのいずれかの指定のデバイスに接続します。

RSTP 概要

RSTP は、ポイントツーポイントの配線を利用して、スパニングツリーの高速コンバージェンスを実現します。また、1 秒未満の間に、スパニングツリーを再構成できます（IEEE 802.1D スパニングツリーのデフォルトに設定されている 50 秒とは異なります）。

ポートの役割およびアクティブ トポロジ

RSTP は、ポートに役割を割り当てて、アクティブ トポロジを学習することによって高速コンバージェンスを実現します。RSTP は デバイス をルート デバイスとして最も高いデバイス プライオリティ（プライオリティの数値が一番小さい）に選択するために、IEEE 802.1D STP 上

に構築されます。RSTP は、次のうちいずれかのポートの役割をそれぞれのポートに割り当てます。

- ルート ポート：デバイス がルートデバイス にパケットを転送するとき、最適なパス（最低コスト）を提供します。
- 指定ポート：指定デバイスに接続し、その LAN からルート デバイスにパケットを転送するとき、パスコストを最低にします。DPは、指定デバイスがLANに接続されているポートです。
- 代替ポート：現在のルート ポートが提供したパスに代わるルート デバイスへの代替パスを提供します。
- バックアップ ポート：指定ポートが提供した、スパニングツリーのリーフに向かうパスのバックアップとして機能します。バックアップ ポートは、2 つのポートがループバック内でポイントツーポイント リンクによって接続されるか、共有 LAN セグメントとの複数の接続がデバイスにある場合に限って存在できます。
- ディセーブル ポート：スパニングツリーの動作において何も役割が与えられていません。

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

ネットワーク全体のポートの役割に矛盾のない安定したトポロジでは、RSTPは、すべてのルートポートおよび指定ポートがただちにフォワーディング ステートに移行し、代替ポートとバックアップ ポートが必ず廃棄ステート（IEEE 802.1D のブロッキング ステートと同じ）になるように保証します。ポートのステートにより、転送処理および学習処理の動作が制御されます。

表 *6*: ポート ステートの比較

動作ステータス	STP ポート ステート（IEEE 802.1D）	RSTP 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
[有効（Enabled）]	ブロッキング	廃棄	なし
[有効（Enabled）]	リスニング	廃棄	なし
[有効（Enabled）]	ラーニング	ラーニング	○
[有効（Enabled）]	転送	転送	○
無効	無効	廃棄	なし

Cisco STP の実装との一貫性を保つため、このマニュアルでは、ポート ステートを廃棄ではなくブロッキングとして定義します。DP はリスニング ステートから開始します。

高速コンバージェンス

RSTPは、デバイス、デバイスポート、LANのうちいずれかの障害のあと、接続の高速回復を提供します。エッジ ポート、新しいルート ポート、ポイントツーポイント リンクで接続したポートに、高速コンバージェンスが次のように提供されます。

- エッジ ポート：**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して RSTP デバイスでエッジ ポートとしてポートを設定した場合、エッジ ポートはフォワーディング ステートにすぐに移行します。エッジ ポートは Port Fast 対応ポートと同じであり、単一エンドステーションに接続しているポートだけでイネーブルにする必要があります。
- ルート ポート：RSTP は、新しいルート ポートを選択した場合、古いルート ポートをブロックし、新しいルート ポートをフォワーディング ステートにすぐに移行します。
- 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。

図 7: 高速コンバージェンスの提案と合意のハンドシェイク

デバイス A がデバイス B にポイントツーポイント リンクで接続され、すべてのポートはブロッキング ステートになっています。デバイス A の優先度がデバイス B の優先度よりも数値的に小さいとします。デバイス A は提案メッセージ（提案フラグを設定した設定 BPDU）をデバイス B に送信し、指定デバイスとしてそれ自体を提案します。

デバイスBは、提案メッセージの受信後、提案メッセージを受信したポートを新しいルート ポートとして選択し、エッジ以外のすべてのポートを強制的にブロッキング ステートにして、新しいルートポートを介して合意メッセージ（合意フラグを設定したBPDU）を送信します。

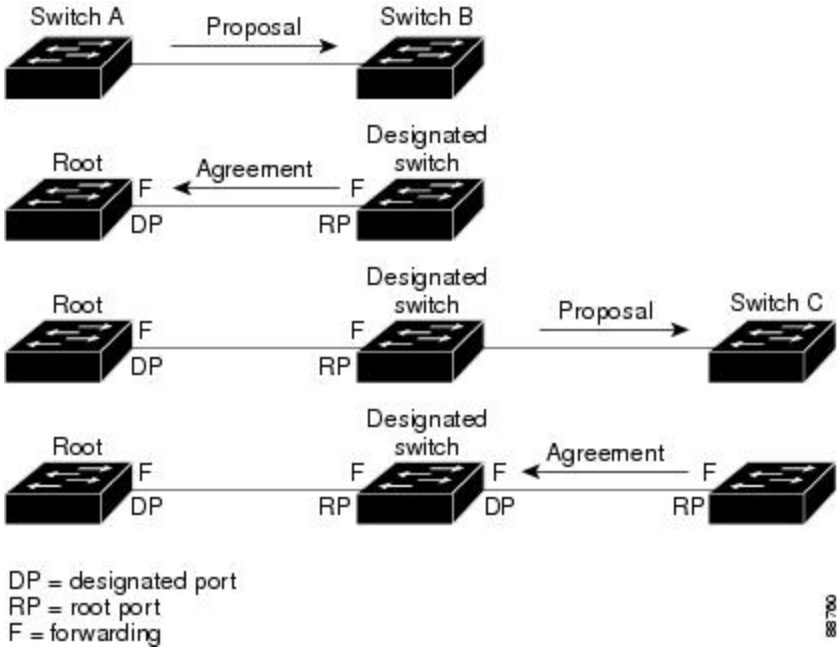
デバイス A も、デバイス B の合意メッセージの受信後、指定ポートをフォワーディングステートにすぐに移行します。デバイスBはすべてのエッジ以外のポートをブロックし、デバイス A およびルータ B の間にポイントツーポイント リンクがあるので、ネットワークにループは形成されません。

デバイス C がデバイス B に接続すると、同様のセットのハンドシェーク メッセージが交換されます。デバイス C はデバイス B に接続されているポートをルート ポートとして選択し、両端がフォワーディングステートにすぐに移行します。このハンドシェーク処理を繰り返して、もう1つのデバイスがアクティブ トポロジーに加わります。ネットワークが収束すると、この提案/合意ハンドシェイクがルートからスパニングツリーのリーフへと進みます。

デバイス スタックでは、Cross-Stack Rapid Transition（CSRT）機能を使用すると、ポートがフォワーディング ステートに移行する前に、スタック メンバで、提案/合意ハンドシェイク中にすべてのスタック メンバーから確認メッセージを受信できます。デバイスがMSTモードの場合、CSRT は自動的に有効にされます。

デバイスはポートのデュプレックス モードによってリンク タイプを学習します。全二重ポートはポイントツーポイント接続と見なされ、半二重接続は共有接続と見なされます。

spanning-tree link-type インターフェイス コンフィギュレーション コマンドを使用すると、デュプレックス設定によって制御されるデフォルト設定を無効にすることができます。



ポート ロールの同期

デバイスがそのルータのポートの1つ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、RSTP によってその他すべてのポートが新しいルートの情報と強制的に同期化します。

その他すべてのポートが同期化されている場合、デバイスはルート ポートで受信した上位ルート情報で同期化されます。デバイスのそれぞれのポートは、次のような場合に同期化します。

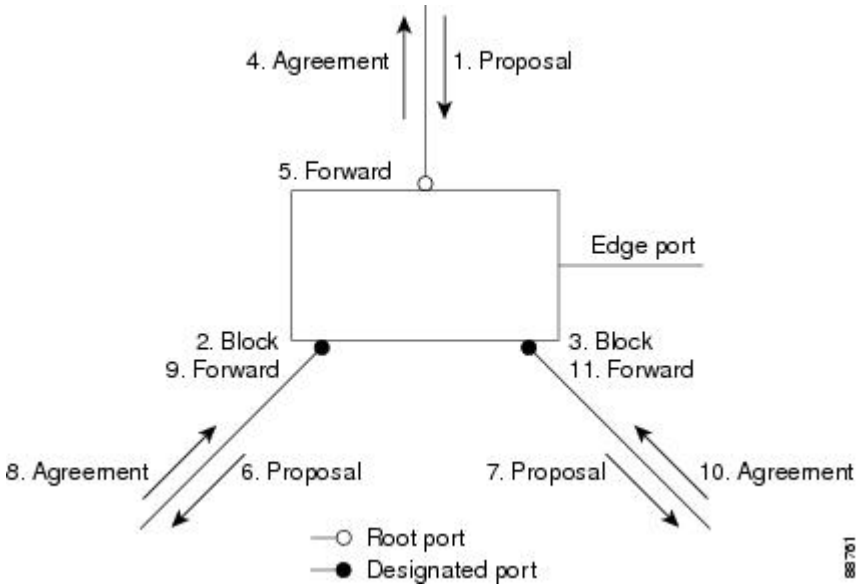
- ポートがブロッキング ステートである。
- エッジ ポートである（ネットワークのエッジに存在するように設定されたポート）。

指定ポートがフォワーディング ステートでエッジ ポートとして設定されていない場合、RSTP によって新しいルート情報と強制的に同期されると、その指定ポートはブロッキング ステートに移行します。一般的に RSTP がルート情報でポートを強制的に同期化し、ポートが上の条件を満たしていない場合、そのポート ステートはブロッキングに設定されます。

図 *8*: 高速コンバージェンス中のイベントのシーケンス

デバイスは、すべてのポートが同期化されたことを確認した後で、ルート ポートに対応する指定デバイスに合意メッセージを送信します。ポイントツーポイント リンクで接続されたデバイ

スがポートの役割で合意すると、RSTP はポート ステートをフォワーディングにすぐに移行します。



ブリッジ プロトコル データ ユニットの形式および処理

RSTP BPDU のフォーマットは、プロトコル バージョンが 2 に設定されている点を除き、IEEE 802.1D BPDU のフォーマットと同じです。新しい 1 バイトのバージョン 1 の Length フィールドは 0 に設定されます。これはバージョン 1 のプロトコルの情報がないことを示しています。

表 *7 : RSTP BPDU* フラグ

ビット	機能
[0]	トポロジーの変化（TC）
1	提案
2 ～ 3: 00 01 10 11	ポートの役割： 不明 Alternate port Root port Designated port
4	ラーニング
5	転送
[6]	契約
7	トポロジー変更確認応答（TCA）

送信側デバイスはRSTP BPDUの提案フラグを設定し、そのLANの指定デバイスとして自分自身を提案します。提案メッセージのポートの役割は、常に DP に設定されます。

送信側デバイスは、RSTP BPDUの合意フラグを設定して以前の提案を受け入れます。合意メッセージ内のポート ロールは、常にルート ポートに設定されます。

RSTPには個別のトポロジ変更通知（TCN）BPDUはありません。TCフラグが使用されて、TCが示されます。ただし、IEEE 802.1D デバイスとの相互運用性を保つために、RSTP デバイスは TCN BPDU の処理と生成を行います。

ラーニング フラグおよびフォワーディング フラグは、送信側ポートのステートに従って設定されます。

優位 BPDU 情報の処理

ポートに現在保存されているルート情報よりも優位のルート情報（小さいデバイス ID、低いパス コストなど）をポートが受け取ると、RSTP は再構成を開始します。ポートが新しいルート ポートとして提案されて選択されると、RSTP は強制的にその他すべてのポートを同期化します。

受信した BPDU が、提案フラグが設定されている RSTP BPDU である場合、デバイスはその他すべてのポートが同期化されてから合意メッセージを送信します。BPDU が IEEE 802.1D BPDU の場合、デバイスは提案フラグを設定せずに、そのポートの転送遅延タイマーを起動します。新しいルート ポートでは、フォワーディング ステートに移行するために、2 倍の転送遅延時間が必要となります。

ポートで優位の情報が受信されたために、その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、RSTP はそのポートをブロッキング ステートに設定し、合意メッセージは送信しません。DP は、転送遅延タイマーが失効するまで、提案フラグを設定して BPDU を送信し続け、転送遅延タイマーの失効時に、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

指定ポートの役割を持つ下位BPDU（そのポートに現在保存されている値より大きいデバイス ID 、高いパス コストなど）を指定ポートが受信した場合、その指定ポートはただちに現在の自身の情報で応答します。

トポロジの変更

ここでは、スパニングツリー トポロジの変更処理について、RSTP と IEEE 802.1D の相違を説明します。

- 検出：IEEE 802.1D では、どのようなブロッキング ステートとフォワーディング ステートとの間の移行でもトポロジの変更が発生しますが、RSTP でトポロジの変更が発生するのは、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場合だけです（トポロジの変更と見なされるのは、接続数が増加する場合だけです）。エッジポートにおけるステート変更は、TC の原因になりません。RSTP デバイスは、TC を検出すると、TCN を受信したポートを除く、エッジ以外のすべてのポートで学習した情報を削除します。

- 通知：IEEE 802.1D は TCN BPDU を使用しますが、RSTP は使用しません。ただし、IEEE 802.1D との相互運用性を保つために、RSTP デバイスは TCN BPDU の処理と生成を行います。
- 確認：RSTP デバイスは、指定ポートで IEEE 802.1D デバイスから TCN メッセージを受信した場合、TCA ビットが設定された IEEE 802.1D コンフィギュレーション BPDU で応答します。ただし、IEEE 802.1D デバイスに接続されたルート ポートで TC 時間タイマー（IEEE 802.1D のトポロジ変更タイマーと同じ）がアクティブであり、TCA ビットが設定されたコンフィギュレーション BPDU が受信された場合、TC 時間タイマーはリセットされます。

  この処理は、IEEE 802.1D デバイスをサポートする目的でのみ必要とされます。RSTP BPDU は TCA ビットが設定されていません。
- 伝播：RSTP デバイスは、DP またはルート ポートを介して別のデバイスから TC メッセージを受信すると、エッジ以外のすべての DP、およびルート ポート（TC メッセージを受信したポートを除く）に変更を伝播します。デバイスはこのようなすべてのポートで TC-while タイマーを開始し、そのポートで学習した情報を消去します。
- プロトコルの移行：IEEE 802.1D デバイスとの下位互換性を保つため、RSTP は IEEE 802.1D コンフィギュレーション BPDU および TCN BPDU をポート単位で必要に応じて送信します。

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

  デバイスはポートの移行遅延タイマーが満了した後に IEEE 802.1D BPDU を受信した場合、IEEE 802.1D デバイスに接続されていると想定し、IEEE 802.1D BPDU のみの使用を開始します。ただし、RSTP デバイスが 1 つのポートで IEEE 802.1D BPDU を使用していて、タイマーが満了した後に RSTP BPDU を受信した場合、タイマーが再起動し、そのポートで RSTP BPDU の使用が開始されます。

プロトコル移行プロセス

MSTP が稼働しているデバイスは、IEEE 802.1D 準拠のレガシー デバイスとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。このデバイスは、レガシー IEEE 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）を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。また、MST デバイスは、レガシー BPDU、別のリージョンに関連付けられている MSTP BPDU（バージョン 3）、または RST BPDU（バージョン 2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、デバイスが IEEE 802.1D BPDU を受信していない場合は、自動的に MSTP モードに戻りません。これはレガシー デバイスが指定デバイスでない限り、レガシー デバイスがリンクから削除されたかどうか検出できないためです。また、接続するデバイスがリージョンに加入していると、デバイスはポートに境界の役割を割り当て続ける場合があります。

関連トピック

プロトコルの移行プロセスの再開（CLI）（67 ページ）

MSTP のデフォルト設定

表 *8 : MSTP* のデフォルト設定

機能	デフォルト設定
スパニングツリー モード	
デバイス プライオリティ（CIST ポートごとに設定可能）	32768
スパニングツリー ポート プライオリティ（CIST ポート単位で設定可能）	128
スパニングツリー ポート コスト（CIST ポート単位で設定可能）	
hello タイム	
転送遅延時間	
最大エージング タイム	20 秒
最大ホップ カウント	20 ホップ

関連トピック

サポートされるスパニングツリー インスタンス（12 ページ）
MST リージョン設定の指定と MSTP のイネーブル化（CLI）（50 ページ）

MSTP 機能の設定方法

MST リージョン設定の指定と MSTP のイネーブル化（CLI）

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

リージョンには、MST 設定が同一である、1 つ以上のメンバーを含めることができます。各メンバーでは、RSTP BPDU を処理できる必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリーインスタンスの数は 65 までです。VLAN には、一度に 1 つのスパニングツリー インスタンス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	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree mst configuration** 例： `Device(config)# spanning-tree mst configuration`	MST コンフィギュレーション モードを開始します。
ステップ 4	**instance** *instance-id* **vlan** *vlan-range* 例： `Device(config-mst)# instance 1 vlan 10-20`	VLAN を MSTI にマップします。 • *instance-id* に指定できる範囲は、0 ～ 4094 です。 • vlan**vlan**に指定できる範囲は、1 ～ 4094 です。 VLAN を MSTI にマップする場合、マッピングは増加され、コマンドに指定した VLAN は、以前マッピングした VLAN に追加されるか、そこから削除されます。 VLAN の範囲を指定するには、ハイフンを使用します。たとえば **instance 1 vlan 1-63** では、VLAN 1 ～ 63 が MST インスタンス 1 にマップされます。 一連の VLAN を指定するには、カンマを使用します。たとえば **instance 1 vlan 10, 20, 30** と指定すると、VLAN 10、20、30 が MST インスタンス 1 にマップされます。
ステップ 5	**name** 名前 例：	コンフィギュレーション名を指定します。*name* 文字列の最大の長さは 32 文

	コマンドまたはアクション	目的
	`Device(config-mst)# name region1`	字であり、大文字と小文字が区別されます。
ステップ 6	**revision** バージョン 例： `Device(config-mst)# revision 1`	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。
ステップ 7	**show pending** 例： `Device(config-mst)# show pending`	保留中の設定を表示し、設定を確認します。
ステップ 8	**exit** 例： `Device(config-mst)# exit`	すべての変更を適用し、グローバルコンフィギュレーションモードに戻ります。
ステップ 9	**spanning-tree mode mst** 例： `Device(config)# spanning-tree mode mst`	MSTP をイネーブルにします。RSTP もイネーブルになります。 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は以前のモードであるため停止し、新しいモードで再起動するので、トラフィックを中断させる可能性があります。 MSTP と PVST+ または MSTP と Rapid PVST+ を同時に実行することはできません。
ステップ 10	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MSTP 設定時の注意事項 （33 ページ）
MST リージョン （35 ページ）
MSTP の前提条件 （31 ページ）
MSTP の制約事項 （32 ページ）
スパニングツリーの相互運用性と下位互換性 （12 ページ）
オプションのスパニングツリー設定時の注意事項

BackboneFast （78 ページ）
UplinkFast （73 ページ）
MSTP のデフォルト設定 （50 ページ）
ルート デバイスの設定（CLI） （53 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID
セカンダリ ルート デバイスの設定（CLI） （54 ページ）
ポート プライオリティの設定（CLI） （55 ページ）
パス コストの設定（CLI） （57 ページ）
デバイス プライオリティの設定（CLI） （59 ページ）
hello タイムの設定（CLI） （61 ページ）
転送遅延時間の設定（CLI） （62 ページ）
最大エージング タイムの設定（CLI） （63 ページ）
最大ホップ カウントの設定（CLI） （63 ページ）
高速移行を確実にするためのリンク タイプの指定（CLI） （64 ページ）
ネイバー タイプの設定（CLI） （66 ページ）
プロトコルの移行プロセスの再開（CLI） （67 ページ）

ルート デバイスの設定（CLI）

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID も把握する必要があります。この例のステップ 2 では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree mst** *instance-id* **root primary** 例： `Device(config)# spanning-tree mst 0 root primary`	ルート デバイスとしてデバイスを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

ルート スイッチ （34 ページ）
MST リージョン設定の指定と MSTP のイネーブル化（CLI） （50 ページ）
MSTP の制約事項 （32 ページ）
ブリッジ ID、デバイス プライオリティ、および拡張システム ID
セカンダリ ルート デバイスの設定（CLI） （54 ページ）

セカンダリ ルート デバイスの設定（CLI）

拡張システム ID をサポートするデバイスをセカンダリ ルートとして設定する場合、デバイス プライオリティはデフォルト値（32768）から 28672 に修正されます。プライマリ ルート デバイスで障害が発生した場合は、このデバイスが指定インスタンスのルート デバイスになる可能性があります。ここでは、その他のネットワーク デバイスが、デフォルトのデバイス プライオリティの 32768 を使用しているためにルート デバイスになる可能性が低いことが前提となっています。

このコマンドを複数のデバイスに対して実行すると、複数のバックアップ ルート デバイスを設定できます。**spanning-tree mst** *instance-id* **root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート デバイスを設定したときと同じネットワーク直径および hello タイム値を使用してください。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID も把握する必要があります。この例では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree mst** *instance-id***root secondary** 例： `Device(config)# spanning-tree mst 0 root secondary`	セカンダリ ルート デバイスとしてデバイスを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）　（50 ページ）
ルート デバイスの設定（CLI）　（53 ページ）

ポート プライオリティの設定（CLI）

ループが発生した場合、MSTP はポート プライオリティを使用して、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。最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）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に同じプライ

オリティ値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

（注） デバイスがデバイス スタックのメンバーの場合、**spanning-tree mst** [*instance-id*] **port-priority** *priority* インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree mst** [*instance-id*] **cost** *cost* インターフェイス コンフィギュレーション コマンドを使用し、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必要があります。最初に選択させたいポートには、より小さいコスト値を割り当て、最後に選択させたいポートには、より大きいコスト値を割り当てることができます。詳細については、関連項目の下に表示されるパス コストのトピックを参照してください。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。この例では、インスタンス ID として 0 を使用し、インターフェイスとして GigabitEthernet1/0/1 を使用します。これは「関連トピック」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**spanning-tree mst** *instance-id***port-priority** *priority*	ポート プライオリティを設定します。

	コマンドまたはアクション	目的
	例： `Device(config-if)# spanning-tree mst 0 port-priority 64`	• *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。指定できる範囲は 0 ～ 4094 です。 • *priority* 値の範囲は 0 ～ 240 で、16 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くなります。 使用可能な値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 だけです。その他の値はすべて拒否されます。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

show spanning-tree mstinterface *interface-id* 特権 EXEC コマンドは、ポートがリンク アップ動作可能状態であるかどうかの情報のみ表示します。そうでない場合は、**show running-config interface** 特権 EXEC コマンドを使用して設定を確認してください。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）（50 ページ）
パス コストの設定（CLI）（57 ページ）

パス コストの設定（CLI）

MSTP 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に基づきます。ループが発生した場合、MSTP 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。最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択される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。すべてのインターフェイスに同じコスト値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定されたMSTインスタンスIDと使用されるインターフェイスも把握する必要があります。この例では、インスタンスIDとして0を使用し、インターフェイスとしてGigabitEthernet1/0/1を使用します。これは「関連トピック」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	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。有効なインターフェイスには、物理ポートとポートチャネル論理インターフェイスがあります。指定できるポートチャネルの範囲は1～48 です。
ステップ 4	**spanning-tree mst** *instance-id***cost** *cost* 例： `Device(config-if)# spanning-tree mst 0 cost 17031970`	コストを設定します。 ループが発生した場合、MSTP はパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 • *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。指定できる範囲は 0 ～ 4094 です。

	コマンドまたはアクション	目的
		• *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

show spanning-tree mst interface *interface-id* 特権 EXEC コマンドによって表示されるのは、リンク アップ動作可能状態のポートの情報だけです。そうでない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

関連トピック

ポート プライオリティの設定（CLI）　（55 ページ）
MST リージョン設定の指定と MSTP のイネーブル化（CLI）　（50 ページ）

デバイス プライオリティの設定（CLI）

デバイスのプライオリティを変更すると、スタンドアロンデバイスまたはスタック内のデバイスであるかに関係なく、ルートデバイスとして選択される可能性が高くなります。

（注）　このコマンドの使用には注意してください。通常のネットワーク設定では、**spanning-tree mst** *instance-id* **root primary** および **spanning-tree mst** *instance-id* **root secondary** グローバル コンフィグレーション コマンドを使用し、デバイスをルートまたはセカンダリ ルート デバイスに指定することを推奨します。これらのコマンドが動作しない場合にのみデバイスプライオリティを変更する必要があります。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

使用する指定された MST インスタンス ID も把握する必要があります。この例では、インスタンス ID として 0 を使用します。これは「関連項目」で示されている手順によって設定されたインスタンス ID が 0 であるためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree mst** *instance-id***priority** *priority* 例： `Device(config)# spanning-tree mst 0 priority 40960`	デバイス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。指定できる範囲は 0 ～ 4094 です。 • *priority* の範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。この値が低いほど、デバイスがルート デバイスとして選択される可能性が高くなります。 使用可能な値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。これらは唯一の許容値です。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）　（50 ページ）

hello タイムの設定（CLI）

hello タイムはルート デバイスによって設定メッセージが生成されて送信される時間の間隔です。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree mst hello-time** 秒 例： `Device(config)# spanning-tree mst hello-time 4`	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 タイムはルートデバイスによって設定メッセージが生成されて送信される時間の間隔です。このメッセージは、デバイスが活動中であることを表します。 *seconds* に指定できる範囲は 1 ～ 10 です。デフォルトは 3 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）　（50 ページ）

転送遅延時間の設定（CLI）

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree mst forward-time** 秒 例： `Device(config)# spanning-tree mst forward-time 25`	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。転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、ポートが待機する秒数です。 *seconds* に指定できる範囲は 4 ～ 30 です。デフォルトは 20 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）　（50 ページ）

最大エージング タイムの設定（CLI）

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree mst max-age** 秒 例： `Device(config)# spanning-tree mst max-age 40`	すべての MST インスタンスについて、最大経過時間を設定します。最大エージング タイムは、デバイスが再設定を試す前にスパニングツリー設定メッセージを受信せずに待機する秒数です。 *seconds* に指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）　（50 ページ）

最大ホップ カウントの設定（CLI）

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree mst max-hops** *hop-count* 例： `Device(config)# spanning-tree mst max-hops 25`	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* に指定できる範囲は 1 ～ 255 です。デフォルト値は 20 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）　（50 ページ）

高速移行を確実にするためのリンク タイプの指定（CLI）

ポイントツーポイント リンクでポート間を接続し、ローカル ポートが DP になると、RSTP は提案と合意のハンドシェークを使用して別のポートと高速移行をネゴシエーションし、ループがないトポロジを保証します。

デフォルトの場合、リンク タイプ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、半二重ポートは共有接続と見なされます。MSTP を実行しているリモート デバイスの単一ポートに、半二重リンクを物理的にポイントツーポイントで接続した場合は、リンク タイプのデフォルト設定を無効にして、フォワーディング ステートへの高速移行をイネーブルにすることができます。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

指定されたMSTインスタンスIDと使用されるインターフェイスも把握する必要があります。この例では、インスタンスIDとして0を使用し、インターフェイスとしてGigabitEthernet1/0/1を使用します。これは「関連トピック」で示されている手順によってインスタンス ID とインターフェイスがそのように設定されているためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet1/0/1`	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。有効なインターフェイスには、物理ポート、VLAN、およびポート チャネル論理インターフェイスがあります。VLAN ID の範囲は 1 ～ 4094 です。指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 4	**spanning-tree link-type point-to-point** 例： `Device(config-if)# spanning-tree link-type point-to-point`	ポートのリンク タイプがポイントツーポイントであることを指定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI） （50 ページ）

ネイバー タイプの設定（CLI）

トポロジには、先行標準に準拠したデバイスと IEEE 802.1s 標準準拠のデバイスの両方を加えることができます。デフォルトの場合、ポートは準規格デバイスを自動的に検出できますが、規格 BPDU および準規格 BPDU の両方を受信できます。デバイスとそのネイバーの間に不一致がある場合は、CIST だけがインターフェイスで動作します。

準規格 BPDU だけを送信するようにポートを設定できます。ポートが STP 互換モードになっていても、すべての **show** コマンドで準規格フラグが表示されます。

この手順は任意です。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet1/0/1`	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。有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	**spanning-tree mst pre-standard** 例： `Device(config-if)# spanning-tree mst pre-standard`	ポートが準規格 BPDU だけを送信できることを指定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）　（50 ページ）

プロトコルの移行プロセスの再開（CLI）

この手順では、プロトコル移行プロセスを再開し、ネイバーデバイスとの再ネゴシエーションを強制します。また、デバイスを MST モードに戻します。これは、IEEE 802.1D BPDU の受信後にデバイスがそれらを受信しない場合に必要です。

デバイスでプロトコルの移行プロセスを再開する（隣接するデバイスで再ネゴシエーションを強制的に行う）手順については、これらの手順に従ってください。

始める前に

マルチ スパニングツリー（MST）が、デバイスで指定されて有効になっている必要があります。詳細については、関連項目を参照してください。

コマンドのインターフェイス バージョンを使用する場合は、使用する MST インターフェイスが分かっている必要があります。この例では、インターフェイスとして GigabitEthernet1/0/1 を使用します。それが「関連項目」で示されている手順によって設定されたインターフェイスであるからです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	次のいずれかのコマンドを入力します。 • **clear spanning-tree detected-protocols** • **clear spanning-tree detected-protocolsinterface** *interface-id* 例： `Device# clear spanning-tree detected-protocols`	デバイスが MSTP モードに戻り、プロトコルの移行プロセスが再開されます。

	コマンドまたはアクション	目的
	または `Device# clear spanning-tree detected-protocols interface GigabitEthernet1/0/1`	

次のタスク

この手順は、デバイスでさらにレガシー IEEE 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 に設定された BPDU）を受信する場合に、繰り返しが必要なことがあります。

関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI） （50 ページ）
プロトコル移行プロセス （49 ページ）

MSTP に関する追加情報

関連資料

関連項目	参照先
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9500 Series Switches)* の「Layer 2/3 Commands」の項を参照してください

標準および RFC

標準/RFC	役職（Title）
なし	—

MIB

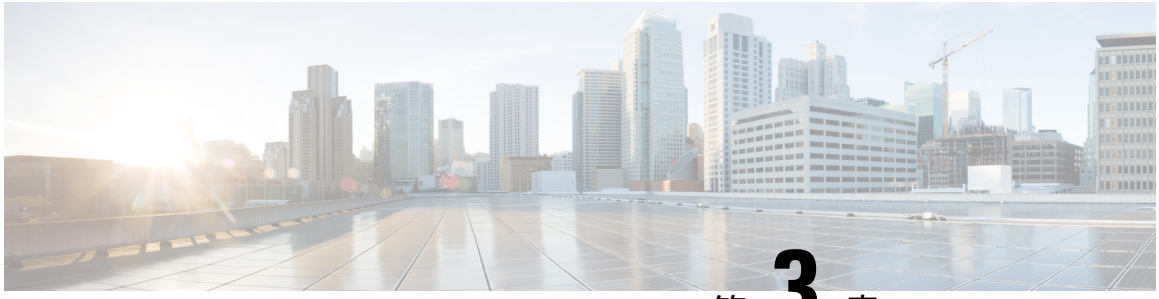
MIB	MIB リンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

MSTP の機能情報

リリース	変更箇所
Cisco IOS XE Everest 16.5.1a	この機能が導入されました。



第 3 章

オプションのスパニングツリー機能の設定

- オプションのスパニングツリー機能について （71 ページ）
- オプションのスパニングツリー機能の設定方法 （82 ページ）
- スパニングツリー ステータスのモニタリング （94 ページ）
- オプションのスパニング ツリー機能に関する追加情報 （95 ページ）
- オプションのスパニングツリー機能の機能情報 （96 ページ）

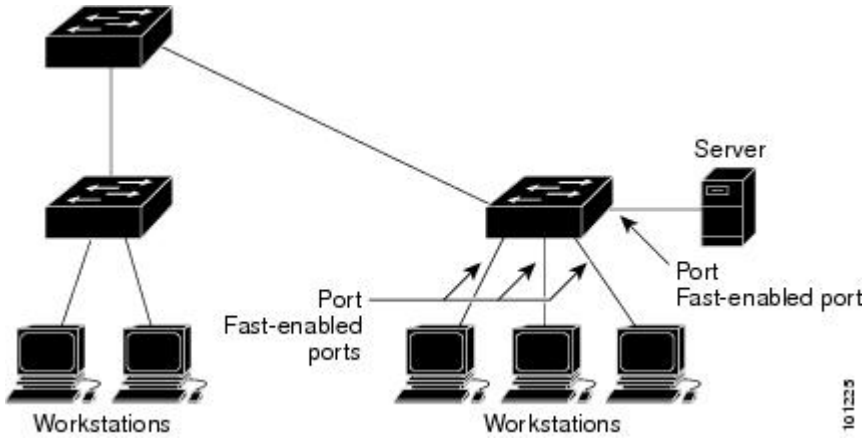
オプションのスパニングツリー機能について

PortFast

PortFast 機能を使用すると、アクセス ポートまたはトランク ポートとして設定されているインターフェイスが、リスニング ステートおよびラーニング ステートを経由せずに、ブロッキング ステートから直接フォワーディング ステートに移行します。

図 *9 : PortFast* が有効なインターフェイス

単一のワークステーションまたはサーバに接続されたインターフェイス上で PortFast を使用すると、スパニング ツリーが収束するのを待たずにデバイスをただちにネットワークに接続できます。



1 台のワークステーションまたはサーバに接続されたインターフェイスがブリッジプロトコルデータ ユニット（BPDU）を受信しないようにする必要があります。スイッチを再起動すると、PortFast が有効に設定されているインターフェイスは通常のスパニングツリー ステータスの遷移をたどります。

インターフェイスまたはすべての非トランク ポートで有効にして、この機能を有効にできます。

関連トピック

PortFast のイネーブル化（CLI）（82 ページ）
オプションのスパニング ツリー機能の制約事項

BPDU ガード

ブリッジプロトコルデータ ユニット（BPDU）ガード機能はスイッチ上でグローバルにイネーブルにすることも、ポート単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

PortFast エッジ対応ポート上でグローバル レベルで BPDU ガードをイネーブルにすると、スパニング ツリーは、BPDU が受信されると、PortFast エッジ動作ステートのポートをシャット ダウンします。有効な設定では、PortFast エッジ対応ポートは BPDU を受信しません。PortFast エッジ対応ポートが BPDU を受信した場合は、許可されていないデバイスの接続などの無効な設定が存在することを示しており、BPDU ガード機能によってポートは error-disabled ステートになります。この状態になると、スイッチは違反が発生したポート全体をシャットダウンします。

PortFast エッジ機能をイネーブルにせずにインターフェイス レベルでポート上の BPDU ガードをイネーブルにした場合、ポートが BPDU を受信すると、error-disabled ステートになります。

インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービスプロバイダー ネットワーク内でアクセス ポートがスパニングツリーに参加しないようにするには、BPDU ガード機能を使用します。

関連トピック

BPDU ガードのイネーブル化（CLI）（84 ページ）

BPDU フィルタリング

BPDU フィルタリング機能はスイッチ上でグローバルにイネーブルにすることも、インターフェイス単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

グローバル レベルでは、PortFast エッジ対応インターフェイスで BPDU フィルタリングをイネーブルにすると、PortFast エッジ動作ステートにあるインターフェイスでの BPDU の送受信が防止されます。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。これらのインターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。PortFast エッジ対応インター

フェイスでは、BPDU を受信すると、PortFast エッジ動作ステートが解除され、BPDU フィルタリングがディセーブルになります。

PortFastエッジ機能をイネーブルにせずに、インターフェイスでBPDUフィルタリングをイネーブルにすると、インターフェイスでの BPDU の送受信が防止されます。

注意 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ことは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリーループが発生することがあります。

スイッチ全体または1つのインターフェイスでBPDUフィルタリング機能をイネーブルにできます。

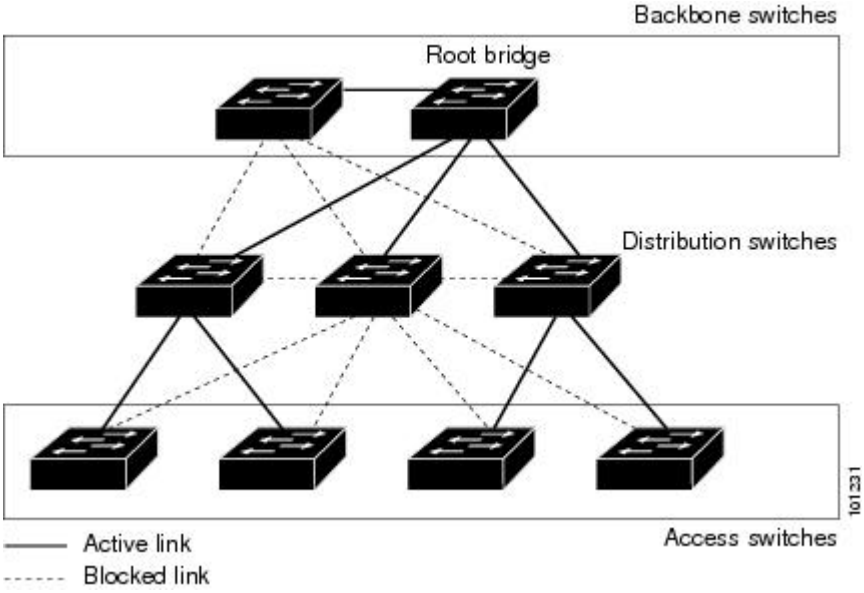
関連トピック

BPDU フィルタリングのイネーブル化（CLI） （86 ページ）

UplinkFast

図 *10*：階層型ネットワークのスイッチ

階層型ネットワークに配置されたスイッチは、バックボーン スイッチ、ディストリビューション スイッチ、およびアクセス スイッチに分類できます。この複雑なネットワークには、ディストリビューション スイッチとアクセス スイッチがあり、ループを防止するために、スパニング ツリーがブロックする冗長リンクが少なくとも 1 つあります。



スイッチの接続が切断されると、スイッチはスパニングツリーが新しいルート ポートを選択すると同時に代替パスの使用を開始します。リンクやスイッチに障害が発生した場合、またはスパニングツリーが UplinkFast の有効化によって自動的に再設定された場合に、新しいルートポートを短時間で選択できます。ルート ポートは、通常のスパニングツリー手順とは異なり、

リスニング ステートおよびラーニング ステートを経由せず、ただちにフォワーディング ステートに移行します。

スパニングツリーが新規ルート ポートを再設定すると、他のインターフェイスはネットワークにマルチキャスト パケットをフラッディングし、インターフェイス上で学習した各アドレスにパケットを送信します。max-update-rate パラメータの値を小さくすることで、これらのマルチキャスト トラフィックのバーストを制限できます（このパラメータはデフォルトで毎秒 150 パケットです）。ただし、0 を入力すると、ステーション学習フレームが生成されないので、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。

（注） UplinkFast は、ネットワークのアクセスまたはエッジに位置する、ワイヤリング クローゼットのスイッチで非常に有効です。バックボーン デバイスには適していません。他のアプリケーションにこの機能を使用しても、有効とは限りません。

UplinkFast は、直接リンク障害発生後に高速コンバージェンスを行い、アップリンク グループを使用して、冗長レイヤ 2 リンク間でロード バランシングを実行します。アップリンク グループは、（VLAN ごとの）レイヤ 2 インターフェイスの集合であり、いかなるときも、その中の 1 つのインターフェイスだけが転送を行います。つまり、アップリンク グループは、（転送を行う）ルート ポートと、（セルフループを行うポートを除く）ブロックされたポートの集合で構成されます。アップリンク グループは、転送中のリンクで障害が起きた場合に代替パスを提供します。

図 *11 :* 直接リンク障害が発生する前の *UplinkFast* の例

このトポロジにはリンク障害がありません。ルート スイッチであるスイッチ A は、リンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

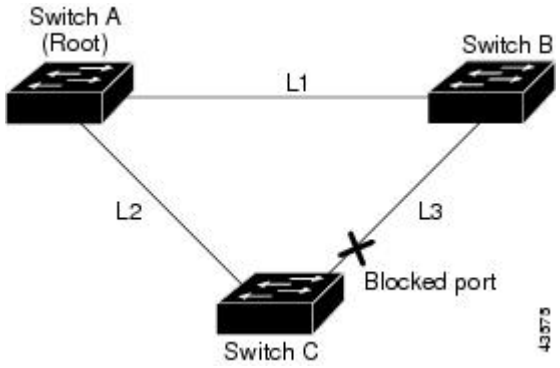
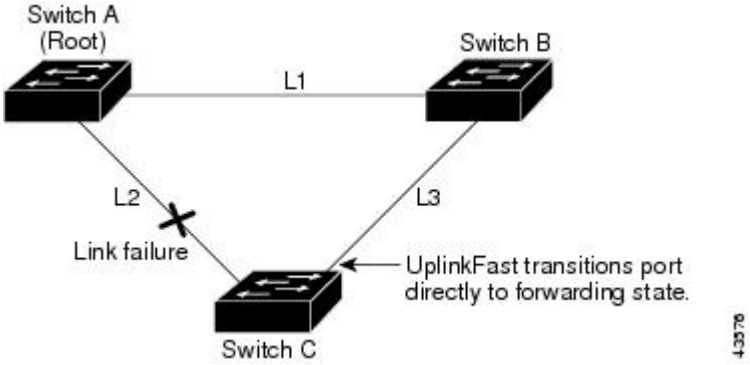


図 *12 :* 直接リンク障害が発生したあとの *UplinkFast* の例

スイッチ C が、ルート ポートの現在のアクティブ リンクである L2 でリンク障害（直接リンク障害）を検出すると、UplinkFast がスイッチ C でブロックされていたインターフェイスのブロックを解除し、リスニング ステートおよびラーニング ステートを経由せずに、直接フォワー

ディング ステートに移行させます。この切り替えに必要な時間は、約 1 ～ 5 秒です。



関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI）（50 ページ）
MSTP 設定時の注意事項（33 ページ）
MST リージョン（35 ページ）
冗長リンクで使用するための UplinkFast のイネーブル化（CLI）（87 ページ）
高速コンバージェンスを発生させるイベント（77 ページ）

Cross-Stack UplinkFast

クロススタック UplinkFast（CSUF）は、スイッチ スタック全体にスパニングツリー高速移行（通常のネットワーク状態の下では1秒未満の高速コンバージェンス）を提供します。高速移行の間は、スタック上の代替冗長リンクがフォワーディング ステートになり、一時的なスパニングツリーループもバックボーンへの接続の損失も発生させません。一部の設定では、この機能により、冗長性と復元力を備えたネットワークが得られます。CSUF は UplinkFast 機能をイネーブルにすると、自動的にイネーブルになります。

CSUF で高速移行が得られない場合もあります。この場合は、通常のスパニングツリー移行が発生し、30 ～ 40 秒以内に完了します。詳細については、「関連項目」を参照してください。

関連トピック

冗長リンクで使用するための UplinkFast のイネーブル化（CLI）（87 ページ）
高速コンバージェンスを発生させるイベント（77 ページ）

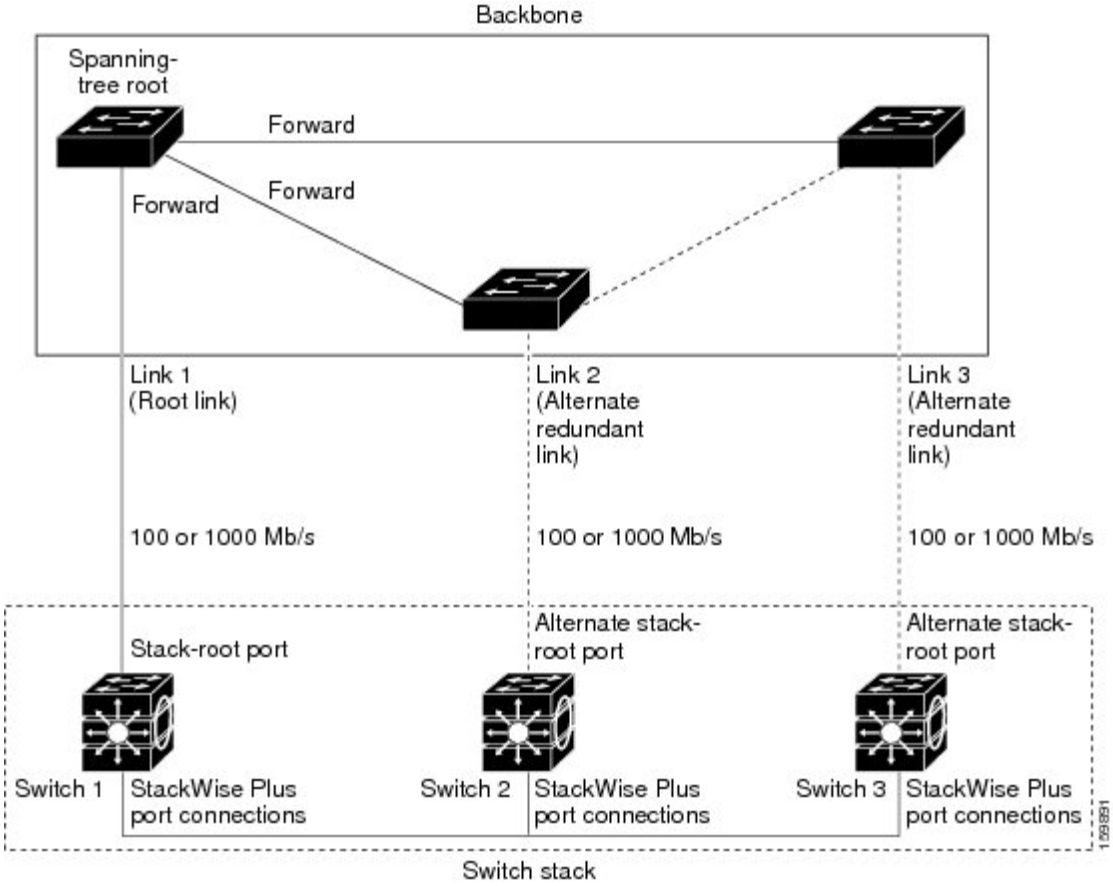
クロススタック UplinkFast の動作

クロススタック UplinkFast（CSUF）によって、ルートへのパスとしてスタック内で1つのリンクが確実に選択されます。

図 *13 :* クロススタック *UplinkFast* トポロジ

スイッチ1のスタックルート ポートは、スパニングツリーのルートへパスを提供しています。スイッチ 2 およびスイッチ 3 の代替スタックルート ポートは、現在のスタックルート スイッチに障害が発生したか、またはそのスパニングツリールートへのリンクに障害が発生した場合に、スパニングツリー ルートへの代替パスを提供できます。

ルート リンクである Link 1 は、スパニングツリー フォワーディング ステートになっています。Link 2 と Link 3 は、スパニングツリー ブロッキング ステートになっている代替冗長リンクです。スイッチ 1 に障害が発生したか、そのスタック ルート ポートに障害が発生したか、または Link 1 に障害が発生した場合には、CSUF が、1 秒未満でスイッチ 2 またはスイッチ 3 のいずれかにある代替スタックルート ポートを選択して、それをフォワーディング ステートにします。



特定のリンク損失またはスパニングツリーイベントが発生した場合（次のトピックを参照）、Fast Uplink Transition Protocol は、ネイバー リストを使用して、高速移行要求をスタック メンバーに送信します。

高速移行要求を送信するスイッチは、ルートポートとして選択されたポートをフォワーディングステートへ高速移行する必要があります。また、高速移行を実行するには、事前に各スタックから確認応答を取得しておく必要があります。

スタック内の各スイッチが、ルート、コスト、およびブリッジ ID を比較することにより、このスパニングツリー インスタンスのスタック ルートとなるよりも送信スイッチの方がよりよい選択肢であるかどうかを判断します。スタックルートとして送信スイッチが最も良い選択である場合は、スタック内の各スイッチが確認応答を返します。それ以外の場合は、高速移行要求を送信します。この時点では、送信スイッチは、すべてのスタック スイッチから確認応答を受け取っていません。

すべてのスタック スイッチから確認応答を受け取ると、送信スイッチの Fast Uplink Transition Protocol は代替スタックルート ポートをすぐにフォワーディング ステートに移行させます。送信スイッチがすべてのスタック スイッチからの確認応答を取得しなかった場合、通常のスパニングツリー移行（ブロッキング、リスニング、ラーニング、およびフォワーディング）が行われ、スパニングツリー トポロジが通常のレート（2 × 転送遅延時間 + 最大エージング タイム）で収束します。

Fast Uplink Transition Protocol は、VLAN ごとに実装されており、一度に 1 つのスパニングツリー インスタンスにしか影響しません。

関連トピック

冗長リンクで使用するための UplinkFast のイネーブル化（CLI）（87 ページ）
高速コンバージェンスを発生させるイベント（77 ページ）

高速コンバージェンスを発生させるイベント

CSUF 高速コンバージェンスは、ネットワーク イベントまたはネットワーク障害に応じて、発生する場合もあれば発生しない場合もあります。

高速コンバージェンス（通常のネットワーク状態で 1 秒未満）は、次のような状況で発生します。

- スタック ルート ポート リンクに障害が発生した。

  スタック内の 2 つのスイッチがルートへの代替パスを持つ場合、それらのスイッチの片方だけが高速移行を行います。

- スタック ルートをスパニングツリー ルートに接続するリンクに障害が発生し、回復した。
- ネットワークの再設定により、新しいスタックルート スイッチが選択された。
- ネットワークの再設定により、現在のスタックルート スイッチ上で新しいポートがスタック ルート ポートとして選択された。

（注） 複数のイベントが同時に発生すると、高速移行が行われなくなる場合もあります。たとえば、スタック メンバの電源がオフになり、それと同時にスタック ルートをスパニングツリー ルートに接続しているリンクが回復した場合、通常のスパニングツリー コンバージェンスが発生します。

通常のスパニングツリー コンバージェンス（30 ～ 40 秒）は、次のような状況で発生します。

- スタック ルート スイッチの電源がオフになったか、またはソフトウェアに障害が発生した。
- 電源がオフになっていたか、または障害が発生していたスタック ルート スイッチの電源が入った。
- スタック ルートになる可能性のある新しいスイッチがスタックに追加された。

関連トピック

冗長リンクで使用するための UplinkFast のイネーブル化（CLI）（87 ページ）
UplinkFast（73 ページ）
Cross-Stack UplinkFast（75 ページ）
クロススタック UplinkFast の動作（75 ページ）

BackboneFast

BackboneFast は、バックボーンのコアにおける間接障害を検出します。BackboneFast は、UplinkFast 機能を補完するテクノロジーです。UplinkFast は、アクセス スイッチに直接接続されたリンクの障害に対応します。BackboneFastは、最大エージング タイマーを最適化します。最大エージング タイマーによって、スイッチがインターフェイスで受信したプロトコル情報を保存しておく時間の長さが制御されます。スイッチが別のスイッチの指定ポートから下位BPDUを受信した場合、BPDUは他のスイッチでルートまでのパスが失われた可能性を示すシグナルとなり、BackboneFast はルートまでの別のパスを見つけようとします。

スイッチのルート ポートまたはブロックされたインターフェイスが、指定スイッチから下位 BPDU を受け取ると、BackboneFast が開始します。下位 BPDU は、ルート ブリッジと指定スイッチの両方を宣言しているスイッチを識別します。スイッチが下位BPDUを受信した場合、そのスイッチが直接接続されていないリンク（間接リンク）で障害が発生したことを意味します（指定スイッチとルート スイッチ間の接続が切断されています）。スパニングツリーのルールに従い、スイッチは最大エージング タイム（デフォルトは 20 秒）の間、下位 BPDU を無視します。

スイッチは、ルート スイッチへの代替パスの有無を判別します。下位 BPDU がブロック インターフェイスに到達した場合、スイッチ上のルート ポートおよび他のブロック インターフェイスがルート スイッチへの代替パスになります（セルフループ ポートはルート スイッチの代替パスとは見なされません）。下位 BPDU がルート ポートに到達した場合には、すべてのブロック インターフェイスがルート スイッチへの代替パスになります。下位 BPDU がルート ポートに到達し、しかもブロック インターフェイスがない場合、スイッチはルート スイッチへの接続が切断されたものと見なし、ルート ポートの最大エージング タイムが経過するまで待ち、通常のスパニングツリー ルールに従ってルート スイッチになります。

スイッチが代替パスでルート スイッチに到達できる場合、スイッチはその代替パスを使用して、Root Link Query（RLQ）要求を送信します。スイッチは、スタック メンバーがルート スイッチへの代替ルートを持つかどうかを学習するために、すべての代替パスに RLQ 要求を送信し、ネットワーク内およびスタック内の他のスイッチからのRLQ応答を待機します。スイッチは、すべての代替パスに RLQ 要求を送信し、ネットワーク内の他のスイッチからの RLQ 応答を待機します。

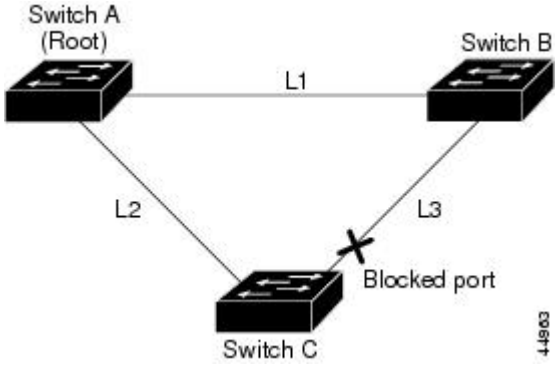
スタック メンバが、ブロック インターフェイス上の非スタック メンバから RLQ 応答を受信し、その応答が他の非スタック スイッチ宛てのものであった場合、そのスタック メンバは、スパニングツリー インターフェイス ステートに関係なく、その応答パケットを転送します。

スタック メンバが非スタック メンバから RLQ 応答を受信し、その応答がスタック宛てのものであった場合、そのスタック メンバは、他のすべてのスタック メンバがその応答を受信するようにその応答を転送します。

ルートへの代替パスがまだ存在していると判断したスイッチは、下位 BPDU を受信したインターフェイスの最大エージング タイムが経過するまで待ちます。ルート スイッチへのすべての代替パスが、スイッチとルート スイッチ間の接続が切断されていることを示している場合、スイッチは RLQ 応答を受信したインターフェイスの最大エージング タイムを満了させます。1 つまたは複数の代替パスからルート スイッチへ引き続き接続できる場合、スイッチは下位 BPDU を受信したすべてのインターフェイスを指定ポートにして、（ブロッキング ステートになっていた場合）ブロッキング ステートを解除し、リスニング ステート、ラーニング ステートを経てフォワーディング ステートに移行させます。

図 *14*：間接リンク障害が発生する前の *BackboneFast* の例

これは、リンク障害が発生していないトポロジ例です。ルート スイッチであるスイッチ A はリンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング



ステートです。

図 *15*：間接リンク障害が発生したあとの *BackboneFast* の例

リンク L1 で障害が発生した場合、スイッチ C はリンク L1 に直接接続されていないので、この障害を検出できません。一方スイッチ B は、L1 によってルート スイッチに直接接続されているため障害を検出し、スイッチ B 自身をルートとして選定して、自らをルートとして特定した状態で BPDU をスイッチ C へ送信し始めます。スイッチ B から下位 BPDU を受信したスイッチ C は、間接障害が発生していると見なします。この時点で、BackboneFast は、スイッチ C のブロック インターフェイスを、インターフェイスの最大エージング タイムが満了するまで待たずに、ただちにリスニング ステートに移行させます。BackboneFast は、次に、スイッチ C のレイヤ2インターフェイスをフォワーディング ステートに移行させ、スイッチ B からスイッチ A へのパスを提供します。ルートスイッチの選択には約 30 秒必要です。これは転送遅延時間がデフォルトの 15 秒に設定されていればその倍の時間です。BackboneFast がリンク L1 で発

生した障害に応じてトポロジを再設定します。

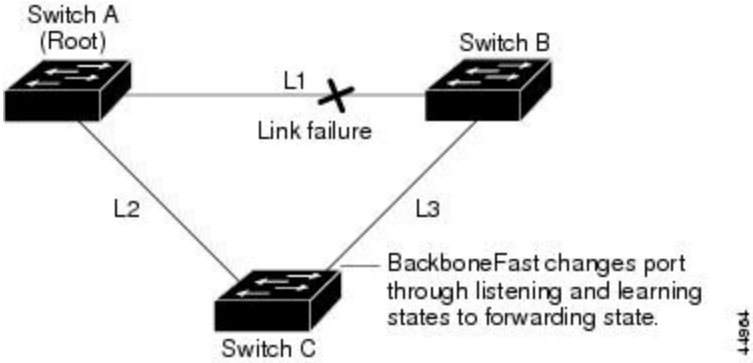
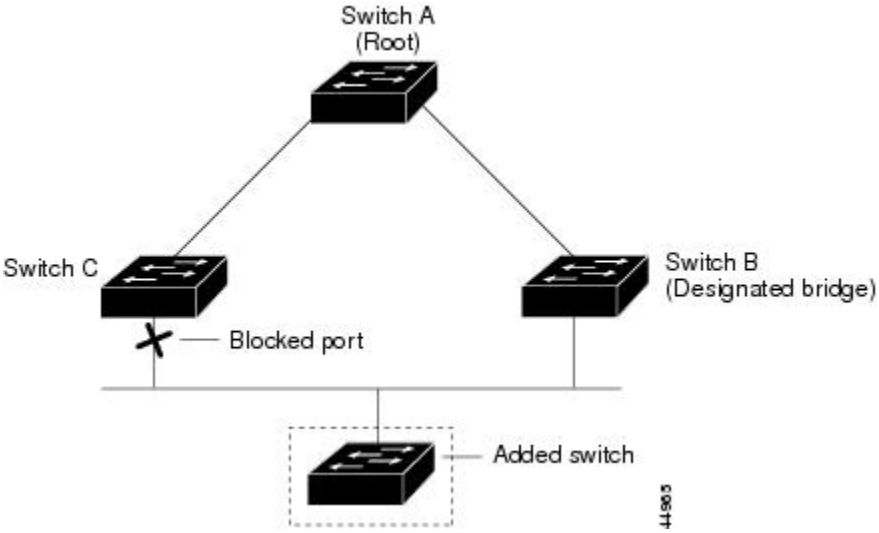


図 *16 :* メディア共有型トポロジにおけるスイッチの追加

新しいスイッチがメディア共有型トポロジに組み込まれた場合、認識された指定スイッチ（スイッチ B）から下位 BPDU が届いていないので、BackboneFast はアクティブになりません。新しいスイッチは、自身がルート スイッチであることを伝える下位 BPDU の送信を開始します。ただし、他のスイッチはこれらの下位 BPDU を無視し、新しいスイッチはスイッチ B がルート スイッチであるスイッチ A への指定スイッチであることを学習します。



関連トピック

MST リージョン設定の指定と MSTP のイネーブル化（CLI） （50 ページ）
MSTP 設定時の注意事項 （33 ページ）
MST リージョン （35 ページ）
BackboneFast をイネーブル化（CLI） （90 ページ）

EtherChannel ガード

EtherChannel ガードを使用すると、スイッチと接続したデバイス間での EtherChannel の設定の矛盾を検出できます。スイッチ インターフェイスは EtherChannel として設定されているものの、もう一方のデバイスのインターフェイスではその設定が行われていない場合、設定の矛盾

が発生します。また、EtherChannel の両端でチャネルのパラメータが異なる場合にも、設定の矛盾が発生します。

スイッチが、他のデバイス上で設定の矛盾を検出した場合、EtherChannel ガードは、スイッチのインターフェイスを errdisable ステートにし、エラー メッセージを表示します。

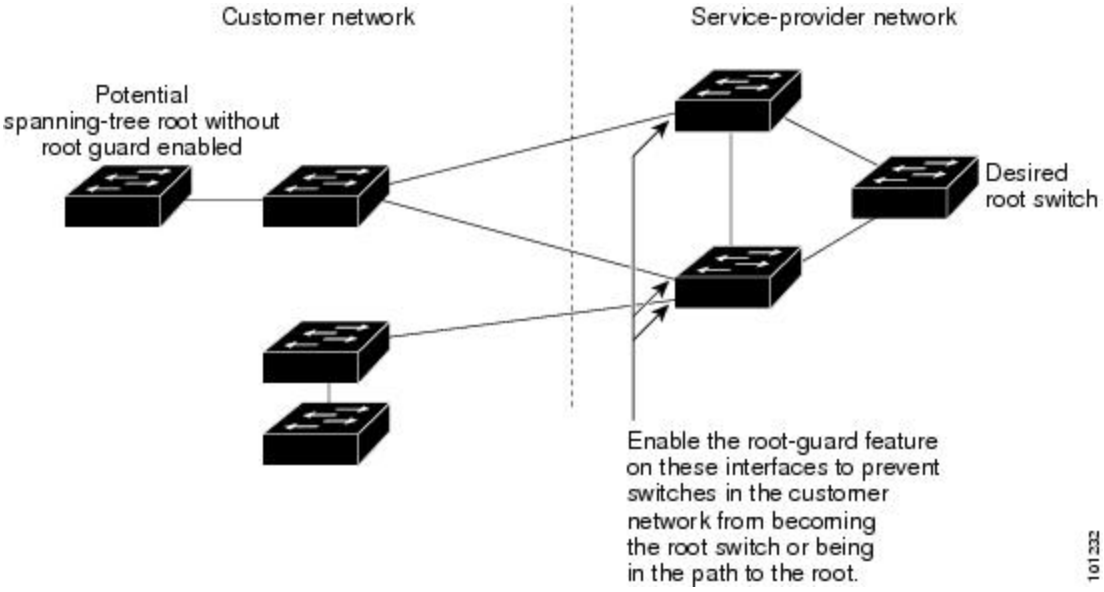
関連トピック

EtherChannel ガードのイネーブル化（CLI） （91 ページ）

ルート ガード

図 *17*：サービス プロバイダー ネットワークのルート ガード

サービス プロバイダー（SP）のレイヤ 2 ネットワークには、SP 以外が所有するスイッチへの接続が多く含まれている場合があります。このようなトポロジでは、スパニングツリーが再構成され、カスタマー スイッチをルート スイッチとして選択する可能性があります。この状況を防ぐには、カスタマー ネットワーク内のスイッチに接続する SP スイッチ インターフェイス上でルート ガード機能を有効に設定します。スパニングツリーの計算によってカスタマーネットワーク内のインターフェイスがルート ポートとして選択されると、ルート ガードがそのインターフェイスを root-inconsistent（ブロッキング）ステートにして、カスタマーのスイッチがルート スイッチにならないようにするか、ルートへのパスに組み込まれないようにします。



SP ネットワーク外のスイッチがルート スイッチになると、インターフェイスがブロックされ（root-inconsistent ステートになり）、スパニングツリーが新しいルート スイッチを選択します。カスタマーのスイッチがルートスイッチになることはありません。ルートへのパスに組み込まれることもありません。

スイッチが MST モードで動作している場合、ルート ガードが強制的にそのインターフェイスを指定ポートにします。また、境界ポートがルート ガードによって Internal Spanning-Tree（IST）インスタンスでブロックされている場合にも、このインターフェイスはすべての MST インス

タンスでもブロックされます。境界ポートは、指定スイッチが IEEE 802.1D スイッチまたは異なる MST リージョン設定を持つスイッチのいずれかである LAN に接続されるインターフェイスです。

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。VLAN は、MST インスタンスに対してグループ化された後、マッピングされます。

⚠

注意 ルート ガード機能を誤って使用すると、接続が切断されることがあります。

関連トピック

ルート ガードのイネーブル化（CLI） （92 ページ）

ループ ガード

ループ ガードを使用すると、代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。この機能は、スイッチドネットワーク全体でイネーブルにした場合に最も効果があります。ループ ガードによって、代替ポートおよびルート ポートが指定ポートになることが防止され、スパニングツリーがルート ポートまたは代替ポートで BPDU を送信することはありません。

スイッチが PVST+ または Rapid PVST+ モードで動作している場合、ループ ガードによって、代替ポートおよびルート ポートが指定ポートになることが防止され、スパニングツリーがルート ポートまたは代替ポートで BPDU を送信することはありません。

スイッチが MST モードで動作しているとき、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされている場合でのみ、非境界ポートで BPDU を送信しません。境界ポートでは、ループ ガードがすべての MST インスタンスでインターフェイスをブロックします。

関連トピック

ループ ガードのイネーブル化（CLI） （93 ページ）

オプションのスパニングツリー機能の設定方法

PortFast のイネーブル化（CLI）

PortFast 機能がイネーブルに設定されているインターフェイスは、標準の転送遅延時間の経過を待たずに、すぐにスパニングツリー フォワーディング ステートに移行されます。

音声 VLAN 機能をイネーブルにすると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

⚠

注意 PortFast を使用するのは、1 つのエンド ステーションがアクセス ポートまたはトランク ポートに接続されている場合に限定されます。スイッチまたはハブに接続するインターフェイス上でこの機能をイネーブルにすると、スパニングツリーがネットワーク ループを検出または阻止できなくなり、その結果、ブロードキャスト ストームおよびアドレス ラーニングの障害が起きる可能性があります。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**spanning-tree portfast** [**trunk**] 例： `Device(config-if)# spanning-tree portfast trunk`	単一ワーク ステーションまたはサーバに接続されたアクセス ポート上で PortFast をイネーブルにします。 **trunk** キーワードを指定すると、トランク ポート上で PortFast をイネーブルにできます。

	コマンドまたはアクション	目的
		（注） トランク ポートで PortFast をイネーブルにするには、**spanning-tree portfast trunk** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**spanning-tree portfast** コマンドは、トランク ポート上では機能しないためです。 トランク ポート上で PortFast をイネーブルにする場合は、事前に、トランク ポートとワークステーションまたはサーバの間にループがないことを確認してください。 デフォルトでは、PortFast はすべてのインターフェイスでディセーブルです。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

次のタスク

spanning-tree portfast default グローバル コンフィギュレーション コマンドを使用すると、すべての非トランク ポート上で PortFast 機能をグローバルにイネーブルにできます。

関連トピック

PortFast （71 ページ）
オプションのスパニング ツリー機能の制約事項

BPDU ガードのイネーブル化（CLI）

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU ガード機能をイネーブルにできます。

⚠

注意 PortFast エッジは、エンド ステーションに接続するインターフェイスのみに設定します。それ以外に設定すると、予期しないトポロジ ループが原因でデータのパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree portfast edge bpduguard default** 例： `Device(config)# spanning-tree portfast edge bpduguard default`	BPDU ガードをグローバルにイネーブルにします。 BPDU ガードは、デフォルトではディセーブルに設定されています。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	エンドステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**spanning-tree portfast edge** 例： `Device(config-if)# spanning-tree portfast edge`	PortFast エッジ機能をイネーブルにします。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

次のタスク

ポートのシャットダウンを防ぐには、**errdisable detect cause bpduguard shutdown vlan** グローバル コンフィギュレーション コマンドを使用すると、違反の発生時にポートで問題になっている VLAN のみをシャットダウンできます。

PortFast エッジ機能をイネーブルにしなくても、**spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のポートで BPDU ガードをイネーブルにすることもできます。BPDU を受信したポートは、errdisable ステートになります。

関連トピック

BPDU ガード （72 ページ）

BPDU フィルタリングのイネーブル化（CLI）

PortFast エッジ機能をイネーブルにしなくても、**spanning-tree bpdufilter enable** インターフェイス コンフィギュレーション コマンドを使用して、任意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することもできます。このコマンドを実行すると、インターフェイスは BPDU を送受信できなくなります。

注意 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ことは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリーループが発生することがあります。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU フィルタリング機能をイネーブルにできます。

注意 PortFast エッジは、エンド ステーションに接続するインターフェイスのみに設定します。それ以外に設定すると、予期しないトポロジ ループが原因でデータのパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree portfast edge bpdufilter default** 例： `Device(config)# spanning-tree portfast edge bpdufilter default`	BPDU フィルタリングをグローバルにイネーブルにします。 BPDU フィルタリングは、デフォルトではディセーブルに設定されています。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	エンドステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**spanning-tree portfast edge** 例： `Device(config-if)# spanning-tree portfast edge`	指定したインターフェイスで PortFast エッジ機能をイネーブルにします。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

BPDU フィルタリング （72 ページ）

冗長リンクで使用するための UplinkFast のイネーブル化（CLI）

（注） UplinkFast をイネーブルにすると、スイッチまたはスイッチ スタックのすべての VLAN に影響します。個々の VLAN について UplinkFast を設定することはできません。

Rapid PVST+ または MSTP に対して UplinkFast または Cross-Stack UplinkFast（CSUF）機能を設定できますが、この機能は、スパニングツリーのモードを PVST+ に変更するまではディセーブル（非アクティブ）になったままです。

この手順は任意です。UplinkFast および CSUF をイネーブルにするには、次の手順に従います。

始める前に

スイッチ プライオリティが設定されている VLAN 上で UplinkFast をイネーブルにすることはできません。スイッチ プライオリティが設定されている VLAN 上で UplinkFast をイネーブルにする場合は、最初に **no spanning-tree vlan** *vlan-id***priority** 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って、VLAN のスイッチ プライオリティをデフォルト値に戻す必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree uplinkfast** [**max-update-rate** *pkts-per-second*] 例： `Device(config)# spanning-tree uplinkfast max-update-rate 200`	UplinkFast をイネーブルにします。 （任意）*pkts-per-second* に指定できる範囲は毎秒 0 ～ 32000 パケットです。デフォルト値は 150 です。 0 を入力すると、ステーション学習フレームが生成されないので、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。 このコマンドを入力すると、すべての非スタック ポート インターフェイス上で CSUF もイネーブルになります。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチ プライオリティは 49152 に設定されます。UplinkFast をイネーブルにする場合、または UplinkFast がすでにイネーブルに設定されている場合に、パス コストを 3000 未満の値に変更すると、すべてのインターフェイスおよび VLAN トランクのパス コストが 3000 だけ増加します（パス コストを 3000 以上の値に変更した場合、パス コストは変更されません）。スイッチ プライオリティおよびパス コストを変更すると、スイッチがルート スイッチになる可能性が低くなります。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

次の手順に従って UplinkFast 機能をイネーブルにすると、CSUF は非スタック ポート インターフェイスで自動的にグローバルにイネーブルになります。

関連トピック

UplinkFast （73 ページ）
Cross-Stack UplinkFast （75 ページ）
クロススタック UplinkFast の動作 （75 ページ）
高速コンバージェンスを発生させるイベント （77 ページ）

UplinkFast のディセーブル化（CLI）

この手順は任意です。

UplinkFast および Cross-Stack UplinkFast（SUF）をディセーブルにするには、次の手順に従います。

始める前に

UplinkFast を有効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	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**no spanning-tree uplinkfast** 例： `Device(config)# no spanning-tree uplinkfast`	スイッチおよびそのスイッチのすべての VLAN で UplinkFast および CSUF をディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

次の手順に従って UplinkFast 機能をディセーブルにすると、CSUF は非スタック ポート インターフェイスで自動的にグローバルにディセーブルになります。

BackboneFast をイネーブル化（CLI）

BackboneFast をイネーブルにすると、間接リンク障害を検出し、スパニングツリーの再構成をより早く開始できます。

Rapid PVST+ または MSTP に対して BackboneFast 機能を設定できます。ただし、スパニングツリーモードを PVST+ に変更するまで、この機能はディセーブル（非アクティブ）のままです。

この手順は任意です。スイッチ上で BackboneFast をイネーブルにするには、次の手順に従います。

始める前に

BackboneFast を使用する場合は、ネットワーク上のすべてのスイッチでイネーブルする必要があります。BackboneFast は、トークンリング VLAN ではサポートされません。この機能は他社製スイッチでの使用にサポートされています。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree backbonefast** 例： `Device(config)# spanning-tree backbonefast`	BackboneFast をイネーブルにします。
ステップ 4	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	

関連トピック

BackboneFast （78 ページ）

EtherChannel ガードのイネーブル化（CLI）

デバイスで PVST+、Rapid PVST+、または MSTP が稼働している場合、EtherChannel の設定の矛盾を検出する EtherChannel ガード機能をイネーブルにできます。

この手順は任意です。

デバイスで EtherChannel ガードをイネーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**spanning-tree etherchannel guard misconfig** 例： `Device(config)# spanning-tree etherchannel guard misconfig`	EtherChannel ガードをイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

次のタスク

show interfaces status err-disabled 特権 EXEC コマンドを使用することで、EtherChannel の設定矛盾が原因でディセーブルになっているデバイス ポートを表示できます。リモート デバイス上では、**show etherchannel summary** 特権 EXEC コマンドを使用して、EtherChannel の設定を確認できます。

設定を修正した後、誤って設定していたポート チャネル インターフェイス上で、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してください。

関連トピック

EtherChannel ガード （80 ページ）

ルート ガードのイネーブル化（CLI）

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。UplinkFast 機能が使用するインターフェイスで、ルート ガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に（ブロック ステートの）バックアップ インターフェイスがルート ポートになります。ただし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップ インターフェイスが root-inconsistent（ブロック）ステートになり、フォワーディング ステートに移行できなくなります。

（注） ルート ガードとループ ガードの両方を同時にイネーブルにすることはできません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

この手順は任意です。

スイッチ上でルート ガードをイネーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**spanning-tree guard root** 例： `Device(config-if)# spanning-tree guard root`	インターフェイス上でルート ガードをイネーブルにします。 デフォルトでは、ルート ガードはすべてのインターフェイスでディセーブルです。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

ルート ガード （81 ページ）

ループ ガードのイネーブル化（CLI）

ループ ガードを使用すると、代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。この機能は、スイッチドネットワーク全体に設定した場合に最も効果があります。ループ ガードは、スパニングツリーがポイントツーポイントと見なすインターフェイス上でのみ動作します。

（注） ループ ガードとルート ガードの両方を同時にイネーブルにすることはできません。

デバイスで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。

この手順は任意です。デバイスでループ ガードをイネーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	次のいずれかのコマンドを入力します。 • **show spanning-tree active** • **show spanning-tree mst**	どのインターフェイスが代替ポートまたはルート ポートであるかを確認します。

	コマンドまたはアクション	目的

	例：
	`Device# show spanning-tree active`
	または
	`Device# show spanning-tree mst`	

ステップ 2	**configure terminal** 例： `Device# 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 3	**spanning-tree loopguard default** 例： `Device(config)# spanning-tree loopguard default`	ループ ガードをイネーブルにします。 ループ ガードは、デフォルトではディセーブルに設定されています。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

ループ ガード （82 ページ）

スパニングツリー ステータスのモニタリング

表 *9*: スパニングツリー ステータスをモニタリングするコマンド

コマンド（Command）	目的
show spanning-tree active	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree mst interface *interface-id*	指定インターフェイスのMST情報を表示します。

コマンド（Command）	目的
show spanning-tree summary [totals]	インターフェイス ステートのサマリーを表示します。またはスパニングツリー ステート セクションのすべての行を表示します。
show spanning-tree mst interface *interface-id***portfast edge**	指定したインターフェイスのスパニングツリー portfast 情報を表示します。

オプションのスパニング ツリー機能に関する追加情報

関連資料

関連項目	参照先
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9500 Series Switches)*

標準および RFC

標準/RFC	役職（Title）
なし	—

MIB

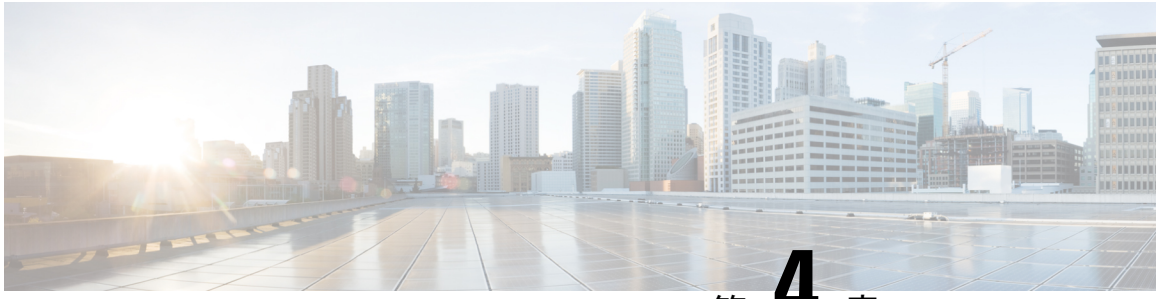
MIB	MIB リンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

オプションのスパニングツリー機能の機能情報

リリース	変更箇所
Cisco IOS XE Everest 16.5.1a	この機能が導入されました。



第 4 章

EtherChannel の設定

- 機能情報の確認 （97 ページ）
- EtherChannel の制約事項 （97 ページ）
- EtherChannel について （98 ページ）
- EtherChannel の設定方法 （113 ページ）
- EtherChannel、PAgP、および LACP ステータスのモニタ （133 ページ）
- EtherChannel の設定例 （134 ページ）
- EtherChannels の追加リファレンス （137 ページ）
- EtherChannels の機能情報 （138 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびCisco ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

EtherChannel の制約事項

次に、EtherChannels の制約事項を示します。

- EtherChannel のすべてのポートは同じ VLAN に割り当てるか、またはトランク ポートとして設定する必要があります。

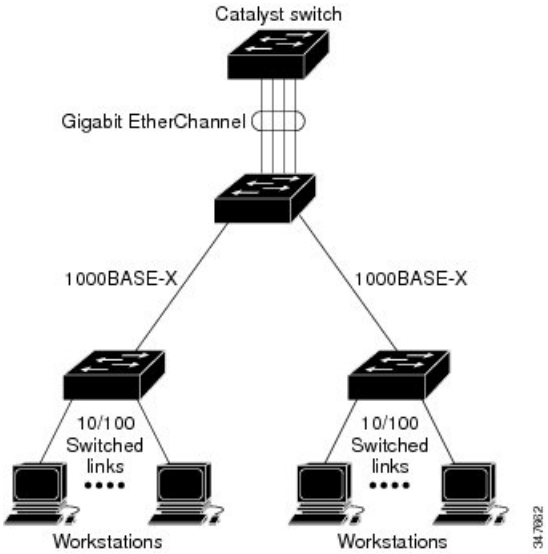
EtherChannel について

EtherChannel の概要

EtherChannel は、スイッチ、ルータ、およびサーバ間にフォールトトレラントな高速リンクを提供します。EtherChannel を使用して、ワイヤリング クローゼットとデータセンター間の帯域幅を増やすことができます。さらに、ボトルネックが発生しやすいネットワーク上のあらゆる場所に EtherChannel を配置できます。EtherChannel は、他のリンクに負荷を再分散させることによって、リンク切断から自動的に回復します。リンク障害が発生した場合、EtherChannel は自動的に障害リンクからチャネル内の他のリンクにトラフィックをリダイレクトします。

EtherChannel は、単一の論理リンクにバンドルする個別のイーサネット リンクで構成されます。

図 *18 :* 一般的な *EtherChannel* 構成



EtherChannel は、スイッチ間またはスイッチとホスト間に、最大 8 Gb/s（ギガビット EtherChannel）または 80 Gb/s（10 ギガビット EtherChannel）の全二重帯域幅を提供します。

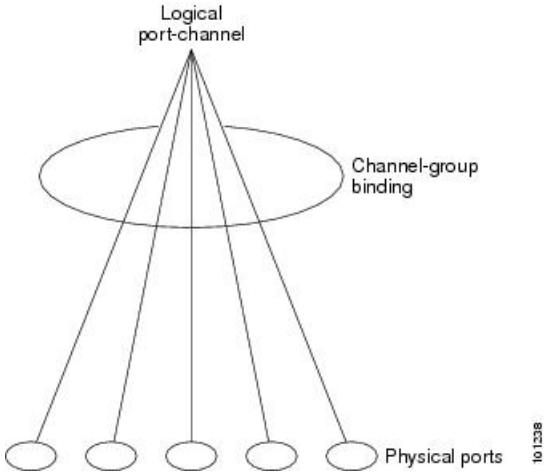
各 EtherChannel は、互換性のある設定のイーサネット ポートを 8 つまで使用して構成できます。

チャネル グループおよびポートチャネル インターフェイス

EtherChannel は、チャネル グループとポートチャネル インターフェイスから構成されます。チャネル グループはポートチャネル インターフェイスに物理ポートをバインドします。ポートチャネル インターフェイスに適用した設定変更は、チャネル グループにまとめてバインドされるすべての物理ポートに適用されます。

図 *19* : 物理ポート、チャネル グループおよびポートチャネル インターフェイスの関係

channel-group コマンドは、物理ポートおよびポートチャネル インターフェイスをまとめてバインドします。各 EtherChannel には 1 ～ 128 までの番号が付いたポートチャネル論理インターフェイスがあります。このポートチャネル インターフェイス番号は、**channel-group** インターフェイス コンフィギュレーション コマンドで指定した番号に対応しています。



- レイヤ 2 ポートの場合は、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ポートチャネル インターフェイスを動的に作成します。

  また、**interface port-channel** *port-channel-number* グローバル コンフィギュレーション コマンドを使用して、ポートチャネル論理インターフェイスを手動で作成することもできます。ただし、その場合、論理インターフェイスを物理ポートにバインドするには、**channel-group** *channel-group-number* コマンドを使用する必要があります。*channel-group-number* は *port-channel-number* と同じ値に設定することも、違う値を使用することもできます。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポート チャネルを作成します。

- レイヤ 3 ポートの場合は、**interface port-channel** グローバル コンフィギュレーション コマンド、およびそのあとに **no switchport** インターフェイス コンフィギュレーション コマンドを使用して、論理インターフェイスを手動で作成する必要があります。その後、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、手動で EtherChannel にインターフェイスを割り当てます。

- レイヤ 3 ポートでレイヤ 3 インターフェイスとしてインターフェイスを設定するには、**no switchport** インターフェイス コマンドを使用した上で **channel-group** インターフェイス コンフィギュレーション コマンドを使用して動的にポートチャネル インターフェイスを作成します。

関連トピック

ポートチャネル論理インターフェイスの作成 （CLI）
EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （109 ページ）

レイヤ 2 EtherChannel 設定時の注意事項 （111 ページ）
物理インターフェイスの設定（CLI）

Port Aggregation Protocol; ポート集約プロトコル

ポート集約プロトコル（PAgP）はシスコ独自のプロトコルで、Cisco デバイスおよび PAgP をサポートするベンダーによってライセンス供与されたデバイスでのみ稼働します。PAgP を使用すると、イーサネット ポート間で PAgP パケットを交換することにより、EtherChannel を自動的に作成できます。PAgP はクロススタック EtherChannel でイネーブルにできます。

デバイスまたはデバイス スタックは PAgP を使用することによって、PAgP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似している（スタック内の単一デバイス上の）ポートを、単一の論理リンク（チャネルまたは集約ポート）に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。たとえば、PAgP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同じポートをグループとしてまとめます。リンクを EtherChannel にグループ化した後で、PAgP は単一デバイス ポートとして、スパニングツリーにそのグループを追加します。

PAgP モード

PAgP モードは、PAgP ネゴシエーションを開始する PAgP パケットをポートが送信できるか、または受信した PAgP パケットに応答できるかを指定します。

表 *10 : EtherChannel PAgP* モード

[モード（Mode）]	説明
auto	ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。これにより、PAgP パケットの送信は最小限に抑えられます。
desirable	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。

スイッチ ポートは、**auto** モードまたは **desirable** モードに設定された相手ポートとだけ PAgP パケットを交換します。**on** モードに設定されたポートは、PAgP パケットを交換しません。

auto モードおよび **desirable** モードはともに、相手ポートとネゴシエーションして、ポート速度などの条件に基づいて（レイヤ 2 EtherChannel の場合は、トランク ステートおよび VLAN 番号などの基準に基づいて）、ポートで EtherChannel を形成できるようにします。

PAgP モードが異なっていても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。次に例を示します。

- **desirable** モードのポートは、**desirable** モードまたは **auto** モードの別のポートとともに EtherChannel を形成できます。
- **auto** モードのポートは、**desirable** モードの別のポートとともに EtherChannel を形成できます。

どのポートも PAgP ネゴシエーションを開始しないため、**auto** モードのポートは、**auto** モードの別のポートとは EtherChannel を形成できません。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI） （113 ページ）
EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （109 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （111 ページ）
ポートチャネル論理インターフェイスの作成 （CLI）
物理インターフェイスの設定（CLI）

サイレント モード

PAgP 対応のデバイスにスイッチを接続する場合、**non-silent** キーワードを使用すると、非サイレント動作としてスイッチ ポートを設定できます。**auto** モードまたは **desirable** モードとともに **non-silent** を指定しなかった場合は、サイレント モードが指定されていると見なされます。

サイレント モードを使用するのは、PAgP 非対応で、かつほとんどパケットを送信しないデバイスにスイッチを接続する場合です。サイレント パートナーの例は、トラフィックを生成しないファイル サーバ、またはパケット アナライザなどです。この場合、サイレント パートナーに接続された物理ポート上で PAgP を稼働させると、このスイッチ ポートが動作しなくなります。ただし、サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI） （113 ページ）
EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （109 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （111 ページ）
ポートチャネル論理インターフェイスの作成 （CLI）
物理インターフェイスの設定（CLI）

PAgP 学習方式およびプライオリティ

ネットワーク デバイスは、PAgP 物理ラーナーまたは集約ポート ラーナーに分類されます。物理ポートによってアドレスを学習し、その知識に基づいて送信を指示するデバイスは物理ラーナーです。集約（論理）ポートによってアドレスを学習するデバイスは、集約ポート ラーナーです。学習方式は、リンクの両端で同一の設定にする必要があります。

デバイスとそのパートナーが両方とも集約ポート ラーナーの場合、論理ポートチャネル上のアドレスを学習します。デバイスは EtherChannel のいずれかのポートを使用することによって、

送信元にパケットを送信します。集約ポート ラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。

PAgP は、パートナー デバイスが物理ラーナーの場合およびローカル デバイスが集約ポート ラーナーの場合には自動検出できません。したがって、物理ポートでアドレスを学習するには、ローカルデバイスに手動で学習方式を設定する必要があります。また、負荷の分散方式を送信元ベース分散に設定して、指定された送信元 MAC アドレスが常に同じ物理ポートに送信されるようにする必要もあります。

グループ内の 1 つのポートですべての伝送を行うように設定して、他のポートをホット スタンバイに使用することもできます。選択された 1 つのポートでハードウェア信号が検出されなくなった場合は、数秒以内に、グループ内の未使用のポートに切り替えて動作させることができます。パケット伝送用に常に選択されるようにポートを設定するには、**pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用してプライオリティを変更します。プライオリティが高いほど、そのポートが選択される可能性が高まります。

（注） CLI で **physical-port** キーワードを指定した場合でも、デバイスがサポートするのは、集約ポート上でのアドレス ラーニングのみです。**pagp learn-method** コマンドおよび **pagp port-priority** コマンドは、デバイスのハードウェアには作用しませんが、Catalyst 1900 スイッチなどの物理ポートによるアドレス ラーニングだけをサポートするデバイスと PAgP の相互運用性を確保するために必要です。

デバイスのリンク パートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用して物理ポート ラーナーとしてデバイスを設定することを推奨します。送信元 MAC アドレスに基づいて負荷の分散方式を設定するには、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用します。すると、デバイスは送信元アドレスを学習した EtherChannel 内の同じポートを使用して、物理ラーナーにパケットを送信します。**pagp learn-method** コマンドは、このような場合のみ使用してください。

関連トピック

PAgP 学習方式およびプライオリティの設定 （CLI） （122 ページ）
EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （109 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ （133 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （111 ページ）

PAgP と他の機能との相互作用

ダイナミック トランキング プロトコル（DTP）および Cisco Discovery Protocol（CDP）は、EtherChannel の物理ポートを使用してパケットを送受信します。トランク ポートは、番号が最も小さい VLAN 上で PAgP プロトコル データ ユニット（PDU）を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを提供します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つ

が EtherChannel に MAC アドレスを提供します。レイヤ 3 EtherChannel の場合は、（**interface port-channel** グローバル コンフィギュレーション コマンドを使用して）ポートが作成された直後に、アクティブなデバイスによって MAC アドレスが割り当てられます。

PAgP が PAgP PDU を送受信するのは、PAgP が auto モードまたは desirable モードでイネーブルになっている、稼働状態のポート上だけです。

リンク アグリケーション制御プロトコル

LACP は IEEE 802.3ad で定義されており、Cisco デバイスが IEEE 802.3ad プロトコルに適合したデバイス間のイーサネットチャネルを管理できるようにします。LACP を使用すると、イーサネット ポート間で LACP パケットを交換することにより、EtherChannel を自動的に作成できます。

デバイスまたはデバイス スタックは LACP を使用することによって、LACP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似しているポートを単一の倫理リンク（チャネルまたは集約ポート）に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポートパラメータ制約です。たとえば、LACP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同じポートをグループとしてまとめます。リンクをまとめて EtherChannel を形成した後で、LACP は単一デバイス ポートとして、スパニングツリーにそのグループを追加します。

ポート チャネル内のポートの独立モード動作が変更されます。CSCtn96950 では、デフォルトでスタンドアロン モードが有効になっています。LACP ピアから応答が受信されない場合、ポート チャネル内のポートは中断状態に移動されます。

LACP モード

LACP モードでは、ポートが LACP パケットを送信できるか、LACP パケットの受信のみができるかどうかを指定します。

表 *11 : EtherChannel LACP* モード

[モード（Mode）]	説明
active	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。
passive	ポートはパッシブ ネゴシエーション ステートになります。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。これにより、LACP パケットの送信を最小限に抑えます。

active モードおよび **passive LACP** モードはともに、相手ポートとネゴシエーションして、ポート速度などの条件に基づいて（レイヤ 2 EtherChannel の場合は、トランク ステートおよび VLAN 番号などの基準に基づいて）、ポートで EtherChannel を形成できるようにします。

LACP モードが異なっていても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。次に例を示します。

- **active** モードのポートは、**active** モードまたは **passive** モードの別のポートとともに EtherChannel を形成できます。
- 両ポートとも LACP ネゴシエーションを開始しないため、**passive** モードのポートは、**passive** モードの別のポートと EtherChannel を形成することはできません。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI） （113 ページ）
EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （109 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （111 ページ）

LACP とリンクの冗長性

LACP ポートチャネルの最小リンクおよび LACP の最大バンドルの機能を使用して、LACP ポートチャネル動作、帯域幅の可用性およびリンク冗長性をさらに高めることができます。

LACP ポートチャネルの最小リンク機能：

- LACP ポート チャネルでリンクし、バンドルする必要があるポートの最小数を設定します。
- 低帯域幅の LACP ポート チャネルがアクティブにならないようにします。
- 必要な最低帯域幅を提供する十分なアクティブ メンバ ポートがない場合、LACP ポート チャネルが非アクティブになるようにします。

LACP の最大バンドル機能：

- LACP ポート チャネルのバンドル ポートの上限数を定義します。
- バンドル ポートがより少ない場合のホット スタンバイ ポートを可能にします。たとえば、5 個のポートがある LACP ポート チャネルで、3 個の最大バンドルを指定し、残りの 2 個のポートをホット スタンバイ ポートとして指定できます。

関連トピック

LACP 最大バンドル機能の設定（CLI） （124 ページ）
LACP ホット スタンバイ ポートの設定：例 （136 ページ）
LACP ポート チャネルの最小リンク機能の設定（CLI） （126 ページ）

LACP と他の機能との相互作用

DTP および CDP は、EtherChannel の物理ポートを介してパケットを送受信します。トランクポートは、番号が最も小さい VLAN 上で LACP PDU を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを提供します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。レイヤ 3 EtherChannel の場合は、**interface port-channel** グローバル コンフィギュレーション コマンドでインターフェイスが作成された直後に、アクティブなデバイスによって MAC アドレスが割り当てられます。

LACP が LACP PDU を送受信するのは、LACP が active モードまたは passive モードでイネーブルになっている稼働状態のポートとの間だけです。

EtherChannel の On モード

EtherChannel の **on** モードは、EtherChannel の手動設定に使用します。**on** モードを使用すると、ポートはネゴシエーションせずに強制的に EtherChannel に参加します。リモート デバイスが PAgP や LACP をサポートしていない場合にこの **on** モードが役立ちます。**on** モードでは、リンクの両端のデバイスが **on** モードに設定されている場合のみ EtherChannel を使用できます。

同じチャネル グループの **on** モードで設定されたポートは、速度やデュプレックスのようなポート特性に互換性を持たせる必要があります。**on** モードで設定されている場合でも、互換性のないポートは suspended ステートになります。

注意 **on** モードの使用には注意が必要です。これは手動の設定であり、EtherChannel の両端のポートには、同一の設定が必要です。グループの設定を誤ると、パケット損失またはスパニングツリー ループが発生することがあります。

ロードバランシングおよび転送方式

EtherChannel は、フレーム内のアドレスに基づいて形成されたバイナリ パターンの一部を、チャネル内の 1 つのリンクを選択する数値に縮小することによって、チャネル内のリンク間でトラフィックのロード バランシングを行います。MAC アドレス、IP アドレス、送信元アドレス、宛先アドレス、または送信元と宛先両方のアドレスに基づいた負荷分散など、複数の異なるロードバランシング モードから 1 つを指定できます。選択したモードは、デバイス上で設定されているすべての EtherChannel に適用されます。

（注） レイヤ 3 等コスト マルチ パス（ECMP）のロード バランシングは、送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびレイヤ 4 プロトコルに基づいています。フラグメント化されたパケットは、これらのパラメータを使用して計算されたアルゴリズムに基づいて 2 つの異なるリンクで処理されます。これらのパラメータのいずれかを変更すると、ロード バランシングが実行されます。

関連トピック

EtherChannel ロードバランシングの設定（CLI）（119 ページ）
EtherChannel 設定時の注意事項
レイヤ 2 EtherChannel 設定時の注意事項（111 ページ）
EtherChannel のデフォルト設定（109 ページ）
レイヤ 3 EtherChannel 設定時の注意事項（112 ページ）

MAC アドレス転送

送信元 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 MAC アドレスに基づいてチャネル ポート間で分配されます。したがって、ロード バランシングを行うために、送信元ホストが異なるパケットはそれぞれ異なるチャネルポートを使用しますが、送信元ホストが同じパケットは同じチャネル ポートを使用します。

宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットの宛先ホストの MAC アドレスに基づいてチャネル ポート間で分配されます。したがって、宛先が同じパケットは同じポートに転送され、宛先の異なるパケットはそれぞれ異なるチャネル ポートに転送されます。

送信元および宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、送信元および宛先の両方の MAC アドレスに基づいてチャネル ポート間で分配されます。この転送方式は、負荷分散の送信元 MAC アドレス転送方式と宛先 MAC アドレス転送方式を組み合わせたものです。特定のデバイスに対して送信元 MAC アドレス転送と宛先 MAC アドレス転送のどちらが適切であるかが不明な場合に使用できます。送信元および宛先 MAC アドレス転送の場合、ホスト A からホスト B、ホスト A からホスト C、およびホスト C からホスト B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

関連トピック

EtherChannel ロードバランシングの設定（CLI）（119 ページ）
EtherChannel 設定時の注意事項
レイヤ 2 EtherChannel 設定時の注意事項（111 ページ）
EtherChannel のデフォルト設定（109 ページ）
レイヤ 3 EtherChannel 設定時の注意事項（112 ページ）

IP アドレス転送

送信元 IP アドレスベース転送の場合、パケットは、着信パケットの送信元 IP アドレスに基づいて EtherChannel ポート間で分配されます。ロード バランシングを行うために、IP アドレスが異なるパケットはチャネルでそれぞれ異なるポートを使用しますが、IP アドレスが同じパケットはチャネルで同じポートを使用します。

宛先 IP アドレスベース転送の場合、パケットは着信パケットの宛先 IP アドレスに基づいて EtherChannel ポート間で分配されます。ロード バランシングを行うために、同じ送信元 IP アドレスから異なる宛先 IP アドレスに送信されるパケットは、チャネルの異なるチャネル ポートに送信できます。異なる送信元 IP アドレスから同じ宛先 IP アドレスに送信されるパケットは、常にチャネルの同じポートに送信されます。

送信元と宛先 IP アドレスベース転送の場合、パケットは着信パケットの送信元および宛先の両方の IP アドレスに基づいて EtherChannel ポート間で分配されます。この転送方式は、送信元 IP アドレスベース転送方式と宛先 IP アドレスベース転送方式を組み合わせたもので、特定のデバイスに対して送信元 IP アドレスベース転送と宛先 IP アドレスベース転送のどちらが適切であるか不明な場合に使用できます。この方式では、IP アドレス A から IP アドレス B に、IP アドレス A から IP アドレス C に、および IP アドレス C から IP アドレス B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

関連トピック

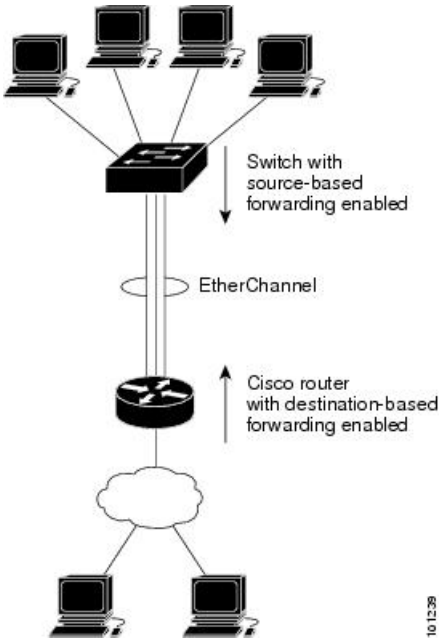
EtherChannel ロードバランシングの設定（CLI） （119 ページ）
EtherChannel 設定時の注意事項
レイヤ 2 EtherChannel 設定時の注意事項 （111 ページ）
EtherChannel のデフォルト設定 （109 ページ）
レイヤ 3 EtherChannel 設定時の注意事項 （112 ページ）

ロードバランシングの利点

ロードバランシング方式には異なる利点があるため、ネットワーク内のデバイスの位置、および負荷分散が必要なトラフィックの種類に基づいて特定のロードバランシング方式を選択する必要があります。

図 *20 :* 負荷の分散および転送方式

次の図では、4 台のワーク ステーションの EtherChannel がルータと通信します。ルータは単一 MAC アドレス デバイスであるため、デバイス EtherChannel で送信元ベース転送を行うことにより、デバイスが、ルータで使用可能なすべての帯域幅を使用することが保証されます。ルータは、宛先アドレスベース転送を行うように設定されます。これは、多数のワークステーションで、トラフィックがルータ EtherChannel から均等に分配されることになっているためです。



設定で一番種類が多くなるオプションを使用してください。たとえば、チャネル上のトラフィックが単一 MAC アドレスを宛先とする場合、宛先 MAC アドレスを使用すると、チャネル内の同じリンクが常に選択されます。ただし、送信元アドレスまたはIPアドレスを使用した方が、ロードバランシングの効率がよくなる場合があります。

関連トピック

EtherChannel ロードバランシングの設定（CLI） （119 ページ）
EtherChannel 設定時の注意事項
レイヤ 2 EtherChannel 設定時の注意事項 （111 ページ）
EtherChannel のデフォルト設定 （109 ページ）
レイヤ 3 EtherChannel 設定時の注意事項 （112 ページ）

EtherChannel およびデバイス スタック

EtherChannel に加入しているポートが含まれているスタック メンバに障害が発生したり、スタックを離れると、アクティブなデバイスにより、障害が発生したスタック デバイス メンバ ポートが削除されます。EtherChannel に残っているポートがある場合、接続は引き続き確保されます。

デバイスが既存のスタックに追加されると、新しいデバイスがアクティブなデバイスから実行コンフィギュレーションを受信し、EtherChannel 関連のスタック コンフィギュレーションで更新されます。スタック メンバでは、動作情報（動作中で、チャネルのメンバであるポートのリスト）も受信します。

2 つのスタック間で設定されている EtherChannel がマージされた場合、セルフループ ポートになります。スパニングツリーにより、この状況が検出され、必要な動作が発生します。権利を獲得したデバイス スタックにある PAgP 設定または LACP 設定は影響を受けませんが、権利を失った デバイス スタックの PAgP 設定または LACP 設定は、スタックのリブート後に失われます。

デバイス スタックおよび PAgP

PAgP では、アクティブ デバイスに障害が発生するか、スタックを離れた場合、スタンバイ デバイスが新しいアクティブ デバイスになります。新しいアクティブ デバイスはアクティブ デバイスの該当項目にスタック メンバの設定を同期します。PAgP 設定は、EtherChannel に古いアクティブ デバイス上にあるポートがない限り、アクティブ デバイスの変更後も影響を受けません。

デバイス スタックおよび LACP

LACP の場合、システム ID は、アクティブ デバイスから取得したスタック MAC アドレスが使用されます。アクティブ デバイスに障害が発生したり、スタックを離れ、スタンバイ デバイスが新しいアクティブ デバイスが変更になっても、LACP システム ID は変更されません。デフォルトでは、LACP 設定はアクティブ デバイスの変更後も影響を受けません。

EtherChannel のデフォルト設定

EtherChannel のデフォルト設定を、次の表に示します。

表 *12 : EtherChannel* のデフォルト設定

機能	デフォルト設定
チャネル グループ	割り当てなし
ポートチャネル論理インターフェイス	未定義
PAgP モード	デフォルトなし。
PAgP 学習方式	すべてのポートで集約ポート ラーニング
PAgP プライオリティ	すべてのポートで 128
LACP モード	デフォルトなし。
LACP 学習方式	すべてのポートで集約ポート ラーニング
LACP ポート プライオリティ	すべてのポートで 32768
LACP システム プライオリティ	32768
LACP システム ID	LACP システムのプライオリティ、デバイスまたはスタックの MAC アドレス。
ロード バランシング	デバイス上での負荷分散は着信パケットの送信元MAC アドレスに基づきます。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI） （113 ページ）
EtherChannel の概要
EtherChannel のモード
デバイス上の EtherChannel
EtherChannel リンクのフェールオーバー
LACP モード （103 ページ）
PAgP モード （100 ページ）
サイレント モード （101 ページ）
ポートチャネル論理インターフェイスの作成 （CLI）
チャネル グループおよびポートチャネル インターフェイス （98 ページ）
物理インターフェイスの設定（CLI）
EtherChannel ロードバランシングの設定（CLI） （119 ページ）
ロードバランシングおよび転送方式 （105 ページ）

MAC アドレス転送 （106 ページ）
IP アドレス転送 （106 ページ）
ロードバランシングの利点 （107 ページ）
PAgP 学習方式およびプライオリティの設定 （CLI） （122 ページ）
PAgP 学習方式およびプライオリティ （101 ページ）
LACP システム プライオリティの設定（CLI） （127 ページ）
LACP ポート プライオリティの設定（CLI） （128 ページ）

EtherChannel 設定時の注意事項

EtherChannel ポートを正しく設定していない場合は、ネットワーク ループおよびその他の問題を回避するために、一部の EtherChannel インターフェイスが自動的にディセーブルになります。設定上の問題を回避するために、次の注意事項に従ってください。

- デバイスまたはデバイス スタック上では、64 を超える EtherChannel を設定しないでください。
- PAgP EtherChannel は、同じタイプのイーサネット ポートを 8 つまで使用して設定します。
- 同じタイプのイーサネット ポートを最大で 16 個備えた LACP EtherChannel を設定してください。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
- EtherChannel 内のすべてのポートを同じ速度および同じデュプレックス モードで動作するように設定します。
- EtherChannel 内のすべてのポートをイネーブルにします。**shutdown** インターフェイス コンフィギュレーション コマンドによってディセーブルにされた EtherChannel 内のポートは、リンク障害として扱われます。そのポートのトラフィックは、EtherChannel 内の他のポートの 1 つに転送されます。
- グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次のパラメータのいずれかで設定を変更した場合は、グループ内のすべてのポートでも変更する必要があります。
  - 許可 VLAN リスト
  - 各 VLAN のスパニングツリー パス コスト
  - 各 VLAN のスパニングツリー ポート プライオリティ
  - スパニングツリー PortFast の設定
- 1 つのポートが複数の EtherChannel グループのメンバになるように設定しないでください。
- EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。PAgP および LACP を実行している EtherChannel グループはスタックの同一デバイス、または異なるデバイスで共存できます。個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用することはできません。

- アクティブまたはアクティブでない EtherChannel メンバであるポートを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。
- EtherChannel がデバイス インターフェイス上に設定されている場合、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを使用して、IEEE 802.1x をデバイス上でグローバルにイネーブルにする前に、EtherChannel の設定をインターフェイスから削除します。

レイヤ 2 EtherChannel 設定時の注意事項

レイヤ 2 EtherChannels を設定する場合は、次の注意事項に従ってください。

- EtherChannel 内のすべてのポートを同じ VLAN に割り当てるか、またはトランクとして設定してください。複数のネイティブ VLAN に接続されるポートは、EtherChannel を形成できません。
- EtherChannel は、トランキング レイヤ 2 EtherChannel 内のすべてのポート上で同じ VLAN 許容範囲をサポートしています。VLAN 許容範囲が一致していないと、PAgP が **auto** モードまたは **desirable** モードに設定されていても、ポートは EtherChannel を形成しません。
- スパニングツリー パス コストが異なるポートは、設定上の矛盾がない限り、EtherChannel を形成できます。異なるスパニングツリー パス コストを設定すること自体は、EtherChannel を形成するポートの矛盾にはなりません。

関連トピック

レイヤ 2 EtherChannel の設定 （CLI） （113 ページ）
EtherChannel の概要
EtherChannel のモード
デバイス上の EtherChannel
EtherChannel リンクのフェールオーバー
LACP モード （103 ページ）
PAgP モード （100 ページ）
サイレント モード （101 ページ）
ポートチャネル論理インターフェイスの作成 （CLI）
チャネル グループおよびポートチャネル インターフェイス （98 ページ）
物理インターフェイスの設定（CLI）
EtherChannel ロードバランシングの設定（CLI） （119 ページ）
ロードバランシングおよび転送方式 （105 ページ）
MAC アドレス転送 （106 ページ）
IP アドレス転送 （106 ページ）
ロードバランシングの利点 （107 ページ）
PAgP 学習方式およびプライオリティの設定 （CLI） （122 ページ）
PAgP 学習方式およびプライオリティ （101 ページ）

LACP システム プライオリティの設定（CLI） （127 ページ）
LACP ポート プライオリティの設定（CLI） （128 ページ）

レイヤ 3 EtherChannel 設定時の注意事項

- レイヤ 3 EtherChannel の場合は、レイヤ 3 アドレスをチャネル内の物理ポートでなく、ポートチャネル論理インターフェイスに割り当ててください。

関連トピック

EtherChannel ロードバランシングの設定（CLI） （119 ページ）
ロードバランシングおよび転送方式 （105 ページ）
MAC アドレス転送 （106 ページ）
IP アドレス転送 （106 ページ）
ロードバランシングの利点 （107 ページ）

Auto-LAG

Auto-LAG 機能は、スイッチに接続されたポートで EtherChannel を自動的に作成できる機能です。デフォルトでは、Auto-LAG がグローバルに無効にされ、すべてのポートインターフェイスで有効になっています。Auto-LAG は、グローバルに有効になっている場合にのみ、スイッチに適用されます。

Auto-LAG をグローバルに有効にすると、次のシナリオが可能になります。

- パートナー ポート インターフェイス上に EtherChannel が設定されている場合、すべてのポートインターフェイスが自動 EtherChannel の作成に参加します。詳細については、次の表「アクターとパートナー デバイス間でサポートされる *Auto-LAG* 設定」を参照してください。
- すでに手動 EtherChannel の一部であるポートは、自動 EtherChannel の作成に参加することはできません。
- Auto-LAG がすでに自動で作成された EtherChannel の一部であるポート インターフェイスで無効になっている場合、ポートインターフェイスは自動 EtherChannel からバンドル解除されます。

次の表に、アクターとパートナー デバイス間でサポートされる Auto-LAG 設定を示します。

表 *13*：アクターとパートナー デバイス間でサポートされる *Auto-LAG* 設定

アクター/パートナー	Active	パッシブ	Auto
Active	○	○	○
パッシブ	[はい（Yes）]	[いいえ（No）]	○
Auto	○	○	○

Auto-LAG をグローバルに無効にすると、自動で作成されたすべての Etherchannel が手動 EtherChannel になります。

既存の自動で作成された EtherChannel で設定を追加することはできません。追加するには、最初に **port-channel**<*channel-number*>**persistent** を実行して、手動 EtherChannel に変換する必要があります。

（注） Auto-LAG は自動 EtherChannel の作成に LACP プロトコルを使用します。一意のパートナー デバイスで自動的に作成できる EtherChannel は 1 つだけです。

Auto-LAG 設定時の注意事項

Auto-LAG 機能を設定するときには、次の注意事項に従ってください。

- Auto-LAG がグローバルで有効な場合、およびポート インターフェイスで有効な場合に、ポート インターフェイスを自動 EtherChannel のメンバーにしたくない場合は、ポート インターフェイスで Auto-LAG を無効にします。
- ポート インターフェイスは、すでに手動 EtherChannel のメンバーである場合、自動 EtherChannel にバンドルされません。自動 EtherChannel にバンドルされるようにするには、まずポート インターフェイスで手動 EtherChannel のバンドルを解除します。
- Auto-LAG が有効になり、自動 EtherChannel が作成されると、同じパートナー デバイスで複数の EtherChannel を手動で作成できます。ただし、デフォルトでは、ポートはパートナー デバイスで自動 EtherChannel の作成を試行します。
- Auto-LAG は、レイヤ 2 EtherChannel でのみサポートされています。レイヤ 3 インターフェイスおよびレイヤ 3 EtherChannel ではサポートされていません。
- Auto-LAG は、Cross-Stack EtherChannel でサポートされています。

EtherChannel の設定方法

EtherChannel の設定後、ポートチャネル インターフェイスに適用した設定変更は、そのポートチャネル インターフェイスに割り当てられたすべての物理ポートに適用されます。また、物理ポートに適用した設定変更は、設定を適用したポートだけに作用します。

レイヤ 2 EtherChannel の設定 （CLI）

レイヤ 2 EtherChannel を設定するには、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、チャネル グループにポートを割り当てます。このコマンドにより、ポートチャネル論理インターフェイスが自動的に作成されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# 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** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスは、物理ポートです。 PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 まで設定できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
ステップ 3	**switchport mode** {**access** | **trunk**} 例： `Device(config-if)# switchport mode access`	すべてのポートをスタティックアクセス ポートとして同じ VLAN に割り当てるか、またはトランクとして設定します。 ポートをスタティックアクセス ポートとして設定する場合は、ポートを1つの VLANにのみ割り当ててください。指定できる範囲は 1 ～ 4094 です。
ステップ 4	**switchport access vlan** *vlan-id* 例： `Device(config-if)# switchport access vlan 22`	ポートをスタティックアクセス ポートとして設定する場合は、ポートを1つの VLANにのみ割り当ててください。指定できる範囲は 1 ～ 4094 です。
ステップ 5	**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on** } | { **active** | **passive**} 例： `Device(config-if)# channel-group 5 mode auto`	チャネル グループにポートを割り当て、PAgP モードまたは LACP モードを指定します。 **mode** には、次のキーワードのいずれか 1 つを選択します。

	コマンドまたはアクション	目的
		• **auto**–PAgP 装置が検出された場合に限り、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。。 • **desirable**–無条件に PAgP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。。 • **on**–PAgP または LACP を使用せずにポートが強制的にチャネル化されます。**on** モードでは、使用可能な EtherChannel が存在するのは、**on** モードのポート グループが、**on** モードの別のポート グループに接続する場合だけです。 • **non-silent**–（任意）デバイスが PAgP 対応のパートナーに接続されている場合、ポートが **auto** または **desirable** モードになると非サイレント動作を行うようにデバイス ポートを設定します。**non-silent** を指定しないと、サイレントが想定されます。サイレント設定は、ファイル サーバまたはパケット アナライザとの接続に適しています。サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。 • **active**：LACP 装置が検出された場合に限り、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートはLACPパケットを

	コマンドまたはアクション	目的
		送信することによって、相手ポートとのネゴシエーションを開始します。 • **passive**–ポート上で LACP をイネーブルにして、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

EtherChannel の概要
EtherChannel のモード
デバイス上の EtherChannel
EtherChannel リンクのフェールオーバー
LACP モード （103 ページ）
PAgP モード （100 ページ）
サイレント モード （101 ページ）
EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （109 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （111 ページ）

レイヤ 3 EtherChannel の設定 （CLI）

レイヤ 3 EtherChannel にイーサネット ポートを割り当てるには、この手順を実行します。この手順は必須です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。 PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 まで設定できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
ステップ 4	**no ip address** 例： `Device(config-if)# no ip address`	物理ポートに割り当てられている IP アドレスがないことを確認します。
ステップ 5	**noswitchport** 例： `Device(config-if)# no switchport`	ポートをレイヤ 3 モードにします。
ステップ 6	**channel-group** *channel-group-number* **mode** {**auto** ［**non-silent**］ | **desirable** ［**non-silent**］ | **on**} | {**active** | **passive**} 例：	チャネル グループにポートを割り当て、PAgP モードまたは LACP モードを指定します。 **mode** には、次のキーワードのいずれか 1 つを選択します。

	コマンドまたはアクション	目的
	`Device(config-if)# channel-group 5 mode auto`	• **auto**：PAgP 装置が検出された場合に限り、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。このキーワードは、EtherChannel メンバがデバイス スタックの異なるデバイスのものである場合にはサポートされません。 • **desirable**：無条件に PAgP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。このキーワードは、EtherChannel メンバがデバイス スタックの異なるデバイスのものである場合にはサポートされません。 • **on**：PAgP や LACP を使用しないで、ポートを強制的にチャネル化します。**on** モードでは、使用可能な EtherChannel が存在するのは、**on** モードのポート グループが、**on** モードの別のポート グループに接続する場合だけです。 • **non-silent**：（任意）デバイスが PAgP 対応のパートナーに接続されている場合、ポートが **auto** または **desirable** モードになると非サイレント動作を行うようにデバイス ポートを設定します。**non-silent** を指定しないと、サイレントが想定されます。サイレント設定は、ファイル サーバまたはパケット アナライザとの接続に適しています。サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。

	コマンドまたはアクション	目的
		• **active**：LACP 装置が検出された場合に限り、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートはLACPパケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • **passive**–ポート上で LACP をイネーブルにして、ポートをパッシブ ネゴシエーションステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。
ステップ 7	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

EtherChannel ロードバランシングの設定（CLI）

複数の異なる転送方式の 1 つを使用するように EtherChannel ロードバランシングを設定できます。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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-channel load-balance** {**dst-ip** | **dst-mac** | **dst-mixed-ip-port** | **dst-port** | **extended** [**dst-ip** | **dst-mac** | **dst-port** | **ipv6-label** | **l3-proto** | **src-ip** | **src-mac** | **src-port**] |	EtherChannel のロードバランシング方式を設定します。 デフォルトは **src-mac** です。

	コマンドまたはアクション	目的
	src-dst-ip | **src-dst-mac** **src-dst-mixed-ip-port src-dst-portsrc-ip** | **src-mac** | **src-mixed-ip-port** | **src-port**} 例： `Device(config)# port-channel load-balance src-mac`	次のいずれかの負荷分散方式を選択します。 • **dst-ip**：宛先ホストの IP アドレスを指定します。 • **dst-mac**：着信パケットの宛先ホストの MAC アドレスを指定します。 • **dst-mixed-ip-port**：ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • **dst-port**：宛先 TCP/UDP ポートを指定します。 • **extended**：標準コマンドで使用可能なもの以外に、送信元および宛先の方式を組み合わせた、拡張ロードバランシング方式を指定します。 • **ipv6-label**：IPv6 フロー ラベルを指定します。 • **l3-proto**：レイヤ 3 プロトコルを指定します。 • **src-dst-ip**：送信元および宛先ホストの IP アドレスを指定します。 • **src-dst-mac**：送信元および宛先ホストの MAC アドレスを指定します。 • **src-dst-mixed-ip-port**：送信先および宛先ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • **src-dst-port**：送信元および宛先 TCP/UDP ポートを指定します。 • **src-ip**：送信元ホストの IP アドレスを指定します。 • **src-mac**：着信パケットの送信元 MAC アドレスを指定します。 • **src-mixed-ip-port**：送信元ホストの IP アドレスおよび TCP/UDP ポートを指定します。

	コマンドまたはアクション	目的
		• **src-port**：送信元 TCP/UDP ポートを指定します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

ロードバランシングおよび転送方式 （105 ページ）
MAC アドレス転送 （106 ページ）
IP アドレス転送 （106 ページ）
ロードバランシングの利点 （107 ページ）
EtherChannel 設定時の注意事項
レイヤ 2 EtherChannel 設定時の注意事項 （111 ページ）
EtherChannel のデフォルト設定 （109 ページ）
レイヤ 3 EtherChannel 設定時の注意事項 （112 ページ）

EtherChannel 拡張ロードバランシングの設定（CLI）

ロードバランシング方式を組み合わせて使用する場合には、拡張ロードバランシングを設定します。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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-channel load-balance extended** ［**dst-ip** ｜ **dst-macdst-port** ｜ **ipv6-label** ｜ **l3-proto** ｜ **src-ip** ｜ **src-mac** ｜ **src-port** ］ 例： `Device(config)# port-channel load-balance extended dst-ip dst-mac src-ip`	EtherChannel 拡張ロードバランシング方式を設定します。 デフォルトは **src-mac** です。 次のいずれかの負荷分散方式を選択します。 • **dst-ip**：宛先ホストの IP アドレスを指定します。

	コマンドまたはアクション	目的
		• **dst-mac**：着信パケットの宛先ホストのMACアドレスを指定します。 • **dst-port**：宛先TCP/UDPポートを指定します。 • **ipv6-label**：IPv6 フロー ラベルを指定します。 • **l3-proto**：レイヤ 3 プロトコルを指定します。 • **src-ip**：送信元ホストのIPアドレスを指定します。 • **src-mac**：着信パケットの送信元MAC アドレスを指定します。 • **src-port**：送信元TCP/UDPポートを指定します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

PAgP 学習方式およびプライオリティの設定 （CLI）

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	伝送ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**pagp learn-methodphysical-port** 例： `Device(config-if)# pagp learn-method physical port`	PAgP 学習方式を選択します。 デフォルトでは、**aggregation-port learning** が選択されています。つまり、EtherChannel 内のポートのいずれかを使用して、デバイスがパケットを送信元に送信します。集約ポート ラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。 物理ポート ラーナー is別のデバイスに接続する**physical-port**を選択します。 **port-channel load-balance** グローバル コンフィギュレーション コマンドを **src-mac** に設定してください。 学習方式はリンクの両端で同じ方式に設定する必要があります。
ステップ 4	**pagp port-priority** *[プライオリティ（priority）]* 例： `Device(config-if)# pagp port-priority 200`	選択したポートがパケット伝送用として選択されるように、プライオリティを割り当てます。 *priority* に指定できる範囲は 0 ～ 255 です。デフォルトは 128 です。プライオリティが高いほど、ポートが PAgP 伝送に使用される可能性が高くなります。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

PAgP 学習方式およびプライオリティ （101 ページ）
EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （109 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ （133 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （111 ページ）

LACP ホット スタンバイ ポートの設定

LACP がイネーブルの場合、ソフトウェアはデフォルトで、チャネルにおける LACP 互換ポートの最大数（最大 16 個のポート）の設定を試みます。一度にアクティブにできる LACP リン

クは 8 つだけです。残りの 8 個のリンクがホット スタンバイ モードになります。アクティブリンクの 1 つが非アクティブになると、ホット スタンバイ モードのリンクが代わりにアクティブになります。

チャネルでアクティブ ポートの最大数を指定することでデフォルト動作を上書きできます。この場合、残りのポートがホット スタンバイ ポートになります。たとえばチャネルで最大 5 個のポートを指定した場合、11 個までのポートがホット スタンバイ ポートになります。

9 つ以上のリンクが EtherChannel グループとして設定された場合、ソフトウェアは LACP プライオリティに基づいてアクティブにするホット スタンバイ ポートを決定します。ソフトウェアは、LACP を操作するシステム間のすべてのリンクに、次の要素（プライオリティ順）で構成された一意のプライオリティを割り当てます。

- LACP システム プライオリティ
- システム ID（デバイス MAC アドレス）
- LACP ポート プライオリティ
- ポート番号

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。プライオリティは、ハードウェア上の制約がある場合に、すべての互換ポートが集約されないように、スタンバイ モードにするポートを決定します。

アクティブ ポートかホット スタンバイ ポートかを判別するには、次の（2 つの）手順を使用します。まず、数値的に低いシステム プライオリティとシステム ID を持つシステムの方を選びます。次に、ポートプライオリティおよびポート番号の値に基づいて、そのシステムのアクティブ ポートとホット スタンバイ ポートを決定します。他のシステムのポート プライオリティとポート番号の値は使用されません。

ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響を与えるように、LACP システム プライオリティおよび LACP ポート プライオリティのデフォルト値を変更できます。

LACP 最大バンドル機能の設定（CLI）

ポート チャネルで許可されるバンドル化された LACP ポートの最大数を指定すると、ポート チャネル内の残りのポートがホット スタンバイ ポートとして指定されます。

ポート チャネルの LACP ポートの最大数を設定するには、特権 EXEC モードで開始して、次の手順に従います。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**interface port-channel** *channel-number* 例： `Device(config)# interface port-channel 2`	ポート チャネル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。 指定できる範囲は 1 ～ 128 です。
ステップ 3	**lacp max-bundle** *max-bundle-number* 例： `Device(config-if)# lacp max-bundle 3`	ポートチャネル バンドルで LACP ポートの最大数を指定します。 指定できる範囲は 1 ～ 8 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

LACP とリンクの冗長性 （104 ページ）
LACP ホット スタンバイ ポートの設定：例 （136 ページ）

LACP ポートチャネル スタンドアロン ディセーブルの設定

ポート チャネルのスタンドアロン EtherChannel メンバー ポート ステートをディセーブルにするには、ポート チャネル インターフェイスで次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# 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 port-channel** *channel-group* 例： `Device(config)# interface port-channel channel-group`	設定するポート チャネル インターフェイスを選択します。

	コマンドまたはアクション	目的
ステップ 3	**port-channel standalone-disable** 例： `Device(config-if)# port-channel standalone-disable`	ポートチャネル インターフェイスのスタンドアロン モードをディセーブルにします。
ステップ 4	**end** 例： `Device(config-if)# end`	コンフィギュレーション モードを終了します。

ステップ 5	**show etherchannel**
	例：
	`Device# show etherchannel channel-group port-channel`
	`Device# show etherchannel channel-group detail`
		設定を確認します。

LACP ポート チャネルの最小リンク機能の設定（CLI）

リンク アップ状態で、リンク アップ ステートに移行するポート チャネル インターフェイスの EtherChannel でバンドルする必要のあるアクティブ ポートの最小数を指定できます。EtherChannel の最小リンクを使用して、低帯域幅 LACP EtherChannel がアクティブになることを防止できます。また、LACP EtherChannel にアクティブ メンバー ポートが少なすぎて、必要な最低帯域幅を提供できない場合、この機能により LACP EtherChannel が非アクティブになります。

ポート チャネルに必要なリンクの最小数を設定する。次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**interface port-channel** *channel-number* 例： `Device(config)# interface port-channel`	ポートチャネル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。

	コマンドまたはアクション	目的
	2	*channel-number* の範囲は 1 ～ 63 です。
ステップ 4	**port-channel min-links** *min-links-number* 例： `Device(config-if)# port-channel min-links 3`	リンク アップ状態で、リンク アップ ステートに移行するポート チャネル インターフェイスの EtherChannel でバンドルする必要のあるメンバ ポートの最小数を指定できます。 *min-links-number* の範囲は 2 ～ 8 です。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

LACP とリンクの冗長性 （104 ページ）
LACP ホット スタンバイ ポートの設定：例 （136 ページ）

LACP システム プライオリティの設定（CLI）

lacp system-priority グローバル コンフィギュレーション コマンドを使用して、LACP をイネーブルにしているすべての EtherChannel に対してシステム プライオリティを設定できます。LACP を設定済みの各チャネルに対しては、システム プライオリティを設定できません。デフォルト値を変更すると、ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響します。

show etherchannel summary 特権 EXEC コマンドを使用して、ホット スタンバイ モードのポートを確認できます（ポートステート フラグが H になっています）。

LACP システム プライオリティを設定するには、次の手順に従います。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例：	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
	`Device# configure terminal`	
ステップ 3	**lacp system-priority** *[プライオリティ（priority）]* 例： `Device(config)# lacp system-priority 32000`	LACP システム プライオリティを設定します。 指定できる範囲は 1 ～ 65535 です。デフォルトは 32768 です。 値が小さいほど、システム プライオリティは高くなります。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

関連トピック

EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （109 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （111 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ （133 ページ）

LACP ポート プライオリティの設定（CLI）

デフォルトでは、すべてのポートは同じポート プライオリティです。ローカル システムのシステムプライオリティおよびシステム ID の値がリモート システムよりも小さい場合は、LACP EtherChannel ポートのポート プライオリティをデフォルトよりも小さな値に変更して、最初にアクティブになるホットスタンバイ リンクを変更できます。ホット スタンバイ ポートは、番号が小さい方が先にチャネルでアクティブになります。**show etherchannel summary** 特権 EXEC コマンドを使用して、ホット スタンバイ モードのポートを確認できます（ポートステート フラグが H になっています）。

（注） LACP がすべての互換ポートを集約できない場合（たとえば、ハードウェアの制約が大きいリモート システム）、EtherChannel 中でアクティブにならないポートはすべてホット スタンバイ ステートになり、チャネル化されたポートのいずれかが機能しない場合に限り使用されます。

LACP ポート プライオリティを設定するには、次の手順に従います。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**lacp port-priority** *[プライオリティ（priority）]* 例： `Device(config-if)# lacp port-priority 32000`	LACP ポート プライオリティを設定します。 指定できる範囲は 1 ～ 65535 です。デフォルトは 32768 です。値が小さいほど、ポートが LACP 伝送に使用される可能性が高くなります。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

EtherChannel 設定時の注意事項
EtherChannel のデフォルト設定 （109 ページ）
レイヤ 2 EtherChannel 設定時の注意事項 （111 ページ）
EtherChannel、PAgP、および LACP ステータスのモニタ （133 ページ）

LACP 高速レート タイマーの設定

LACP タイマー レートを変更することにより、LACP タイムアウトの時間を変更することができます。**lacp rate** コマンドを使用すれば、LACP がサポートされているインターフェイスで受

信される LACP 制御パケットのレートを設定できます。タイムアウト レートは、デフォルトのレート（30秒）から高速レート（1秒）に変更することができます。このコマンドは、LACP がイネーブルになっているインターフェイスでのみサポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* 例： `Device(config)# interface gigabitEthernet 2/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**lacp rate** {**normal** | **fast**} 例： `Device(config-if)# lacp rate fast`	LACP がサポートされているインターフェイスで受信される LACP 制御パケットのレートを設定します。 • タイムアウト レートをデフォルトにリセットするには、**no lacp rate** コマンドを使用します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ステップ 6	**show lacp internal**
	例：
	`Device# show lacp internal`
	`Device# show lacp counters`
		設定を確認します。

グローバルな Auto-LAG の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**[no] port-channel auto** 例： `Device(config)# port-channel auto`	スイッチ上の Auto-LAG 機能をグローバルで有効にします。スイッチ上の Auto-LAG 機能をグローバルで無効にするには、このコマンドの no 形式を使用します。 （注） デフォルトでは、auto-LAG 機能は各ポート上でイネーブルになっています。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show etherchannel auto** 例： `Device# show etherchannel auto`	EtherChannel が自動的に作成されたことが表示されます。

ポート インターフェイスでの Auto-LAG の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	Auto-LAG を有効にするポート インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**[no] channel-group auto** 例： `Device(config-if)# channel-group auto`	（任意）個々のポート インターフェイスで Auto-LAG 機能を有効にします。個々のポート インターフェイス上で Auto-LAG 機能を無効にするには、このコマンドの no 形式を使用します。 （注） デフォルトでは、auto-LAG 機能は各ポート上でイネーブルになっています。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show etherchannel auto** 例： `Device# show etherchannel auto`	EtherChannel が自動的に作成されたことが表示されます。

次のタスク

Auto-LAG での持続性の設定

自動で作成された EtherChannel を手動のものに変更し、既存の EtherChannel に設定を追加するには、persistence コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**port-channel** *channel-number* **persistent** 例： `Device# port-channel 1 persistent`	自動で作成された EtherChannel を手動のものに変更し、EtherChannel に設定を追加することができます。
ステップ 3	**show etherchannel summary** 例： `Device# show etherchannel summary`	EtherChannel 情報を表示します。

EtherChannel、PAgP、および LACP ステータスのモニタ

この表に記載されているコマンドを使用して EtherChannel、PAgP、および LACP ステータスを表示できます。

表 *14 : EtherChannel*、*PAgP*、および *LACP* ステータスのモニタ用コマンド

コマンド（Command）	説明
clear lacp { *channel-group-number* **counters** | **counters**}	LACP チャネル グループ情報およびトラフィック カウンタをクリアします。
clear pagp { *channel-group-number* **counters** | **counters**}	PAgP チャネル グループ情報およびトラフィック カウンタをクリアします。
show etherchannel [*channel-group-number* {**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**}] [**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **auto** | **summary**]	EtherChannel 情報が簡潔、詳細に、1 行のサマリー形式で表示されます。負荷分散方式またはフレーム配布方式、ポート、ポート チャネル、プロトコル、および Auto-LAG 情報も表示されます。

コマンド（Command）	説明
show pagp ［*channel-group-number*］｛**counters** ｜ **internal** ｜ **neighbor**｝	トラフィック情報、内部PAgP設定、ネイバー情報などの PAgP 情報が表示されます。
show pagp [*channel-group-number*] **dual-active**	デュアルアクティブ検出ステータスが表示されます。
show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor** | **sys-id**}	トラフィック情報、内部LACP設定、ネイバー情報などの LACP 情報が表示されます。
show running-config	設定エントリを確認します。
show etherchannel load-balance	ポートチャネル内のポート間のロードバランシング、またはフレーム配布方式を表示します。

関連トピック

PAgP 学習方式およびプライオリティの設定 （CLI） （122 ページ）
PAgP 学習方式およびプライオリティ （101 ページ）
LACP システム プライオリティの設定（CLI） （127 ページ）
LACP ポート プライオリティの設定（CLI） （128 ページ）

EtherChannel の設定例

レイヤ 2 EtherChannel の設定：例

この例では、スタック内の 1 つのデバイスに EtherChannel を設定する例を示します。2 つのポートを VLAN 10 のスタティック アクセス ポートとして、PAgP モードが **desirable** であるチャネル 5 に割り当てます。

```
Device# configure terminal
Device(config)# interface range gigabitethernet2/0/1 -2
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode desirable non-silent
Device(config-if-range)# end
```

この例では、スタック内の 1 つのデバイスに EtherChannel を設定する例を示します。2 つのポートは VLAN 10 のスタティックアクセス ポートとして、LACP モードが active であるチャネル 5 に割り当てられます。 **active：**

```
Device# configure terminal
Device(config)# interface range gigabitethernet2/0/1 -2
Device(config-if-range)# switchport mode access
```

```
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode active
Device(config-if-range)# end
```

次の例では、クロススタック EtherChannel を設定する方法を示します。LACP パッシブ モードを使用して、VLAN 10 内のスタティックアクセス ポートとしてスタック メンバ 1 のポートを 2 つ、スタック メンバ 2 のポートを 1 つチャネル 5 に割り当てます。

```
Device# configure terminal
Device(config)# interface range gigabitethernet2/0/4 -5
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode passive
Device(config-if-range)# exit
Device(config)# interface gigabitethernet3/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 10
Device(config-if)# channel-group 5 mode passive
Device(config-if)# exit
```

PoE または LACP ネゴシエーションのエラーは、スイッチからアクセスポイント（AP）に 2 つのポートを設定した場合に発生する可能性があります。このシナリオは、ポートチャネルの設定をスイッチ側で行うと回避できます。詳細については、次の例を参照してください。

```
interface Port-channel1
  switchport access vlan 20
 switchport mode access
  switchport nonegotiate
  no port-channel standalone-disable   <--this one
  spanning-tree portfast
```

（注） ポートがポートのフラッピングに関するLACPエラーを検出した場合は、次のコマンドも含める必要があります。 **no errdisable detect cause pagp-flap**

レイヤ 3 EtherChannel の設定：例

この例では、レイヤ 3 インターフェイスの設定方法を示します。2 つのポートは、LACP モードが **active** であるチャネル 5 に割り当てられます。

```
Device# configure terminal
Device(config)# interface range gigabitethernet2/0/1 -2
Device(config-if-range)# no ip address
Device(config-if-range)# no switchport
Device(config-if-range)# channel-group 5 mode active
Device(config-if-range)# end
```

この例では、クロススタック レイヤ 3 EtherChannel の設定方法を示します。スタック メンバー 2 の 2 つのポートとスタック メンバー 3 の 1 つのポートは、LACP active モードでチャネル 7 に割り当てられます。

```
Device# configure terminal
Device(config)# interface range gigabitethernet2/0/4 -5
Device(config-if-range)# no ip address
Device(config-if-range)# no switchport
Device(config-if-range)# channel-group 7 mode active
Device(config-if-range)# exit
Device(config)# interface gigabitethernet3/0/3
Device(config-if)# no ip address
Device(config-if)# no switchport
Device(config-if)# channel-group 7 mode active
Device(config-if)# exit
```

LACP ホット スタンバイ ポートの設定：例

この例では、少なくとも 3 個のアクティブ ポートがある場合にアクティブ化される EtherChannel を設定する例を示します（ポート チャネル 2）。これは、7 個のアクティブ ポートとホット スタンバイ ポートとしての最大 9 個の残りのポートから構成されます。

```
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# port-channel min-links 3
Device(config-if)# lacp max-bundle 7
```

関連トピック

LACP 最大バンドル機能の設定（CLI） （124 ページ）
LACP とリンクの冗長性 （104 ページ）
LACP ポート チャネルの最小リンク機能の設定（CLI） （126 ページ）

Auto-LAG の設定：例

次に、スイッチに Auto-LAG を設定する例を示します。

```
デバイス> enable
デバイス# configure terminal
デバイス (config)# port-channel auto
デバイス (config-if)# end
デバイス#  show etherchannel auto
```

次の例は、自動的に作成された EtherChannel の概要を示します。

```
デバイス# show etherchannel auto
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
```

```
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SUA)        LACP      Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)
```

次の例は、**port-channel** 1 **persistent** コマンドを実行した後の自動 EtherChannel の概要を示します。

```
デバイス# port-channel 1 persistent

デバイス# show etherchannel summary
Switch# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)
```

EtherChannels の追加リファレンス

関連資料

関連項目	参照先
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9500 Series Switches)* の「Layer 2/3 Commands」の項を参照してください

標準および RFC

標準/RFC	役職（Title）
なし	—

MIB

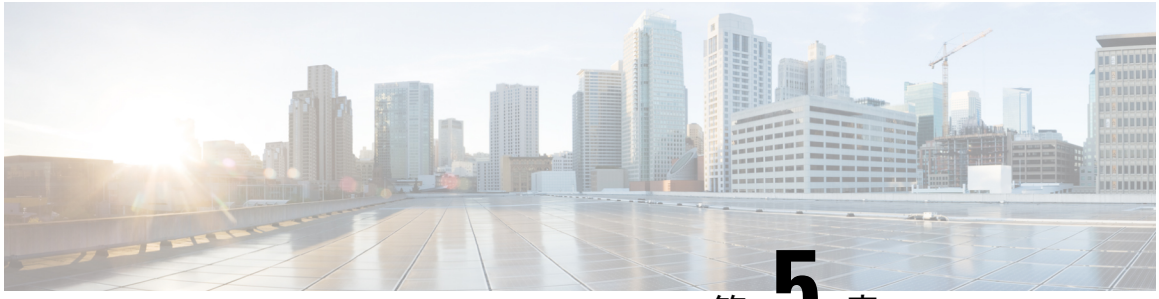
MIB	MIB リンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

EtherChannels の機能情報

リリース	変更箇所
Cisco IOS XE Everest 16.5.1a	この機能が導入されました。



第 5 章

単方向リンク検出の設定

- 機能情報の確認 （139 ページ）
- UDLD 設定の制約事項 （139 ページ）
- UDLD について （140 ページ）
- UDLD の設定方法 （143 ページ）
- UDLD のモニタおよびメンテナンス （146 ページ）
- UDLD の追加リファレンス （146 ページ）
- UDLD の機能情報 （147 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびCisco ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

UDLD 設定の制約事項

次に、単方向リンク検出（UDLD）設定の制約事項を示します。

- UDLD対応ポートが別のデバイスのUDLD非対応ポートに接続されている場合、このポートは単一方向リンクを検出できません。
- モード（通常またはアグレッシブ）を設定する場合、リンクの両側に同じモードを設定します。

⚠

注意 ループ ガードは、ポイントツーポイント リンクでのみサポートされます。リンクの各終端には、STP を実行するデバイスを直接接続することを推奨します。

UDLD について

UniDirectional Link Detection（UDLD）は、光ファイバまたはツイストペア イーサネット ケーブルを通して接続されたデバイスからケーブルの物理設定をモニタリングしたり、単一方向リンクの存在を検出できるようにするためのレイヤ2プロトコルです。このプロトコルが単一方向リンクを正常に識別してディセーブルにするには、接続されたすべてのデバイスで UDLD プロトコルがサポートされている必要があります。UDLD は単一方向リンクを検出すると、影響を受けるポートをディセーブルにして警報を発信します。単一方向リンクは、スパニングツリー トポロジ ループをはじめ、さまざまな問題を引き起こす可能性があります。

動作モード

UDLD は、2 つの動作モードをサポートしています。通常（デフォルト）とアグレッシブです。通常モードの UDLD は、光ファイバ接続におけるポートの誤った接続による単一方向リンクを検出できます。アグレッシブ モードの UDLD は、光ファイバ リンクおよびツイストペア リンク上の片方向トラフィックと、光ファイバ リンク上のポートの誤った接続による単一方向リンクも検出できます。

通常およびアグレッシブの両モードの UDLD は、レイヤ 1 のメカニズムを使用して、リンクの物理ステータスを学習します。レイヤ1では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバー ID の検出、誤って接続されたポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 と 2 の検出機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

ローカルデバイスが送信したトラフィックをネイバーが受信するにもかかわらず、ネイバーから送信されたトラフィックをローカルデバイスが受信しない場合に、単一方向リンクが発生します。

通常モード

通常モードの UDLD は、光ファイバ ポートの光ファイバが誤って接続されている場合に単一方向リンクを検出しますが、レイヤ1メカニズムは、この誤った接続を検出しません。ポートが正しく接続されていてもトラフィックが片方向である場合、単一方向リンクを検出するはずのレイヤ1メカニズムがこの状況を検出できないため、UDLD は単一方向リンクを検出できません。この場合、論理リンクは不確定と見なされ、UDLD はポートをディセーブルにしません。

UDLD が通常モードのときに、ペアの一方の光ファイバが切断されており、自動ネゴシエーションがアクティブであると、レイヤ1メカニズムがリンクの物理的な問題を検出するため、

リンクは稼働状態でなくなります。この場合は、UDLDは何のアクションも行わず、論理リンクは不確定と見なされます。

関連トピック

UDLD のグローバルなイネーブル化（CLI）（143 ページ）
インターフェイスでの UDLD のイネーブル化（CLI）（145 ページ）

Aggressive Mode

アグレッシブ モードでは、UDLD はこれまでの検出方法で単一方向リンクを検出します。アグレッシブ モードの UDLD は、2 つのデバイス間の障害発生が許されないポイントツーポイント リンクの単一方向リンクも検出できます。また、次のいずれかの問題が発生している場合に、単一方向リンクも検出できます。

- 光ファイバ リンクまたはツイストペア リンクで、ポートの 1 つがトラフィックを送受信できない。
- 光ファイバ リンクまたはツイストペア リンクで、ポートの 1 つがダウンし、残りのインターフェイスが稼働している。
- ケーブルのうち 1 本の光ファイバが切断されている。

これらの場合、UDLD は影響を受けたポートをディセーブルにします。

ポイントツーポイント リンクでは、UDLD hello パケットをハートビートと見なすことができ、ハートビートがあればリンクは正常です。逆に、ハートビートがないということは、双方向リンクを再確立できない限り、リンクをシャットダウンする必要があることを意味しています。

レイヤ 1 の観点からケーブルの両方の光ファイバが正常な状態であれば、アグレッシブ モードの UDLD はそれらの光ファイバが正しく接続されているかどうか、およびトラフィックが正しいネイバー間で双方向に流れているかどうかを検出します。自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは自動ネゴシエーションでは実行できません。

関連トピック

UDLD のグローバルなイネーブル化（CLI）（143 ページ）
インターフェイスでの UDLD のイネーブル化（CLI）（145 ページ）

単一方向リンクの検出方法

UDLD は、2 つの方法で動作します。

- ネイバー データベース メンテナンス
- イベント駆動の検出およびエコー

関連トピック

UDLD のグローバルなイネーブル化（CLI）（143 ページ）
インターフェイスでの UDLD のイネーブル化（CLI）（145 ページ）

ネイバー データベース メンテナンス

UDLD は、アクティブな各ポート上で hello パケット（別名アドバタイズまたはプローブ）を定期的に送信して、他の UDLD 対応ネイバーに関して学習し、各デバイスがネイバーに関する情報を常に維持できるようにします。

デバイスが hello メッセージを受信すると、エージング タイム（ホールド タイムまたは存続可能時間）が経過するまで、情報をキャッシュします。古いキャッシュ エントリの期限が切れる前に、デバイスが新しい hello メッセージを受信すると、デバイスが古いエントリを新しいエントリで置き換えます。

UDLD の実行中にポートがディセーブルになったり、ポート上で UDLD がディセーブルになったり、またはデバイスをリセットした場合、UDLD は設定変更の影響を受けるポートの既存のキャッシュ エントリをすべてクリアします。UDLD は、ステータス変更の影響を受けるキャッシュの一部をフラッシュするようにネイバーに通知するメッセージを 1 つまたは複数送信します。このメッセージは、キャッシュを継続的に同期するためのものです。

イベントドリブン検出およびエコー

UDLD は検出動作としてエコーを利用します。UDLD デバイスが新しいネイバーを学習するか、または同期していないネイバーから再同期要求を受信すると、接続の UDLD デバイス側の検出ウィンドウを再起動して、エコー メッセージを返送します。この動作はすべての UDLD ネイバーに対して同様に行われるため、エコー送信側では返信エコーを受信するように待機します。

検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLD モードに応じてシャットダウンされることがあります。UDLD が通常モードにある場合、リンクは不確定と見なされ、シャットダウンされない場合があります。UDLD がアグレッシブ モードにある場合は、リンクは単一方向と見なされ、ポートはディセーブルになります。

関連トピック

UDLD のグローバルなイネーブル化（CLI） （143 ページ）
インターフェイスでの UDLD のイネーブル化（CLI） （145 ページ）

UDLD リセット オプション

インターフェイスが UDLD でディセーブル化された場合、次のオプションの 1 つを使用して UDLD をリセットできます。

- **udld reset** インターフェイス コンフィギュレーション コマンド。
- **shutdown** インターフェイス コンフィギュレーション コマンドに続いて **no shutdown** インターフェイス コンフィギュレーション コマンドを入力すると、ディセーブル化されたポートを再起動できます。
- **no udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドの後に **udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドを実行すると、ディセーブル化されたポートが再びイネーブルになります。

- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port** [**aggressive**] インターフェイス コンフィギュレーション コマンドを実行すると、ディセーブル化された光ファイバ ポートが再びイネーブルになります。
- **errdisable recovery cause udld** グローバル コンフィギュレーション コマンドを入力すると、UDLD の errdisable ステートから自動回復するタイマーをイネーブルにできます。さらに、**errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンドを入力すると、UDLD の errdisable ステートから回復する時間を指定できます。

関連トピック

UDLD のグローバルなイネーブル化（CLI） （143 ページ）
インターフェイスでの UDLD のイネーブル化（CLI） （145 ページ）

UDLD のデフォルト設定

表 *15 : UDLD* のデフォルト設定

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

関連トピック

UDLD のグローバルなイネーブル化（CLI） （143 ページ）
インターフェイスでの UDLD のイネーブル化（CLI） （145 ページ）

UDLD の設定方法

UDLD のグローバルなイネーブル化（CLI）

アグレッシブ モードまたは通常モードで UDLD をイネーブルにし、デバイス上のすべての光ファイバ ポートに設定可能なメッセージ タイマーを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**udld** {**aggressive** | **enable** | **message time** *message-timer-interval*} 例： `Device(config)# udld enable message time 10`	UDLD モードの動作を指定します。 • **aggressive**：すべての光ファイバ ポートにおいて、アグレッシブ モードでUDLDをイネーブルにします。 • **enable**：デバイス上のすべての光ファイバ ポート上で、UDLD を通常モードでイネーブルにします。UDLDはデフォルトでディセーブルです。 個々のインターフェイスの設定は、**udld enable** グローバル コンフィギュレーション コマンドの設定を上書きします。 • **message time** *message-timer-interval*：アドバタイズメント フェーズにあり、双方向リンクが検出されたポートでの UDLD プローブ メッセージの時間間隔を設定します。有効な範囲は 1 ～ 90 秒です。デフォルト値は 15 です。 （注） このコマンドが作用するのは、光ファイバ ポートだけです。他のポート タイプで UDLD をイネーブルにする場合は、**udld** インターフェイス コンフィギュレーション コマンドを使用します。 UDLD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	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	

関連トピック

UDLD のモニタおよびメンテナンス
Aggressive Mode （141 ページ）
通常モード （140 ページ）
単一方向リンクの検出方法 （141 ページ）
イベントドリブン検出およびエコー （142 ページ）
UDLD リセット オプション （142 ページ）
UDLD のデフォルト設定 （143 ページ）

インターフェイスでの UDLD のイネーブル化（CLI）

アグレッシブ モードまたは通常モードをイネーブルにする、またはポート上で UDLD をディセーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	UDLD 用にイネーブルにするポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**udld port** [**aggressive**] 例： `Device(config-if)# udld port aggressive`	UDLD はデフォルトでディセーブルです。 • **udld port**：指定されたポート上で、UDLD を通常モードでイネーブルにします。 • **udld port aggressive**：（任意）指定されたインターフェイスにおいて、アグレッシブ モードで UDLD をイネーブルにします。

	コマンドまたはアクション	目的
		（注） 特定の光ファイバ ポート上で UDLD をディセーブルにする場合は、 **no udld port** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

関連トピック

UDLD のモニタおよびメンテナンス
Aggressive Mode （141 ページ）
通常モード （140 ページ）
単一方向リンクの検出方法 （141 ページ）
イベントドリブン検出およびエコー （142 ページ）
UDLD リセット オプション （142 ページ）
UDLD のデフォルト設定 （143 ページ）

UDLD のモニタおよびメンテナンス

コマンド（Command）	目的
show udld [*interface-id* | **neighbors**]	指定されたポートまたはすべてのポートの UDLD ステータスを表示します。

UDLD の追加リファレンス

関連資料

関連項目	参照先
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9500 Series Switches)* の「Layer 2/3 Commands」の項を参照してください

標準および RFC

標準/RFC	役職（Title）
なし	—

MIB

MIB	MIB リンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

UDLD の機能情報

リリース	変更箇所
Cisco IOS XE Everest 16.5.1a	この機能が導入されました。