



STP 拡張機能の設定

この章の内容は、次のとおりです。

- [STP 拡張機能について, 1 ページ](#)
- [STP 拡張機能の設定, 7 ページ](#)
- [STP 拡張機能の設定の確認, 17 ページ](#)
- [ループ検出のエラー 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

概要

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。



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

STP 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（この直接移行動作は、以前は、シスコ独自の機能 **PortFast** として設定していました）。

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



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

スパニングツリー ネットワークポート

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



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

スパニングツリー標準ポート

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

デフォルトのスパニングツリーインターフェイスは標準ポートです。

Bridge Assurance の概要

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



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

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

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

BPDU ガードの概要

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

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

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



(注) エッジトランク インターフェイス レベルでは、無効な VLAN のリモートサイド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。



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

BPDU フィルタリングの概要

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

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

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



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

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

表 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	イネーブル	イネーブル	イネーブル。ポートは最低 10 個の BPDU を送信します。このポートは、BPDU を受信すると、スパンニングツリー標準ポート状態に戻り、BPDU フィルタリングはディセーブルになります。
デフォルト	イネーブル	ディセーブル	ディセーブル
デフォルト	ディセーブル	イネーブルまたはディセーブル	ディセーブル
Disable	イネーブルまたはディセーブル	イネーブルまたはディセーブル	ディセーブル
イネーブル	イネーブルまたはディセーブル	イネーブルまたはディセーブル	イネーブル 注意 BPDU は送信されませんが、受信した場合には、通常の STP の動作が開始されません。BPDU の使用に当たっては、十分注意してください。

ループガードの概要

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

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

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

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



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

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

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

ループガードはポート単位でイネーブルにできます。ループガードを特定のポートでイネーブルにすると、そのポートが属するすべてのアクティブインスタンスまたは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。

ルートガードの概要

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

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

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

ルートガードをグローバルには設定できません。



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

STP 拡張機能の設定

STP 拡張機能の設定における注意事項

STP 拡張機能を設定する場合は、次の注意事項に従ってください。

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

スパニングツリーポートタイプのグローバルな設定

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

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

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

はじめる前に

STP が設定されていること。

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

手順

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

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

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

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

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

指定インターフェイスでのスパニングツリー エッジポートの設定

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

このコマンドには次の 4 つの状態があります。

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



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

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

はじめる前に

STP が設定されていること。

インターフェイスがホストに接続されていること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interfacetypeslot/port	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# spanning-tree port type edge	指定したアクセスインターフェイスをスパニングエッジポートに設定します。エッジポートは、リンクアップすると、ブロッキングステートやラーニングステートを経由することなく、フォワーディングステートに直接移行します。デフォルトのスパニングツリーポートタイプは「標準」です。

次に、アクセス インターフェイス Ethernet 1/4 をスパンニングツリー 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
```

指定インターフェイスでのスパンニングツリー 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ンニングツリー ネットワーク ポートを設定できます。

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

このコマンドには次の 3 つの状態があります。

- **spanning-tree port type network** : このコマンドは指定したポートを明示的にネットワーク ポートとして設定します。Bridge Assurance をグローバルにイネーブルにすると、スパンニングツリー ネットワーク ポート上で Bridge Assurance が自動的に実行されます。
- **spanning-tree port type normal** : このコマンドは、ポートを明示的に標準スパンニングツリー ポートとして設定します。このインターフェイス上では Bridge Assurance は動作しません。
- **no spanning-tree port type** : このコマンドは、**spanning-tree port type network default** コマンドをグローバル コンフィギュレーション モードで定義した場合に、ポートを暗黙的にスパンニングツリー ネットワーク ポートとしてイネーブルにします。Bridge Assurance をイネーブルにすると、このポート上で Bridge Assurance が自動的に実行されます。



(注) ホストに接続されているポートをネットワーク ポートとして設定すると、そのポートは自動的にブロッキング ステートに移行します。

はじめる前に

STP が設定されていること。

インターフェイスがスイッチまたはルータに接続されていること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface type slot/port	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスには、物理イーサネット ポートを指定できます。

	コマンドまたはアクション	目的
ステップ 3	switch(config-if)# spanning-tree port type network	指定したインターフェイスをスパン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。デフォルトのスパンニングツリーポートタイプは「標準」です。

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

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

BPDU ガードのグローバルなイネーブル化

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



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

はじめる前に

STP が設定されていること。

少なくとも一部のスパンニングツリーエッジポートが設定済みであること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# spanning-tree port type edge bpduguard default	すべてのスパンニングツリーエッジポートで、BPDU ガードを、デフォルトでイネーブルにします。デフォルトでは、グローバルな BPDU ガードはディセーブルです。

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

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

指定インターフェイスでの BPDU ガードのイネーブル化

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

BPDU ガードは、指定インターフェイスで次のように設定にできます。

- **spanning-tree bpduguard enable** : インターフェイス上で BPDU ガードが無条件にイネーブルになります。
- **spanning-tree bpduguard disable** : 指定インターフェイスで BPDU ガードを無条件に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。

はじめる前に

STP が設定されていること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interfacetypeslot/port	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# spanning-tree bpduguard {enable disable}	指定したスパニングツリー エッジ インターフェイスの BPDU ガードをイネーブルまたはディセーブルにします。デフォルトでは、BPDU ガードは、物理イーサネット インターフェイスではディセーブルです。
ステップ 4	switch(config-if)# no spanning-tree bpduguard	(任意) インターフェイス上で BPDU ガードをディセーブルにします。

	コマンドまたはアクション	目的
		(注) 動作中のエッジポートインターフェイスに spanning-tree port type edge bpduguard default コマンドが設定されている場合、そのインターフェイスでBPDUガードをイネーブルにします。

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

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

BPDU フィルタリングのグローバルなイネーブル化

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

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



注意

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



(注)

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

はじめる前に

STP が設定されていること。

少なくとも一部のスパニングツリーエッジポートが設定済みであること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# spanning-tree port type edge bpdufilter default	すべてのスパンニングツリー エッジ ポートで、BPDU フィルタリングを、デフォルトでイネーブルにします。デフォルトでは、グローバルな BPDU フィルタリングはディセーブルです。

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

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

指定インターフェイスでの BPDU フィルタリングのイネーブル化

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



注意

指定インターフェイスで **spanning-tree bpdufilter enable** コマンドを入力するときは注意してください。ホストに接続されていないポート上で BPDU フィルタリングを明示的に設定した場合、ポートは受信したすべての BPDU を無視してフォワーディング ステートになるので、ブリッジンググループが発生する可能性があります。

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

このコマンドには次の 3 つの状態があります。

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



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

はじめる前に

STP が設定されていること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interfacetypeslot/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	switch(config-if)# no spanning-tree bpdudfilter	(任意) インターフェイス上で BPDU フィルタリングをディセーブルにします。 (注) 動作中のスパニング ツリー エッジ ポート インターフェイスに spanning-tree port type edge 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。

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。



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

はじめる前に

STP が設定されていること。

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

手順

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

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

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

指定インターフェイスでのループガードまたはルートガードのイネーブル化

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

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

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



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

はじめる前に

STP が設定されていること。

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

手順

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

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

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

STP 拡張機能の設定の確認

STP 拡張機能の設定情報を表示するには、次の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。

ループ検出のエラーメッセージのトラブルシューティング

この項では、Cisco Nexus 3000 シリーズ スイッチのログにおける FWM-2-STM_LOOP_DETECT エラーメッセージに対応する方法について説明します。

Cisco Nexus 3000 シリーズ スイッチが次のメッセージを表示した場合、スイッチはこれら 2 つのインターフェイスの同じ送信元 MAC アドレスでフレームを受信し、スイッチはこれらのインターフェイス上で同じ MAC アドレスを超高速で学習することを示します。スイッチはループとしてこの状態を検出します。スイッチはコントロールプレーンを保護するため、MAC アドレスの学習を無効にします。これは、ループが 1 つの VLAN のみで発生している場合であっても、すべての VLAN に実装されます。

```
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 アドレスが移動します。
- 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することが原因で、MAC アドレスが移動します。

ループの検出

Forwarding Manager (FWM) には、MAC アドレスが移動する回数をカウントし、MAC アドレスの移動回数に基づいて重み付けするメカニズムがあります。移動した MAC アドレスの総数 (スイッチ全体にわたるすべての VLAN、MAC、インターフェイス) を決定して %FWM-2-STM_LOOP_DETECT 状態を宣言し、ループ状態で FWM を保護するために学習を無効にします。



(注) MAC 学習はシステム単位ではなく、VLAN 単位で無効にされます。

MAC 移動通知のロジックに注意する必要があります。MAC 移動に対する MAC アドレステーブルの通知を有効にすると、MAC 移動を通知することができます。これにより通知ログがコンソールに追加されますが、アクションは実行されません。10 秒の経過スキャン期間内に、特定の MAC アドレスが VLAN の特定のポートのペアを 3 回往復して移動すると、移動が宣言されます。



(注) MAC アドレスは 2 つのポートそれぞれにおいて 50 回検出される必要があります。

どの MAC アドレスが移動したかわかるように、スイッチの MAC 移動通知を有効にすることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# 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	スイッチで MAC 通知を有効にします。

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には、MAC 移動通知を有効にするだけでは不十分な場合があります。syslog メッセージの生成を確認するには、前のコマンドに加えて、これらのコマンド **mac address-table notification mac-move** を入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	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	すべてのスパンニング ツリー イベントの、レベル 6 から最大で最も重大度の高いイベントまでのロギングを有効にします。
ステップ 3	logging level fwm 6	すべての FWM イベントの、レベル 6 から最大で最も重大度の高いイベントまでのロギングを有効にします。
ステップ 4	logging monitor 6	レベル 6 の重大度とそれより上位の重大度に基づいて、デバイスが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ことにより、MAC アドレスの移動があった際に、FWM 検出の syslog で確実に表示されるようにします。スイッチの VLAN 全体で STP ポート ステータスを確認するには、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
```

MAC アドレスが移動したかどうかを確認するには、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
```

MAC アドレスの移動は、最小のロギング レベル 6 でも記録されます。これは、どの MAC アドレスが移動したかを表示するために必要です。

```
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
```

次の作業

正しい STP コンバージェンスを確認し、トポロジ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。競合または不正なポート ステートがないことを確認します。

物理的に移動するデータ フレームのソースが特定された場合は、急速かつ継続的な移動を停止するためにソースを制御します。

デフォルトでは、動的な学習が 180 秒後に再び有効になります。その時点で、すべての STP 競合または不整合は解決されます。そうでなければ、動的な学習が再び無効になります。