



Cisco NX-OS を使用した STP 拡張の設定

- STP 拡張機能について, on page 1
- STP 拡張機能の前提条件, on page 8
- STP 拡張機能の設定に関するガイドラインおよび制約事項, on page 8
- STP 拡張機能のデフォルト設定, on page 10
- STP 拡張機能の設定手順, on page 10
- STP 拡張機能の設定の確認, on page 31
- STP 拡張機能の設定例, on page 31
- STP 拡張機能の追加情報 (CLI バージョン) , on page 32

STP 拡張機能について



Note レイヤ 2 インターフェイスの作成の詳細については、『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』を参照してください。

ループ回避を改善し、ユーザによる設定ミスを削減し、プロトコルパラメータの制御を向上するために、シスコは STP に拡張機能を追加しました。IEEE 802.1w 高速スパンニングツリープロトコル (RSTP) 規格に同様の機能が統合されていることも考えられますが、ここで紹介する拡張機能を使用することを推奨します。PVST シミュレーションを除き、これらの拡張機能はすべて、Rapid PVST+ および MST の両方で使用できます。PVST シミュレーションを使用できるのは、MST だけです。

使用できる拡張機能は、スパンニングツリー エッジポート (従来の PortFast の機能を提供)、ブリッジ保証、BPDU ガード、BPDU フィルタリング、ループ ガード、ルート ガード、および PVT シミュレーションです。これらの機能の大部分は、グローバルに、または指定インターフェイスに適用できます。



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

STP ポート タイプ

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

レイヤ 2 ホストに接続するエッジポートは、アクセスポートまたはトランクポートのどちらかになります。



Note レイヤ 2 スイッチまたはブリッジに接続しているポートをエッジポートとして設定すると、ブリッジングループが発生することがあります。

ネットワークポートは、レイヤ 2 スイッチまたはブリッジだけに接続します。



Note レイヤ 2 ホストまたはエッジデバイスに接続されたポートを、誤ってスパニングツリー ネットワークポートとして設定した場合、これらのポートは自動的にブロッキングステートに移行します。

STP エッジポート

STP エッジポートは、レイヤ 2 ホストだけに接続します。エッジポートインターフェイスは、ブロッキングステートやラーニングステートを経由することなく、フォワーディングステートに直接移行します（この直接移行動作は、以前は、シスコ独自の機能 **PortFast** として設定していました）。

レイヤ 2 ホストに接続したインターフェイスでは、STP の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します。

Bridge Assurance

Bridge Assurance を使用すると、ネットワーク内でブリッジングループの原因となる問題の発生を防ぐことができます。具体的には、Bridge Assurance を使用して、単方向リンク障害または他のソフトウェア障害、およびスパニングツリーアルゴリズムの停止後もデータトラフィックを転送し続けているデバイスから、ネットワークを保護します。



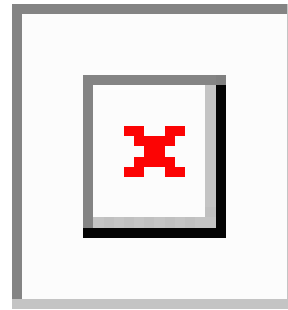
Note Bridge Assurance は、Rapid PVST+ および MST だけでサポートされています。
Bridge Assurance は通常リンクでの作動に 2 秒、VPC ピアリンクでは 84 秒以下かかります。

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

リンクの両端でイネーブルにする必要があります。リンクの一端のデバイスで Bridge Assurance がイネーブルであっても、他端のデバイスが Bridge Assurance をサポートしていない、または Bridge Assurance がイネーブルではない場合、接続ポートはブロックされます。

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

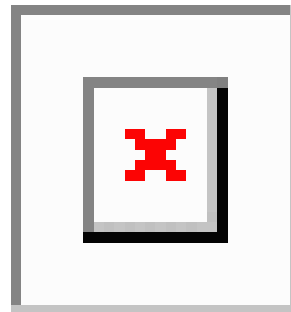
Figure 1: 標準的な STP トポロジのネットワーク



次の図は、標準的な STP トポロジを示しています。

Figure 2: Bridge Assurance を実行していないネットワークの問題

次の図は、Bridge Assurance を実行していない場合、デバイスの障害発生時にネットワークで



発生する可能性のある問題を示しています。

Figure 3: Bridge Assurance を実行しているネットワークの STP トポロジ

次の図は、Bridge Assurance がイネーブルになっているネットワークで、すべての STP ネットワーク ポートから双方向 BPDU が発行される一般的な STP トポロジを示しています。

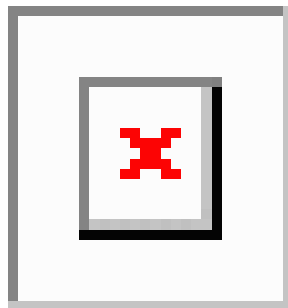
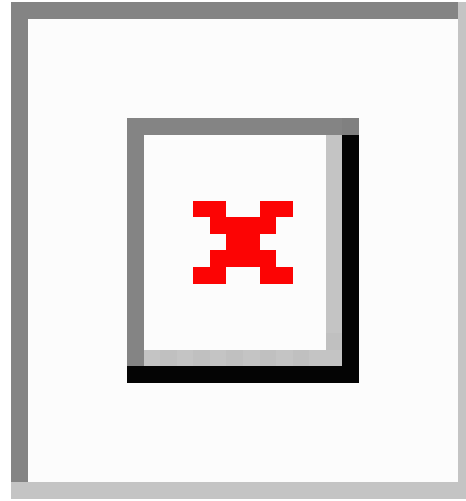


Figure 4: Bridge Assurance によるネットワーク上の問題の回避

次の図は、ネットワーク上で Bridge Assurance をイネーブルにした場合に、ネットワーク上の



問題が発生しない理由を示しています。

BPDU ガード

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

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

BPDU ガードをグローバル単位で設定すると、動作中のスパニングツリー エッジ ポート上だけで有効となります。有効な設定では、レイヤ 2 LAN エッジ インターフェイスは BPDU を受信しません。レイヤ 2 LAN エッジ インターフェイスが BPDU を受信した場合、許可されていないデバイスの接続と同様に、無効な設定として通知されます。BPDU ガードをグローバル単位でイネーブルにすると、BPDU を受信したすべてのスパニングツリーエッジポートがシャットダウンされます。

BPDU ガードでは、無効な設定が通知された場合、レイヤ 2 LAN インターフェイスを手動で再起動させる必要があるため、無効な設定に対して安全に対応できます。



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

BPDU フィルタリング

BPDU フィルタリングを使用すると、デバイスの特定のポート上で BPDU が送信されないように、または BPDU を受信しないように設定できます。

グローバルに設定された BPDU フィルタリングは、動作中のすべてのスパニングツリー エッジポートに適用されます。エッジポートはホストだけに接続してください。ホストでは通常、BPDU は破棄されます。動作中のスパニングツリー エッジポートが BPDU を受信すると、ただちに標準のスパニングツリー ポート タイプに戻り、通常のポート状態遷移が行われます。その場合、当該ポートで BPDU フィルタリングはディセーブルとなり、スパニングツリーによって、同ポートでの BPDU の送信が再開されます。

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


Caution

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

次の表に、すべての BPDU フィルタリングの組み合わせを示します。

Table 1: BPDU フィルタリングの設定

ポート単位の BPDU フィルタリングの設定	グローバルな BPDU フィルタリングの設定	STP エッジ ポート 設定	BPDU フィルタリングの状態
デフォルト ¹	有効	有効	イネーブル ²
デフォルト	有効	無効	無効
デフォルト	無効	N/A	無効
無効	N/A	N/A	無効
有効	N/A	N/A	有効

¹ 明示的なポート設定はありません。

² ポートは最低 10 個の BPDU を送信します。このポートは、BPDU を受信すると、スパニングツリー標準ポート状態に戻り、BPDU フィルタリングはディセーブルになります。

ループ ガード

ループ ガードを使用すると、ポイントツーポイント リンク上の単方向リンク障害によって発生することがあるブリッジンググループを防止できます。

STPループは、冗長なトポロジにおいてブロッキングポートが誤ってフォワーディングステートに移行すると発生します。通常、BPDUの受信を停止する、物理的に冗長なトポロジ内のポート（ブロッキングポートとは限らない）が原因で移行が発生します。

ループガードをグローバルにイネーブルにしても、デバイスがポイントツーポイントリンクで接続されているスイッチドネットワークでしか使用できません。ポイントツーポイントリンクでは、下位BPDUを送信するか、リンクをダウンしない限り、代表ブリッジは消えることはありません。ただし、共有リンク上のループガードはインターフェイス単位でイネーブルに設定できます。

ループガードを使用して、ルートポートまたは代替/バックアップループポートがBPDUを受信するかどうかを確認できます。BPDUを受信していたポートでBPDUを受信されなくなると、ループガードは、ポート上でBPDUの受信が再開されるまで、そのポートを不整合（ブロッキング）ステートにします。これらのポートでBPDUの受信が再開されると、ポートおよびリンクは再び動作可能として認識されます。この回復は自動的に実行されるので、プロトコルによりポートからループ不整合が排除されると、STPによりポートステートが判別されます。

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

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

ルートデバイス上でループガードをイネーブルにしても効果はありませんが、ルートデバイスが非ルートデバイスになった場合、保護が有効になります。

ループ ガード

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

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属しているすべてのVLANにルートガードが適用されます。

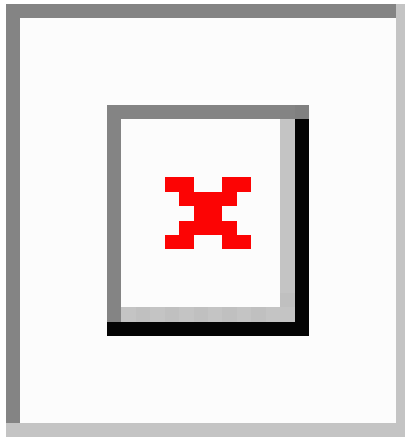
ルートガードを使用すると、ネットワーク内にルートブリッジを強制的に配置できます。ルートガードは、ルートガードがイネーブルにされたポートを指定ポートに選出します。通常、ルートブリッジのポートはすべて指定ポートとなります（ただし、ルートブリッジの2つ以上のポートが接続されている場合はその限りではありません）。ルートブリッジは、ルートガードがイネーブルにされたポートで上位BPDUを受信すると、そのポートをルート不整合STP状態に移行します。このように、ルートガードはルートブリッジの配置を適用します。

ルートガードをグローバルには設定できません。

STP 拡張機能の適用

Figure 5: STP 拡張機能を適正に展開したネットワーク

この図に示すように、ネットワーク上に各種の STP 拡張機能を設定することを推奨します。Bridge Assurance は、ネットワーク全体でイネーブルになります。ホスト インターフェイス上で、BPDU ガードと BPDU フィルタリングのいずれかをイネーブルにすることをお勧めします。



PVST シミュレーション

MST は、ユーザが設定しなくても、Rapid PVST+ と相互運用できます。この相互運用性を提供するものが、PVST シミュレーション機能です。



Note MST をイネーブルにすると、PVST シミュレーションがデフォルトでイネーブルになります。デフォルトでは、デバイス上のすべてのインターフェイスで MST と Rapid PVST+ が相互運用されます。

ただし、MST イネーブル ポートが Rapid PVST+ イネーブル ポートに接続される可能性を防ぐには、MST と Rapid PVST+ 間の接続を制御する必要があります。Rapid PVST+ はデフォルトの STP モードなので、多数の Rapid PVST+ 接続が発生することがあります。

Rapid PVST+ シミュレーションを、ポート単位でディセーブルにするか、デバイス全体でグローバルにディセーブルにすると、MST イネーブル ポートは、Rapid PVST+ イネーブル ポートに接続したことが検出された時点で、ブロッキングステートに移行します。このポートは、Rapid PVST+/SSTP BPDU の受信が停止されるまで不整合のステートのままになります。そしてポートは、通常の STP 送信プロセスに戻ります。

すべての STP インスタンスのルートブリッジは、MST または Rapid PVST+ のどちらかの側に属している必要があります。すべての STP インスタンスのルートブリッジがどちらか一方の側に属していないと、ポートは PVST シミュレーション不整合ステートになります。



Note すべての STP インスタンスのルートブリッジを、MST 側に配置することを推奨します。

STP のハイ アベイラビリティ

ソフトウェアは STP に対してハイ アベイラビリティをサポートしています。ただし、STP を再起動した場合、統計情報およびタイマーは復元されません。タイマーは最初から開始され、統計情報は 0 にリセットされます。



Note ハイ アベイラビリティ機能、の詳細については、『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

STP 拡張機能の前提条件

STP には次の前提条件があります。

- デバイスにログインしていること。
- STP を設定しておく必要があります。

STP 拡張機能の設定に関するガイドラインおよび制約事項

STP 拡張機能の設定に関するガイドラインと制約事項は次のとおりです。

- **show** コマンド (**internal** キーワード付き) はサポートされていません。
- STP ネットワーク ポートは、スイッチだけに接続してください。
- ホスト ポートは、ネットワーク ポートではなく STP エッジ ポートとして設定する必要があります。
- STP ネットワーク ポート タイプをグローバルにイネーブルにする場合には、ホストに接続しているすべてのポートを手動で STP エッジ ポートとして設定してください。
- レイヤ 2 ホストに接続しているすべてのアクセス ポートおよびトランク ポートを、エッジ ポートとして設定する必要があります。
- Bridge Assurance は、ポイントツーポイントのスパニングツリー ネットワーク ポート上だけで実行されます。この機能は、リンクの両端で設定する必要があります。
- Bridge Assurance は、ネットワーク全体でイネーブルにすることを推奨します。

- すべてのエッジポートで BPDU ガードをイネーブルにすることを推奨します。
- グローバルにイネーブルにしたループ ガードは、ポイントツーポイント リンク上でのみ動作します。
- インターフェイス単位でイネーブルにしたループ ガードは、共有リンクおよびポイントツーポイント リンクの両方で動作します。
- ルート ガードを適用したポートは強制的に指定ポートになりますが、ルート ポートにはなりません。ループ ガードは、ポートがルート ポートまたは代替ポートの場合にのみ有効です。ポート上でループ 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。
- ディセーブル化されたスパニングツリー インスタンスまたは VLAN 上では、ループ ガードは無効です。
- スパニングツリーは、BPDUを送信するチャンネル内で最初に動作するポートを常に選択します。このリンクが単方向になると、チャンネル内の他のリンクが正常に動作していても、ループ ガードによりチャンネルがブロックされます。
- ループガードによってブロックされている一連のポートをグループ化してチャンネルを形成すると、これらのポートのステート情報はスパニングツリーからすべて削除され、新しいチャンネルのポートは指定ロールによりフォワーディング ステートに移行できます。
- チャンネルがループガードによりブロックされ、チャンネルのメンバーが個々のリンク ステータスに戻ると、スパニングツリーからすべてのステート情報が削除されます。チャンネルを形成する1つまたは複数のリンクが単方向リンクである場合も、各物理ポートは指定されたロールを使用して、フォワーディング ステートに移行できます。

**Note**

単方向リンク検出 (UDLD) アグレッシブ モードをイネーブルにすると、リンク障害を分離できます。UDLD により障害が検出されるまではループが発生することがありますが、ループガードでは検出できません。UDLD の詳細については、『Cisco NX-OS シリーズ NX-OS インターフェイス構成ガイド』を参照してください。

- 物理ループのあるスイッチ ネットワーク上では、ループ ガードをグローバルにイネーブルにする必要があります。
- 直接の管理制御下でないネットワークデバイスに接続しているポート上では、ルート ガードをイネーブルにする必要があります。
- 最大 MAC 学習制限を超えると、すべての着信パケットは MAC テーブルで学習されず、宛先 MAC に基づいて転送されます。
- Cisco NX-OS リリース 10.2 (2) F以降、STP は Cisco Nexus 93C64E-SG2-Q スイッチでサポートされています。

STP 拡張機能のデフォルト設定

次の表に、STP 拡張機能のデフォルト設定を示します。

Table 2. STP 拡張機能パラメータのデフォルト設定

パラメータ	デフォルト
ポート タイプ	標準
Bridge Assurance	イネーブル (STP ネットワーク ポートのみ)
グローバル BPDU ガード	ディセーブル
インターフェイス単位の BPDU ガード	ディセーブル
グローバル BPDU フィルタリング	ディセーブル
インターフェイス単位の BPDU フィルタリング	ディセーブル
グローバル ループ ガード	ディセーブル
インターフェイス単位のループ ガード	ディセーブル
インターフェイス単位のルート ガード	ディセーブル
PVST シミュレーション	有効 (Enabled)

STP 拡張機能の設定手順



Note Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

ループ ガードは、共有リンクまたはポイントツーポイント リンク上のインターフェイス単位でイネーブルに設定できます。

スパンニングツリー ポート タイプのグローバルな設定

スパンニングツリー ポート タイプの指定は、次のように、ポートの接続先デバイスによって異なります。

- エッジ：エッジポートは、レイヤ 2 ホストに接続するアクセス ポートです。

- ネットワーク：ネットワークポートは、レイヤ2スイッチまたはブリッジだけに接続し、アクセスポートまたはトランクポートのいずれかになります。
- 標準：標準ポートはエッジポートでもネットワークポートでもない、標準のスパニングツリーポートです。これらのポートは、どのデバイスにも接続できます。

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

Before you begin

スパニングツリーポートタイプを設定する前に、次の点を確認してください。

- STP が設定されていること。
- ポートの接続先デバイスに応じて、ポートを正しく設定していること。

SUMMARY STEPS

1. **config t**
2. **spanning-tree port type edge default** または **spanning-tree port type network default**
3. **exit**
4. (Optional) **show spanning-tree summary**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	config t Example: <pre>switch# config t switch(config)#</pre>	コンフィギュレーションモードに入ります。
ステップ 2	spanning-tree port type edge default または spanning-tree port type network default Example: <pre>switch(config)# spanning-tree port type edge default</pre>	<ul style="list-style-type: none"> • spanning-tree port type edge default レイヤ2ホストに接続しているすべてのアクセスポートをエッジポートとして設定します。エッジポートは、リンクアップすると、ブロッキングステートやラーニングステートを経由することなく、フォワーディングステートに直接移行します。デフォルトのスパニングツリーポートタイプは「標準」です。 • spanning-tree port type network default レイヤ2スイッチおよびブリッジに接続しているすべてのインターフェイスを、スパニングツ

	Command or Action	Purpose
		<p>リー ネットワーク ポートとして設定します。Bridge Assurance をイネーブルにすると、各ネットワーク ポート上で Bridge Assurance が自動的に実行されます。デフォルトのスパニングツリー ポート タイプは「標準」です。</p> <p>Note レイヤ2ホストに接続しているインターフェイスをネットワーク ポートとして設定すると、これらのポートは自動的にブロッキングステートに移行します。</p>
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) show spanning-tree summary Example: <pre>switch# show spanning-tree summary</pre>	設定した STP ポート タイプを含む STP コンフィギュレーションを表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

Example

次に、レイヤ 2 ホストに接続しているすべてのアクセス ポートをスパニングツリー エッジ ポートとして設定する例を示します。

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

次に、レイヤ 2 スイッチまたはブリッジに接続しているすべてのポートを、スパニングツリー ネットワーク ポートとして設定する例を示します。

```
switch# config t
switch(config)# spanning-tree port type network default
switch(config)# exit
switch#
```

指定インターフェイスでのスパニングツリー エッジ ポートの設定

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

このコマンドには次の 4 つの状態があります。

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

**Note**

spanning-tree port type edge trunk 構成が適用され、ポートでBPDUが受信されると、PortFast機能は無効になります。その結果、ポートはエッジポートとして機能しません。

**Note**

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

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

Before you begin

スパニングツリー ポート タイプを設定する前に、次の点を確認してください。

- STP が設定されていること。
- ポートの接続先デバイスに応じて、ポートを正しく設定していること。

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree port type edge**
4. **exit**

5. (Optional) **show spanning-tree interface** *type slot/port ethernet x/y*
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	config t Example: switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	interface <i>type slot/port</i> Example: switch(config)# interface ethernet 1/4 switch(config-if)#	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 3	spanning-tree port type edge Example: switch(config-if)# spanning-tree port type edge	指定したアクセス インターフェイスをスパニング エッジ ポートに設定します。エッジ ポートは、リンク アップすると、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。デフォルトのスパニングツリー ポート タイプは「標準」です。
ステップ 4	exit Example: switch(config-if)# exit switch(config)#	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	(Optional) show spanning-tree interface <i>type slot/port ethernet x/y</i> Example: switch# show spanning-tree ethernet 1/4	設定した STP ポート タイプを含む STP コンフィギュレーションを表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、アクセス インターフェイス Ethernet 1/4 をスパニングツリー エッジ ポートとして設定する例を示します。

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

```
switch(config-if)# exit  
switch(config)#
```

指定インターフェイスでのスパニングツリー ネットワーク ポートの設定

指定インターフェイスにスパニングツリー ネットワーク ポートを設定できます。

Bridge Assurance は、スパニングツリー ネットワーク ポート上だけで実行されます。

このコマンドには次の 3 つの状態があります。

- **spanning-tree port type network** : このコマンドはネットワーク ポートとしてポートを明示的に設定します。Bridge Assurance をグローバルにイネーブルにすると、スパニングツリー ネットワーク ポート上で Bridge Assurance が自動的に実行されます。
- **spanning-tree port type normal** : このコマンドは、ポートを標準スパニングツリー ポートとして明示的に設定しますが、Bridge Assurance はこのインターフェイスで実行できません。
- **no spanning-tree port type** : このコマンドは、**spanning-tree port type network default** を定義した場合に、ポートを暗黙的にスパニングツリー ネットワーク ポートとしてイネーブルにします。コマンドを使用します。Bridge Assurance をイネーブルにすると、このポート上で Bridge Assurance が自動的に実行されます。



Note

レイヤ 2 ホストに接続しているポートをネットワーク ポートとして設定すると、自動的にブロッキング ステートに移行します。

Before you begin

スパニングツリー ポート タイプを設定する前に、次の点を確認してください。

- STP が設定されていること。
- ポートの接続先デバイスに応じて、ポートを正しく設定していること。

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree port type network**
4. **exit**
5. (Optional) **show spanning-tree interface** *type slot/port*
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	config t Example: switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	interface type slot/port Example: switch(config)# interface ethernet 1/4 switch(config-if)#	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree port type network Example: switch(config-if)# spanning-tree port type network	指定したインターフェイスをスパニング ネットワーク ポートに設定します。Bridge Assurance をイネーブルにすると、各ネットワーク ポート上で Bridge Assurance が自動的に実行されます。デフォルトのスパニングツリー ポート タイプは「標準」です。
ステップ 4	exit Example: switch(config-if)# exit switch(config)#	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	(Optional) show spanning-tree interface type slot/port Example: switch# show spanning-tree interface ethernet 1/4	設定した STP ポート タイプを含む STP コンフィギュレーションを表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、Ethernet インターフェイス 1/4 をスパニングツリー ネットワーク ポートとして設定する例を示します。

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


BPDU ガードのグローバルなイネーブル化

BPDU ガードをデフォルトでグローバルにイネーブルにできます。BPDU ガードがグローバルにイネーブルにされると、システムは、BPDU を受信したエッジポートをシャットダウンします。



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

Before you begin

スパニングツリーポートタイプを設定する前に、次の点を確認してください。

- STP が設定されていること。
- ポートの接続先デバイスに応じて、ポートを正しく設定していること。

SUMMARY STEPS

1. **config t**
2. **spanning-tree port type edge bpduguard default**
3. **exit**
4. (Optional) **show spanning-tree summary**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure		
	Command or Action	Purpose
ステップ 1	config t Example: <pre>switch# config t switch(config)#</pre>	コンフィギュレーションモードに入ります。
ステップ 2	spanning-tree port type edge bpduguard default Example: <pre>switch(config)# spanning-tree port type edge bpduguard default</pre>	すべてのスパニングツリーエッジポートで、BPDU ガードを、デフォルトでイネーブルにします。デフォルトでは、グローバルな BPDU ガードはディセーブルです。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	コンフィギュレーションモードを終了します。

	Command or Action	Purpose
ステップ 4	(Optional) show spanning-tree summary Example: switch# show spanning-tree summary	STP の概要を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

Example

次に、すべてのスパンニングツリー エッジ ポートで BPDU ガードをイネーブルにする例を示します。

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

指定インターフェイスでの BPDU ガードのイネーブル化

指定インターフェイスで、BPDU ガードをイネーブルにできます。BPDU ガードがイネーブルにされたポートは、BPDU を受信すると、シャットダウンされます。

BPDU ガードは、指定インターフェイスで次のように設定にできます。

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

Before you begin

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。

SUMMARY STEPS

1. **config t**
2. **interface type slot/port**
3. **spanning-tree bpduguard {enable | disable} or no spanning-tree bpduguard**

4. **exit**
5. (Optional) **show spanning-tree interface type slot/port detail**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	config t Example: <pre>switch# config t switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	interface type slot/port Example: <pre>switch(config)# interface ethernet 1/4 switch(config-if)#</pre>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree bpduguard {enable disable} or no spanning-tree bpduguard Example: <pre>switch(config-if)# spanning-tree bpduguard enable</pre>	<ul style="list-style-type: none"> • spanning-tree bpduguard {enable disable} 指定したスパンニングツリーエッジインターフェイスの BPDU ガードをイネーブルまたはディセーブルにします。デフォルトでは、インターフェイス上の BPDU ガードはディセーブルです。 • no spanning-tree bpduguard spanning-tree port type edge bpduguard default コマンドの入力により、インターフェイスに設定されたデフォルトのグローバル BPDU ガード設定に戻します。
ステップ 4	exit Example: <pre>switch(config-if)# exit switch(config)#</pre>	インターフェイス モードを終了します。
ステップ 5	(Optional) show spanning-tree interface type slot/port detail Example: <pre>switch# show spanning-tree interface ethernet detail</pre>	STP の概要を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

Example

次に、エッジポート Ethernet 1/4 で BPDU ガードを明示的にイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpduguard enable
switch(config-if)# exit
switch(config)#
```

BPDU フィルタリングのグローバルなイネーブル化

スパニングツリーエッジポートで、BPDU フィルタリングをデフォルトでグローバルにイネーブルにできます。

BPDU フィルタリングがイネーブルであるエッジポートは、BPDU を受信するとエッジポートとしての稼働ステータスが失われ、通常の STP ステート移行を再開します。ただし、このポートは、エッジポートとしての設定は保持したままです。

**Caution**

このコマンドを使用するときは注意してください。このコマンドを誤って使用すると、ブリッジンググループに陥る可能性があります。

Before you begin

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。
- 少なくとも一部のスパニングツリー エッジポートが設定済みであること。

**Note**

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

SUMMARY STEPS

1. **config t**
2. **spanning-tree port type edge bpduguard default**
3. **exit**
4. (Optional) **show spanning-tree summary**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure		
	Command or Action	Purpose
ステップ 1	config t Example: switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	spanning-tree port type edge bpdupfilter default Example: switch(config)# spanning-tree port type edge bpdupfilter default	すべてのスパニングツリーエッジポートで、BPDU フィルタリングを、デフォルトでイネーブルにします。デフォルトでは、グローバルな BPDU フィルタリングはディセーブルです。
ステップ 3	exit Example: switch(config)# exit switch#	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) show spanning-tree summary Example: switch# show spanning-tree summary	STP の概要を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

Example

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

```
switch# config t
switch(config)# spanning-tree port type edge bpdupfilter default
switch(config)# exit
switch#
```

指定インターフェイスでの BPDU フィルタリングのイネーブル化

指定インターフェイスに BPDU フィルタリングを適用できます。BPDU フィルタリングを特定のインターフェイス上でイネーブルにすると、そのインターフェイスは BPDU を送信しなくなり、受信した BPDU をすべてドロップするようになります。この BPDU フィルタリング機能は、トランキングインターフェイスであるかどうかに関係なく、すべてのインターフェイスに適用されます。

**Caution**

spanning-tree bpdupfilter enable を入力する場合は、慎重に行ってください。指定されたインターフェイスでコマンドを入力します。ホストに接続していないポートに BPDU フィルタリングを設定すると、そのポートは受信した BPDU をすべて無視してフォワーディングに移行するので、ブリッジングループが発生することがあります。

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

このコマンドには次の 3 つの状態があります。

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

Before you begin

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。

**Note**

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

SUMMARY STEPS

1. **config t**
2. **interface type slot/port**
3. **{ } または spanning-tree bpdupfilter enable disable no spanning-tree bpdupfilter**
4. **exit**
5. (Optional) **show spanning-tree summary**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	config t Example: switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	interface type slot/port Example: switch(config)# interface ethernet 1/4 switch(config-if)#	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 3	{{}} または spanning-tree bpdupfilter enable disable no spanning-tree bpdupfilter Example: switch(config-if)# spanning-tree bpdupfilter enable	<ul style="list-style-type: none"> • spanning-tree bpdupfilter {enable disable} 指定したスパニングツリーエッジインターフェイスの BPDU フィルタリングをイネーブルまたはディセーブルにします。デフォルトでは、BPDU フィルタリングはディセーブルです。 • no spanning-tree bpdupfilter 動作中のスパニングツリー エッジ ポート インターフェイスに spanning-tree port type edge bpdupfilter default コマンドが設定されている場合、そのインターフェイスで BPDU フィルタリングをイネーブルにします。
ステップ 4	exit Example: switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 5	(Optional) show spanning-tree summary Example: switch# show spanning-tree summary	STP の概要を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

Example

次に、スパニングツリーエッジポート Ethernet 1/4 で BPDU フィルタリングを明示的にイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpduguard enable
switch(config-if)# exit
switch(config)#
```

ループ ガードのグローバルなイネーブル化

ループガードは、デフォルトの設定により、すべてのポイントツーポイントスパニングツリーの標準およびネットワークポートで、グローバルにイネーブルにできます。ループガードは、エッジポートでは動作しません。

ループガードを使用すると、ブリッジネットワークのセキュリティを高めることができます。ループガードは、単方向リンクを引き起こす可能性のある障害が原因で、代替ポートまたはルートポートが指定ポートになるのを防ぎます。



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

Before you begin

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。
- スパニングツリー標準ポートが存在し、少なくとも一部のネットワークポートが設定済みであること。

SUMMARY STEPS

1. **config t**
2. **spanning-tree loopguard default**
3. **exit**
4. (Optional) **show spanning-tree summary**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	config t Example: <pre>switch# config t switch(config)#</pre>	コンフィギュレーション モードに入ります。

	Command or Action	Purpose
ステップ 2	spanning-tree loopguard default Example: <pre>switch(config)# spanning-tree loopguard default</pre>	スパニングツリーのすべての標準およびネットワークポートで、ループガードを、デフォルトでイネーブルにします。デフォルトでは、グローバルなループガードはディセーブルです。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	コンフィギュレーションモードを終了します。
ステップ 4	(Optional) show spanning-tree summary Example: <pre>switch# show spanning-tree summary</pre>	STP の概要を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

Example

次に、スパニングツリーのすべての標準およびネットワークポートでループガードをイネーブルにする例を示します。

```
switch# config t
switch(config)# spanning-tree loopguard default
switch(config)# exit
switch#
```

指定インターフェイスでのループガードまたはルートガードのイネーブル化



Note ループガードは、スパニングツリーの標準またはネットワークポート上で実行できます。ルートガードは、すべてのスパニングツリーポート（標準、エッジ、ネットワーク）上で実行できます。

ループガードまたはルートガードは、指定インターフェイスでイネーブルにできます。

ポート上でルートガードをイネーブルにすることは、そのポートをルートポートにできないことを意味します。ループガードは、単方向リンクの障害発生時に、代替ポートまたはルートポートが指定ポートになるのを防止します。

特定のインターフェイスでループガードおよびルートガードの両機能をイネーブルにすると、そのインターフェイスが属するすべての VLAN に両機能が適用されます。



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

Before you begin

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。
- ループガードが、スパニングツリーの標準またはネットワーク ポート上で設定されていること。

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. **spanning-tree guard** {loop | root | none}
4. **exit**
5. **interface** *type slot/port*
6. **spanning-tree guard** {loop | root | none}
7. **exit**
8. (Optional) **show spanning-tree interface** *type slot/port detail*
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	config t Example: <pre>switch# config t switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	interface <i>type slot/port</i> Example: <pre>switch(config)# interface ethernet 1/4 switch(config-if)#</pre>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 3	spanning-tree guard {loop root none} Example: <pre>switch(config-if)# spanning-tree guard loop</pre>	ループガードまたはルートガードを、指定インターフェイスでイネーブルまたはディセーブルにします。ルートガードはデフォルトでディセーブル、

	Command or Action	Purpose
		ループガードも指定ポートでディセーブルになります。 Note ループガードは、スパンニングツリーの標準およびネットワークインターフェイスだけで動作します。この例では、指定したインターフェイス上でループガードをイネーブルにしています。
ステップ 4	exit Example: switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 5	interface type slot/port Example: switch(config)# interface ethernet 1/10 switch(config-if)#	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 6	spanning-tree guard {loop root none} Example: switch(config-if)# spanning-tree guard root	ループガードまたはルートガードを、指定インターフェイスでイネーブルまたはディセーブルにします。ルートガードはデフォルトでディセーブル、ループガードも指定ポートでディセーブルになります。 この例では、別のインターフェイス上でルートガードをイネーブルにしています。
ステップ 7	exit Example: switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 8	(Optional) show spanning-tree interface type slot/port detail Example: switch# show spanning-tree interface ethernet 1/4 detail	STP の概要を表示します。
ステップ 9	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

Example

次に、Ethernet ポート 1/4 で、ルート ガードをイネーブルにする例を示します。

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

PVST シミュレーションのグローバル設定 (CLI バージョン)



Note PVST シミュレーションは、デフォルトでイネーブルになっています。デフォルトでは、デバイス上のすべてのインターフェイスで MST と Rapid PVST+ が相互運用されます。

MST は、Rapid PVST+ と相互運用します。ただし、デフォルトの STP モードで、MST を実行していないデバイスに接続する可能性を防ぐには、この自動機能をディセーブルに設定できます。Rapid PVST+ シミュレーションをディセーブルにした場合、MST がイネーブルなポートが Rapid PVST+ がイネーブルなポートに接続されていることが検出されると、MST がイネーブルなポートは、ブロッキングステートに移行します。このポートは、BPDU の受信が停止されるまで、一貫性のないステートのままになり、それから、ポートは、通常の STP 送信プロセスに戻ります。

この自動機能は、グローバルまたはポートごとにブロックできます。グローバルコマンドを入力し、インターフェイス コマンド モードでデバイス全体の PVST シミュレーション設定を変更できます。

SUMMARY STEPS

1. **config t**
2. **no spanning-tree mst simulate pvst global**
3. **exit**
4. (Optional) **show spanning-tree summary**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	config t Example: <pre>switch# config t switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	no spanning-tree mst simulate pvst global Example: <pre>switch(config)# no spanning-tree mst simulate pvst global</pre>	スイッチ上のすべてのインターフェイスで、Rapid PVST+ モードを実行している接続先デバイスとの自動的な相互運用をディセーブルにします。この機能はデフォルトではイネーブルです。デフォルトで

	Command or Action	Purpose
		は、デバイス上のすべてのインターフェイスが、Rapid PVST+ と MST の間で運用されます。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) show spanning-tree summary Example: <pre>switch# show spanning-tree summary</pre>	STP の詳細を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

Example

次に、Rapid PVST+ を実行している接続先デバイスとの自動的な相互運用を回避する例を示します。

```
switch# config t
switch(config)# no spanning-tree mst simulate pvst global
switch(config)# exit
switch#
```

ポートごとの PVST シミュレーションの設定



Note PVST シミュレーションは、デフォルトでイネーブルになっています。デフォルトでは、デバイス上のすべてのインターフェイスで MST と Rapid PVST+ が相互運用されます。

PVST シミュレーションを設定できるのは、デバイス上で MST を実行している場合だけです (Rapid PVST+ がデフォルトの STP モードです)。MST は、Rapid PVST+ と相互運用します。ただし、デフォルトの STP モードで、MST を実行していないデバイスに接続する可能性を防ぐには、この自動機能をディセーブルに設定できます。PVST シミュレーションをディセーブルにすると、Rapid PVST+ イネーブルポートに接続したことが検出された時点で、MST イネーブルポートはブロッキング ステートに移行します。このポートは、Rapid PVST+ BPDU を受信しなくなるまで不整合ステートのままですが、そのあとは標準 STP のステート移行を再開します。

この自動機能は、グローバルまたはポートごとにブロックできます。

SUMMARY STEPS

1. **config t**
2. **interface** *{{type slot/port}}* | **port-channel** *number*}}
3. **spanning-tree mst simulate pvst disable** または **spanning-tree mst simulate pvst** または **no spanning-tree mst simulate pvst**
4. **exit**
5. (Optional) **show spanning-tree interface** *type slot/port detail*
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	config t Example: <pre>switch# config t switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	interface <i>{{type slot/port}}</i> port-channel <i>number</i> }}	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 3	spanning-tree mst simulate pvst disable または spanning-tree mst simulate pvst または no spanning-tree mst simulate pvst Example: <pre>switch(config-if)# spanning-tree mst simulate pvst</pre>	<ul style="list-style-type: none"> • spanning-tree mst simulate pvst disable 指定したインターフェイスで、Rapid PVST+ モードを実行している接続先デバイスとの自動的な相互運用をディセーブルにします。 デフォルトでは、デバイス上のすべてのインターフェイスで Rapid PVST+ と MST が相互運用されます。 • spanning-tree mst simulate pvst 指定したインターフェイスで、MST と Rapid PVST+ のシームレスな相互運用を再びイネーブルにします。 • no spanning-tree mst simulate pvst インターフェイスを、spanning-tree mst simulate pvst global コマンドを使用して設定したデバイス全体で MST と Rapid PVST+ との間で相互動作するよう設定します。

	Command or Action	Purpose
ステップ 4	exit Example: <pre>switch(config-if) # exit switch(config) #</pre>	インターフェイス モードを終了します。
ステップ 5	(Optional) show spanning-tree interface type slot/port detail Example: <pre>switch# show spanning-tree interface ethernet 3/1 detail</pre>	STP の詳細を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch(config) # copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

Example

次に、指定したインターフェイスで、MSTを実行していない接続先デバイスとの自動的な相互運用を回避する例を示します。

```
switch(config-if) # spanning-tree mst simulate pvst
switch(config-if) #
```

STP 拡張機能の設定の確認

STP 拡張機能の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config spanning-tree [all]	STP に関する情報を表示します。
show spanning-tree summary	STP 情報の要約を表示します。
show spanning-tree mstinstance-id interface {ethernet slot/port port-channel channel-number} [detail]	指定したインターフェイスおよびインスタンスの MST 情報を表示します。

STP 拡張機能の設定例

次に、STP 拡張機能を設定する例を示します。

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

```

switch(config)# interface ethernet 1/1
switch(config-if)# spanning-tree port type edge
switch(config-if)# exit

switch(config)# interface ethernet 1/2
switch(config-if)# spanning-tree port type edge
switch(config-if)# exit
switch(config)#

```

STP 拡張機能の追加情報 (CLI バージョン)

関連資料

関連項目	マニュアル タイトル
レイヤ2 インターフェイス	『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』
NX-OS の基礎	『Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide』
高可用性	『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』
システム管理	『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』

標準

標準	タイトル
IEEE 802.1Q-2006 (旧称 IEEE 802.1s)、IEEE 802.1D-2004 (旧称 IEEE 802.1w)、IEEE 802.1D、IEEE 802.1t	—

MIB

MIB	MIB のリンク
<ul style="list-style-type: none"> CISCO-STP-EXTENSION-MIB BRIDGE-MIB 	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。