



STP 拡張機能の設定

- [STP 拡張機能について \(1 ページ\)](#)
- [STP 拡張機能の設定 \(6 ページ\)](#)
- [STP 拡張機能の設定の確認, on page 18](#)
- [ループ検出エラー メッセージのトラブルシューティング \(18 ページ\)](#)
- [syslog エラーメッセージの生成 \(19 ページ\)](#)

STP 拡張機能について

STP 拡張機能について

シスコでは、スパニングツリープロトコル (STP) に、収束をより効率的に行うための拡張機能を追加しました。場合によっては、同様の機能が IEEE 802.1w 高速スパニングツリープロトコル (RSTP) 標準にも組み込まれている可能性があります。シスコの拡張機能を使用することを推奨します。これらの拡張機能はすべて、RPVST+ およびマルチ スパニングツリープロトコル (MST) と組み合わせて使用できます。

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



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 ポートタイプの概要

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

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

スパニングツリーエッジポート

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

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



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

スパニングツリーネットワークポート

ネットワークポートは、スイッチまたはブリッジにだけ接続されます。**Bridge Assurance** がグローバルにイネーブルになっている間にポートをネットワークポートとして設定すると、そのポートで **Bridge Assurance** がイネーブルになります。



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

スパニングツリー標準ポート

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

デフォルトのスパニングツリーインターフェイスは標準ポートです。

Bridge Assurance の概要

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



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

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

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

BPDU ガードの概要

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

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

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



Note エッジトランク インターフェイスレベルでは、無効な VLAN のリモート側がアクセスポートとして設定されている場合、BPDU は無視されます。

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



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 フィルタリングの概要

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

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

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



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。というのは、そうしたポートは受信した BPDU をすべて無視して、フォワーディングステートに移行するからです。

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

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	有効	有効	イネーブルポートは 10 以上の BPDU を送信します。このポートは、BPDU を受信すると、スパニングツリー標準ポート状態に戻り、BPDU フィルタリングはディセーブルになります。
デフォルト	有効	無効	無効

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	無効	Enabled/Disabled	無効
無効	Enabled/Disabled	Enabled/Disabled	無効
有効	Enabled/Disabled	Enabled/Disabled	有効 Caution BPDU は送信されませんが、受信した場合には、通常の STP の動作が開始されません。BPDU の使用に当たっては、十分注意してください。

ループガードの概要

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

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

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

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



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

ループガードを使用して、ルートポートまたは代替/バックアップループポートが BPDU を受信するかどうかを確認できます。BPDU を受信しないポートを検出すると、ループガードは、そのポートを不整合状態（ブロッキングステート）に移行します。このポートは、再度

BPDUの受信を開始するまで、ブロッキング状態のままです。不整合状態のポートはBPDUを送信しません。このようなポートがBPDUを再度受信すると、ループガードはそのループ不整合状態を解除し、STPによってそのポート状態が確定されます。こうしたリカバリは自動的に行われます。

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

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。

ループガードの概要

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

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

ループ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。ループガードは、ループ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、ループ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、ループガードはルートブリッジの配置を適用します。

ループガードをグローバルには設定できません。



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

STP 拡張機能の設定

STP 拡張機能の設定における 注意事項

STP 拡張機能を設定する場合は、次の注意事項に従ってください。

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

スパニングツリーポートタイプのグローバルな設定

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

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

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

Before you begin

STP が設定されていること。

インターフェイスに接続されているデバイスのタイプに合わせてポートが正しく設定されていること。

SUMMARY STEPS

1. `switch# configure terminal`
2. `switch(config)# spanning-tree port type edge default`
3. `switch(config)# spanning-tree port type network default`

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# spanning-tree port type edge default	すべてのインターフェイスをエッジポートとして設定します。このコマンドの使用は、すべてのポートがホスト/サーバに接続されていることが前提になります。エッジポートは、リンクアップすると、ブロッキングステートやラーニングステートを經由することなく、フォワーディングステートに直接移行します。デフォルトのスパニングツリーポートタイプは「標準」です。
ステップ 3	switch(config)# spanning-tree port type network default	すべてのインターフェイスをスパニングツリーネットワークポートとして設定します。このコマンドの使用は、すべてのポートがスイッチまたはブリッジに接続されていることが前提になります。Bridge Assurance をイネーブルにすると、各ネットワークポート上で Bridge Assurance が自動的に実行されます。デフォルトのスパニングツリーポートタイプは「標準」です。 Note ホストに接続されているインターフェイスをネットワークポートとして設定すると、それらのポートは自動的にブロッキングステートに移行します。

Example

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

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

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

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


指定インターフェイスでのスパンニングツリー エッジ ポートの設定

指定インターフェイスにスパンニングツリー エッジ ポートを設定できます。スパンニングツリー 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** : このコマンドを実行すると、アクセス ポート上のエッジ動作が明示的にイネーブルにされます。
- **spanning-tree port type edge trunk** : このコマンドを実行すると、トランク ポート上のエッジ動作が明示的にイネーブルにされます。



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

- **spanning-tree port type normal** : このコマンドを実行すると、ポートは標準スパンニングツリー ポートとして明示的に設定されますが、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されません。
- **no spanning-tree port type** : このコマンドを実行すると、**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、エッジ動作が暗黙にイネーブルにされます。エッジ ポートをグローバルに設定していない場合、**no spanning-tree port type** コマンドは **spanning-tree port type disable** コマンドと同じです。

Before you begin

STP が設定されていること。

インターフェイスがホストに接続されていること。

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface type slot/port	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	Command or Action	Purpose
ステップ 3	<code>switch(config-if)# spanning-tree port type edge</code>	指定したアクセス インターフェイスをスパンニング 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。デフォルトのスパンニング ツリー ポート タイプは「標準」です。

Example

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

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

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

STP が設定されていること。

少なくとも一部のスパンニング ツリー エッジ ポートが設定済みであること。

SUMMARY STEPS

1. `switch# configure terminal`
2. `switch(config)# spanning-tree port type edge bpduguard default`

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	<code>switch# configure terminal</code>	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。

	Command or Action	Purpose
ステップ 2	<code>switch(config)# spanning-tree port type edge bpduguard default</code>	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。

Example

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

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

指定インターフェイスでの BPDU ガードのイネーブル化

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

BPDU ガードは、指定インターフェイスで次のように設定にできます。

- **spanning-tree bpduguard enable** : インターフェイスで BPDU ガードを無条件でイネーブルにします。
- **spanning-tree bpduguard disable** : インターフェイスで BPDU ガードを無条件でディセーブルにします。
- **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

STP が設定されていること。

SUMMARY STEPS

1. `switch# configure terminal`
2. `switch(config)# interface type slot/port`
3. `switch(config-if)# spanning-tree bpduguard {enable | disable}`
4. (Optional) `switch(config-if)# no spanning-tree bpduguard`

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface <i>type slot/port</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	switch(config-if)# spanning-tree bpduguard {enable disable}	指定したスパニングツリー エッジ インターフェイスの BPDU ガードをイネーブルまたはディセーブルにします。デフォルトでは、BPDU ガードは、物理イーサネットインターフェイスではディセーブルです。
ステップ 4	(Optional) switch(config-if)# no spanning-tree bpduguard	インターフェイス上で BPDU ガードをディセーブルにします。 Note 動作中のエッジ ポート インターフェイスで、 spanning-tree port type edge bpduguard default コマンドを入力した場合、そのインターフェイスで BPDU ガードをイネーブルにします。

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# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpduguard enable
switch(config-if)# no spanning-tree bpduguard
```

BPDU フィルタリングのグローバルなイネーブル化

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

BPDU フィルタリングがイネーブルにされたエッジポートは、BPDU を受信すると、エッジポートとしての動作ステータスを失い、通常の STP 状態遷移を再開します。ただし、このポートは、エッジポートとしての設定は保持したままです。

**Caution**

このコマンドを使用するときには注意してください。誤って使用すると、ブリッジンググループが発生するおそれがあります。

**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。

Before you begin

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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **spanning-tree port type edge bpdupfilter default**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# spanning-tree port type edge 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。

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# configure terminal
```

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

指定インターフェイスでの BPDU フィルタリングのイネーブル化

指定インターフェイスに BPDU フィルタリングを適用できます。BPDU フィルタリングを特定のインターフェイス上でイネーブルにすると、そのインターフェイスは BPDU を送信しなくなり、受信した BPDU をすべてドロップするようになります。この BPDU フィルタリング機能は、トランッ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

指定インターフェイスで **spanning-tree bpdudfilter enable** コマンドを入力する場合は注意してください。ホストに接続されていないポートに BPDU フィルタリングを明示的に設定すると、ブリッジンググループに陥る可能性があります。というのは、そうしたポートは受信した BPDU をすべて無視して、フォワーディング ステートに移行するからです。

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

このコマンドには次の 3 つの状態があります。

- **spanning-tree bpdudfilter enable** : インターフェイス上の BPDU フィルタリングを無条件にイネーブルにします。
- **spanning-tree bpdudfilter disable** : インターフェイス上の BPDU フィルタリングを無条件にディセーブルにします。
- **no spanning-tree bpdudfilter** : 動作中のエッジポートインターフェイスに **spanning-tree port type edge bpdudfilter 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。



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。

Before you begin

STP が設定されていること。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **spanning-tree bpdudfilter {enable | disable}**
4. (Optional) switch(config-if)# **no spanning-tree bpdudfilter**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface type slot/port	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# spanning-tree bpdudfilter {enable disable}	指定したスパニングツリー エッジ インターフェイスの BPDU フィルタリングをイネーブルまたはディセーブルにします。デフォルトでは、BPDU フィルタリングはディセーブルです。
ステップ 4	(Optional) switch(config-if)# no spanning-tree bpdudfilter	<p>インターフェイス上で BPDU フィルタリングをディセーブルにします。</p> <p>Note 動作中のエッジ ポート インターフェイスに spanning-tree port type edge bpdudfilter 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。</p>

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# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpdudfilter enable
```

ループガードのグローバルなイネーブル化

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

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



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

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. switch# **configure terminal**
2. switch(config)# **spanning-tree loopguard default**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# spanning-tree loopguard default	スパニングツリーのすべての標準およびネットワークポートで、ループガードを、デフォルトでイネーブルにします。デフォルトでは、グローバルなループガードはディセーブルです。

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# configure terminal
switch(config)# spanning-tree loopguard default
```

指定インターフェイスでのループガードまたはルートガードのイネーブル化

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

特定のポートでルートガードをイネーブルにすると、そのポートはルートポートになることを禁止されます。ループガードは、単方向リンクを発生させる可能性のある障害が原因で代替ポートまたはルートポートが指定ポートになるのを防ぎます。

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



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

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. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **spanning-tree guard {loop | root | none}**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface type slot/port	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# spanning-tree guard {loop root none}	ループガードまたはルートガードを、指定インターフェイスでイネーブルまたはディセーブルにします。ルートガードはデフォルトでディセーブル、ループガードも指定ポートでディセーブルになります。 Note ループガードは、スパニングツリーの標準およびネットワーク インターフェイスだけで動作します。

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

STP 拡張機能の設定の確認

STP 拡張機能の設定情報を表示するには、次のコマンドを使用します。

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

ループ検出エラーメッセージのトラブルシューティング

このセクションでは、Cisco Nexus 3600 プラットフォーム スイッチのログに FWM-2-STM_LOOP_DETECT のエラー メッセージがあった場合の解決方法について説明します。

Cisco Nexus 3600 プラットフォーム スイッチが次のメッセージを表示した場合、スイッチがこれら 2 つのインターフェイスで同じ送信元の MAC アドレスを持つフレームを受信し、これらのインターフェイスで同じ MAC アドレスを高速で認識することを示しています。スイッチはこの条件をループとして検出します。スイッチは、コントロールプレーンを保護するために MAC アドレス ラーニングを無効にします。これは、ループが 1 つの VLAN だけに発生した場合でも、すべての VLAN で実行されます。

```
2016 Apr 11 18:00:18 N3k-4-3229 %FWM-2-STM_LOOP_DETECT: Loops detected in the network
for mac 0000.0602.0602 among ports Eth1/48
and Eth1/50/3 on vlan 4 - Disabling dynamic learning notifications for a period between
120 and 240 seconds on vlan 4
```

エラー メッセージの考えられる原因は次のとおりです。

- 不正なスパニング ツリー プロトコル (STP) ポート ステート コンバージェンスのため、MAC アドレスが移動する。
- STP ステートがコンバージェンスされて正しい状態にあるときに、データの送信元がすべてのスイッチを物理的に横断していることが原因で、MAC アドレスが移動します。

ループの検出

フォワーディング マネージャ (FWM) には、移動した MAC アドレスをカウントし、MAC アドレスの移動回数に基づいてその重み付けをする機能があります。これにより、移動した MAC アドレスの合計 (すべての VLAN、MAC、インターフェイスでのスイッチ全体) が算出され、%FWM-2-STM_LOOP_DETECT 条件が宣言され、ループ状態の FWM を保護するためにラーニングが無効になります。



(注) MAC ラーニングは、システムごとではなく、VLAN ごとにディセーブルになります。

MAC 移動通知のロジックに注意する必要があります。MAC 移動の MAC アドレステーブルの通知が有効の場合、MAC 移動が通知される可能性があります。これによりコンソールの通知ログが追加されますが、アクションは実行されません。移動が宣言されるのは、10秒間の時系列スキャン期間内に VLAN の任意の2つのポート間で特定の MAC アドレスが3回行き来（移動）した場合です。



(注) MAC アドレスは、2つのポートのそれぞれで50回検出される必要があります。

スイッチの MAC アドレス通知を有効にすると、どの MAC アドレスが移動するかを見つけることができます。

手順の概要

1. switch# **conf t**
2. switch# **mac address-table notification mac-move**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# conf t	コンフィギュレーション モードを開始します。
ステップ 2	switch# mac address-table notification mac-move	MAC 移動通知をイネーブルにします。

syslog エラーメッセージの生成

MAC 移動通知に関する syslog メッセージを生成するために、MAC 移動通知を有効にするだけでは、必ずしも十分ではありません。syslog メッセージが確実に生成されるようにするには、前のコマンドと一緒に **mac address-table notification mac-move** というコマンドを入力します。

手順の概要

1. **conf t**
2. **logging level spanning-tree 6**
3. **logging level fwm 6**
4. **logging monitor 6**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	conf t	コンフィギュレーション モードを開始します。
ステップ 2	logging level spanning-tree 6	レベル 6 から最も重大度の高いイベントまでのすべてのスパンニングツリーイベントのログギングをイネーブルにします。
ステップ 3	logging level fwm 6	レベル 6 から最も重大度の高いイベントまでのすべての FWM イベントのログギングをイネーブルにします。
ステップ 4	logging monitor 6	デバイスが重大度 6 以上のメッセージをモニタに記録できるようにします。

これらのコマンドを追加すると、MAC アドレス移動がある場合に FWM 検出が syslog に必ず表示されます。VLAN 全体でスイッチの STP ポート ステートを検証するには、次のコマンドを入力します。

```
switch# show spanning-tree
switch# show spanning-tree vlan <id>
switch# show spanning-tree internal interaction
```

例

MAC アドレスが移動したかどうかを確認するには、次のコマンドを入力します。

```
# show mac address-table notification mac-move
MAC Move Notify Triggers: 1206
Number of MAC Addresses added: 944088
Number of MAC Addresses moved: 265
Number of MAC Addresses removed: 943920
```

どの MAC アドレスが移動したかを表示するには、MAC アドレスの移動も記録される最小ログギング レベルであるレベル 6 が必要です。

```
2016 Jun 12 16:05:31.564 switch %FWM-6-MAC_MOVE_NOTIFICATION:
Host 0000.0000.fe00 in vlan 85 is flapping between
port Eth104/1/8 and port Eth104/1/9
```

次のタスク

正しい STP コンバージェンスを確認し、関係図内のすべてのスイッチで STP ポートステートをチェックします。競合がないこと、および不適切なポートステートがないことを確認します。

物理的に移動しているデータフレームの送信元を特定したら、高速での連続的な移動を停止するために送信元を制御します。

デフォルトでは、動的なラーニングは180秒後に再度有効になります。その時点で、すべてのSTP競合または不整合は解決されている必要があります。そうでない場合、動的なラーニングは再度、無効になります。

