ループガードとBPDUスキュー検出を使用したSTPの設定

内容

概要

このドキュメントでは、レイヤ2ネットワークの安定性を向上させることを目的としたスパニングツリープロトコル(STP)機能について説明します。

前提条件

要件

このドキュメントでは、読者が STP の基本的な動作に精通していることを前提としています。詳細は、『Catalystスイッチでのスパニングツリープロトコル(STP)の説明と設定』を参照してください。

使用するコンポーネント

このドキュメントはCatalystスイッチに基づいていますが、ここで説明する機能のアベイラビリティは、使用するソフトウェアリリースによって異なる場合があります。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく

ださい。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

Spanning Tree Protocol（STP; スパンニング ツリー プロトコル）により、物理的に冗長化されたトポロジがループのないツリー状のトポロジに解決されます。STP の最大の問題は、一部のハードウェアの障害によって STP に障害が発生する点です。このような障害により、フォワーディング ループ（つまり STP ループ）が引き起こされます。STP ループによりネットワークの大規模な停止が引き起こされます。

このドキュメントでは、レイヤ 2 ネットワークの安定性の向上を目的に開発されたループ ガード STP 機能について説明しています。またこのドキュメントでは、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）スキュー検出についても説明しています。BPDU スキュー検出は、時間内に BPDU が受信されなかった場合に syslog メッセージを生成する診断機能です。

機能のアベイラビリティ

CatOS

- STP ループ ガード機能は、Catalyst 4000 および Catalyst 5000 プラットフォームでは Catalyst ソフトウェアの CatOS バージョン 6.2.1、Catalyst 6000 プラットフォームではバージョン 6.2.2 で導入されました。
- BPDU スキュー検出機能は、Catalyst 4000 および Catalyst 5000 プラットフォームでは Catalyst ソフトウェアの CatOS バージョン 6.2.1、Catalyst 6000 プラットフォームではバージョン 6.2.2 で導入されました。

Cisco IOS®

- STP ループ ガード機能は、Catalyst 4500 スイッチでは Cisco IOS ソフトウェア リリース 12.1(12c)EW、Catalyst 6500 では Cisco IOS ソフトウェア リリース 12.1(11b)EX で導入されました。
- BPDUスキュー検出機能は、Cisco IOSシステムソフトウェアが稼働するCatalystスイッチではサポートされていません。

STPポートのロール

STP では、設定、トポロジ、トポロジ内でのポートの相対的な位置、およびその他の考慮事項に基づいて、ブリッジ（またはスイッチ）の各ポートに内部的な役割が与えられます。ポートの役割によって、STP の観点から見たポートの動作が決まります。ポートでは、ポートの役割に基づいて、STP BPDU の送信や受信が行われ、データ トラフィックの転送やブロックが行われます。次のリストは各 STP ポートの役割の簡潔な要約です。

- *指定*：リンク（セグメント）ごとに1つの指定ポートが選択されます。指定ポートはルートブリッジに最も近いポートです。このポートは、そのリンク（セグメント）上で BPDU を送

信し、ルート ブリッジにトラフィックを転送します。STP によってコンバージされたネットワークでは、指定ポートはすべて STP フォワーディング ステートになります。
- *ルート*：ブリッジにはルートポートを1つだけ設定できます。ルート ポートはルート ブリッジに到達するポートです。STP によってコンバージされたネットワークでは、ルート ポートは STP フォワーディング ステートになります。
- *Alternate*：代替ポートはルートブリッジにつながりますが、ルートポートではありません。代替ポートは STP ブロッキング ステートになります。
- *バックアップ*：これは、同じスイッチ間の2つ以上のポートが直接または共有メディアを介して接続されている場合の特殊なケースです。この場合、1つのポートが指定ポートになり、残りのポートはブロックされます。このポートの役割はバックアップです。

STP ループ ガード

機能説明

STP ループ ガード機能では、レイヤ 2 の転送ループ（STP ループ）に対する防御が追加で提供されます。冗長トポロジで STP ブロッキング ポートが誤って forwarding 状態に移行すると、STP ループが発生します。これは通常、物理的に冗長化されたトポロジのいずれかのポート（必ずしも STP ブロッキング ポートとは限らない）で STP BPDU が受信されなくなったために発生します。STP の動作は、ポートのロールに基づく BPDU の継続的な送受信に依存しています。指定ポートでは BPDU が送信され、指定ポート以外のポートでは BPDU が受信されます。

物理的に冗長化されたトポロジのいずれかのポートで BPDU が受信されなくなると、STP ではトポロジにループがないと判断されます。最終的に、ブロッキング ポートが代替またはバックアップ ポートから指定ポートになり、フォワーディング ステートに移行します。この状況により、ループが発生してしまいます。

ループ ガード機能では、追加チェックが行われます。指定ポート以外のポートでループ ガードが有効にされていて、BPDU が受信されない場合、そのポートはリスニング/ラーニング/フォワーディング ステートに移行するのではなく、STP ループ不整合ブロッキング ステートに移行します。Loop Guard 機能がない場合、ポートは、指定ポートのロールを担ってしまいます。ポートは、STP フォワーディング ステートに移行し、ループが発生します。

Loop Guard によって loop-inconsistent ポートがブロックされると、次のメッセージが表示されます。

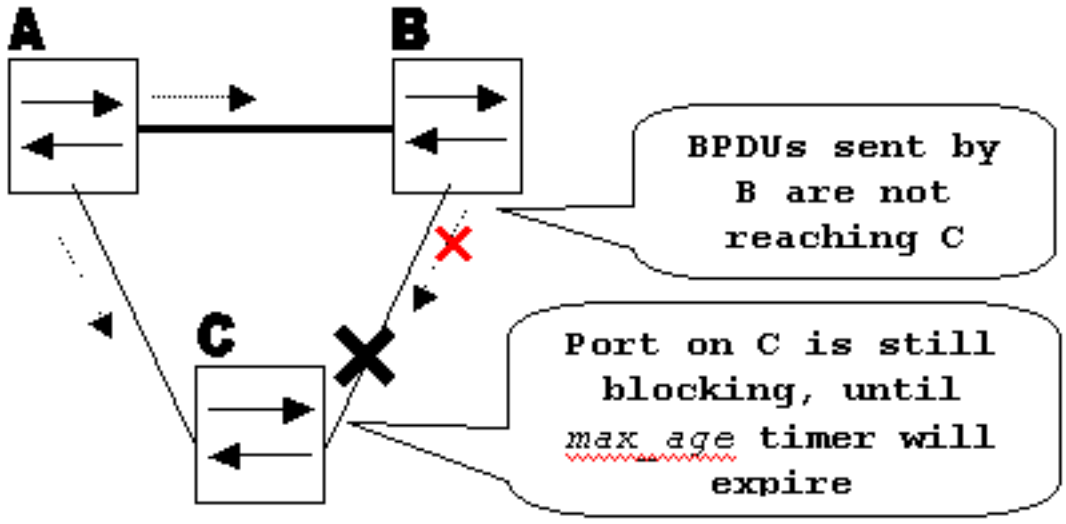
- CatOS
```
%SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 3/2 in vlan 3. Moved to
 loop-inconsistent state.
```
- Cisco IOS
```
%SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port FastEthernet0/24 on
VLAN0050.
```

ループ不整合 STP ステートのポートで BPDU が受信されると、そのポートは別の STP ステートに移行します。これは、受信したBPDUに対して、リカバリが自動的に行われ、介入が不要であることを意味します。復旧すると、次のメッセージがログに記録されます。

- CatOS
```
%SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```
- Cisco IOS
```
%SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port FastEthernet0/24 on
VLAN0050.
```

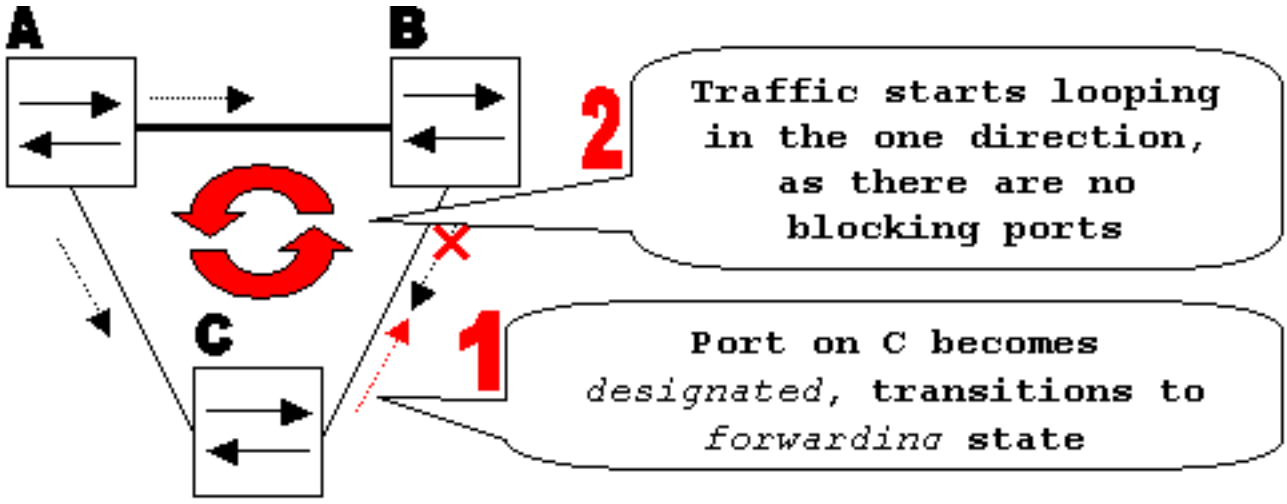
この動作を説明するために、次の例を考えてみましょう。

スイッチ A はルート スイッチです。スイッチ B とスイッチ C の間のリンクで単方向リンク障害が発生しているため、スイッチ C では、スイッチ B からの BPDU が受信されていません。



単方向リンク障害

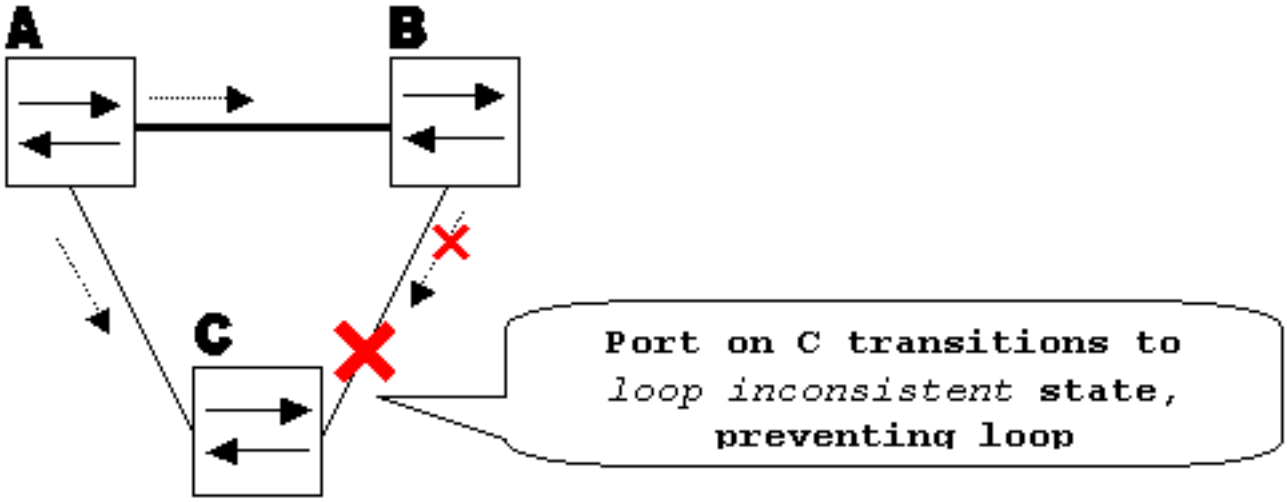
ループ ガードが無効の場合は、max_age タイマーの期限が切れた時点で、スイッチ C の STP ブロッキング ポートが STP リスニング ステートに移行し、さらに forward_delay 時間が 2 回経過してからフォワーディング ステートに移行します。この状況により、ループが発生してしまいます。



ループ

が作成されました

ループ ガードが有効になっている場合は、max_age タイマーの有効期限が切れた時点で、スイッチ C のブロッキング ポートは STP ループ不整合ステートに移行します。STP ループ不整合ステートのポートはユーザ トラフィックを通過させないため、ループは形成されません（このループ不整合ステートは、事実上はブロッキング ステートに等しくなります）。



ループ

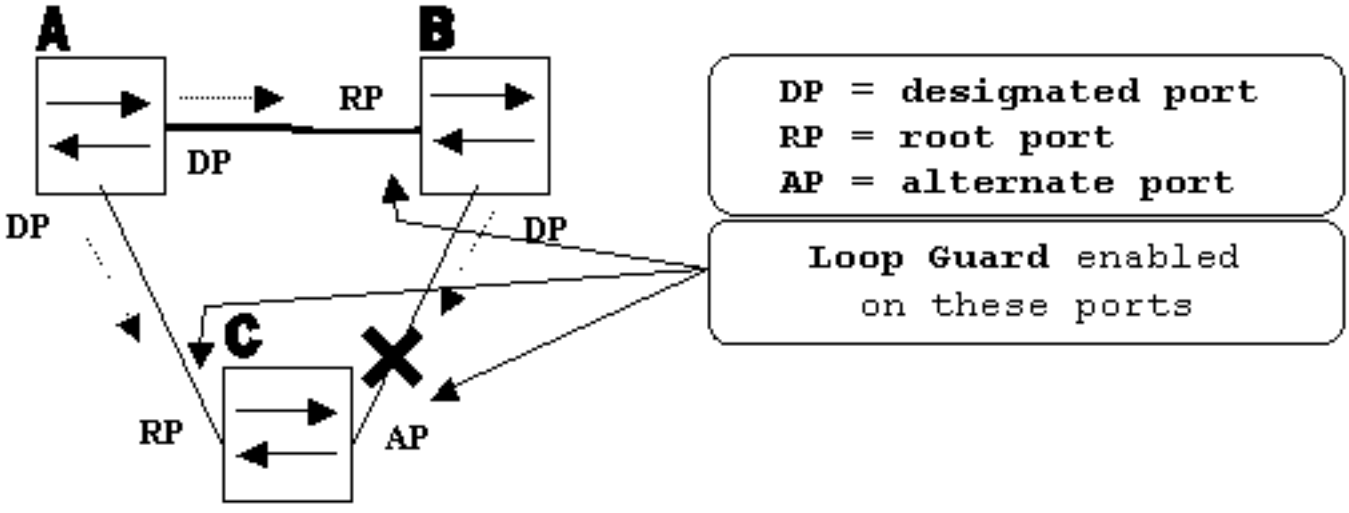
ガードの有効化によるループの防止

設定に関する考慮事項

ループ ガード機能はポート単位で有効になります。しかし、STP レベルでポートをブロックしている限り、ループ ガードでは VLAN 単位で不整合ポートがブロックされます（Per-VLAN STP のため）。つまり、トランク ポートで、ある特定の VLAN の BPDU が受信されない場合、その VLAN のみがブロックされます（ループ不整合 STP ステートに移行します）。同じ理由から、EtherChannel インターフェイスでループ ガードが有効になっている場合は、1 つのリンクだけでなく、特定の VLAN のチャネル全体がブロックされます（STP の観点では、EtherChannel は 1 つの論理ポートと見なされるため）。

Loop Guardを有効にするポートはどれか？最も明白な答えはブロッキング ポートです。ただし、これは全面的に正しいわけではありません。ループ ガードは、アクティブ トポロジのどのような組み合せにおいても、指定ポート以外のポート（より正確には、ルート ポートと代替ポート）で有効にする必要があります。ループガードがVLAN単位の機能でない限り、同じ（トランク）ポートを一方のVLANに指定し、もう一方のVLANに非指定にすることができます。考えられるフェールオーバーシナリオも考慮する必要があります。

例



ル

ープガードが有効なポート

デフォルトでは、ループ ガードは無効になっています。ループ ガードを有効にするには、次のコマンドを使用します。

- CatOS
  set spantree guard loop

```
Console> (enable) set spantree guard loop 3/13
Enable loopguard will disable rootguard if it's currently enabled on the port(s).
Do you want to continue (y/n) [n]? y
Loopguard on port 3/13 is enabled.
```

- Cisco IOS
  spanning-tree guard loop

```
Router(config)#interface gigabitEthernet 1/1
Router(config-if)#spanning-tree guard loop
```

Catalyst ソフトウェア (CatOS) のバージョン 7.1(1) では、すべてのポートでグローバルにループ ガードを有効にできます。実際には、ループ ガードはすべてのポイントツーポイント リンクで有効になります。ポイントツーポイント リンクは、各リンクのデュプレックス ステータスによって検出されます。全二重の場合、リンクはポイントツーポイントであると見なされます。グローバル設定は、ポート単位で設定や上書きが可能です。

ループ ガードをグローバルに有効にするには、次のコマンドを発行します。

- CatOS

```
Console> (enable)  set spantree global-default loopguard enable
```

- Cisco IOS

```
Router(config)# spanning-tree loopguard default
```

ループ ガードを無効にするには、次のコマンドを発行します。

- CatOS

```
Console> (enable) set spantree guard none
```

- Cisco IOS

```
Router(config-if)#no spanning-tree guard loop
```

ループ ガードをグローバルに無効にするには、次のコマンドを発行します。

- CatOS

```
Console> (enable) set spantree global-default loopguard disable
```

- Cisco IOS

```
Router(config)#no spanning-tree loopguard default
```

ループ ガードのステータスを確認するには、次のコマンドを発行します。

- CatOS
  show spantree guard

```
Console> (enable) show spantree guard 3/13
Port                     VLAN Port-State    Guard Type
------------------------ ---- ------------- ----------
3/13                     2    forwarding          loop
Console> (enable)
```

- Cisco IOS
  show spanning-tree

```
Router#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfig guard is enabled
Extended system ID           is disabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Pathcost method used         is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
Total                         0         0        0          0          0
```

ループ ガードと UDLD の対比

ループ ガードと Unidirectional Link Detection（UDLD; 単方向リンク検出）の両機能は、単方向リンクによって生じる STP 障害を防止するという意味で、部分的に共通するところがあります。ただし、これら 2 つの機能では、機能と問題へのアプローチ方法が異なっています。次の表は、ループ ガードと UDLD の機能を説明したものです。

機能	ループ ガード	UDLD
コンフィギュレーション	ポート単位	ポート単位
アクションの精度	VLAN 単位	ポート単位
自動リカバリ	Yes	はい、err-disable タイムアウト機能付き
単方向リンクを原因とする STP 障害に対する保護	はい、冗長トポロジのすべてのルート ポートと代替ポート上で有効になっている場合	はい、冗長トポロジのすべてのリンク上で有効になっている場合
ソフトウェアの問題を原因とする STP 障害に対する保護（指定スイッチが BPDU を送信しない）	Yes	No
誤った配線からの保護。	No	Yes

設計上のさまざまな考慮事項に基づいて、UDLD とループ ガード機能のどちらかを選択できます。STPに関して、2つの機能の最も顕著な違いは、ソフトウェアの問題によって引き起こされるSTP障害に対する保護がUDLDにないことです。その結果、指定スイッチからは BPDU が送信されません。ただし、このタイプの障害は、単方向リンクによって発生する障害よりも（桁違いに

) はるかに少ない障害です。その代わり、EtherChannel上の単方向リンクの場合は、UDLDの方が柔軟性が高くなります。この場合、UDLDは障害が発生したリンクだけを無効にし、チャネルは残ったリンクを使用して機能を維持できます。このような障害では、チャネル全体をブロックするために、ループ ガードではポートがループ不整合ステートにされます。

また、ループガードは、共有リンクやリンクアップ以降常にリンクが単方向の状況では機能しません。最後のケースでは、ポートは BPDU を受信せず、指定ポートになります。この動作は正常である可能性があるため、この特定のケースはループガードではカバーされません。UDLD を使用すれば、このようなシナリオに対しても防止が可能です。

これまでの説明からわかるように、UDLD とループ ガードを両方とも有効にすれば最高レベルの保護が得られます。

ループ ガードと他の STP 機能との相互運用性

ルート ガード

ルート ガードはループ ガードと同時には使用できません。ルート ガードは指定ポートで使用されるもので、ポートが指定ポート以外になることが防止されます。ループ ガードは指定ポート以外のポートで動作し、max_age の期限切れによってポートが指定ポートになることが防止されます。ルート ガードはループ ガードと同じポートで有効にすることはできません。あるポートにループ ガードが設定されると、そのポートではルート ガードは無効になります。

アップリンク ファーストとバックボーン ファースト

アップリンク ファーストとバックボーン ファーストはどちらもループ ガードに対して透過的です。再コンバージェンス時にバックボーン ファーストによって max_age タイマーが無視されたときは、ループ ガードは起動されません。アップリンク ファーストとバックボーン ファーストの詳細については、次のドキュメントを参照してください。

- 『Cisco UplinkFast 機能の説明と設定』
- Catalyst スイッチ上の Backbone Fast についての説明と設定

PortFast、BPDU ガード、ダイナミック VLAN

PortFast が有効になっているポートに対しては、ループ ガードは有効にできません。BPDU ガードは PortFast が有効になっているポートで動作しますが、BPDU ガードにも一部の制限が適用されます。ループ ガードはダイナミック VLAN に対しては有効にできませんが、これはこれらのポートでは PortFast が有効であるためです。

共有リンク

共有リンクではループガードを有効にしないでください。共有リンクでループガードを有効にすると、共有セグメントに接続されたホストからのトラフィックがブロックされる可能性があります。

多重スパニングツリー (MST)

ループ ガードは MST 環境で正常に動作します。

BPDU スキュー検出

ループガードは、BPDUスキュー検出を使用して正しく動作できます。

BPDU スキュー検出

機能説明

STP の動作は BPDU のタイムリーな受信に大きく依存しています。hello_time メッセージ（デフォルトでは 2 秒）ごとに、ルート ブリッジは BPDU を送信します。非ルート ブリッジは hello_time メッセージごとに BPDU を再生成しませんが、ルート ブリッジから送信され、中継された BPDU を受信します。したがって、すべての非ルートブリッジは、hello_timeメッセージごとに、すべてのVLANでBPDUを受信する必要があります。場合によっては、BPDU が失われたり、ブリッジの CPU の負荷が高すぎて BPDU をタイムリーに中継できなかったりすることがあります。これらの問題やその他の問題によって、（たとえ到着する場合でも）BPDU の到達が遅れる可能性があります。これにより、スパニング ツリー トポロジの安定性が損なわれる可能性があります。

BPDU スキュー検出を使用すると、到着が遅れる BPDU をスイッチで常時監視して、syslog メッセージで管理者に通知できます。今までに BPDU が遅れて到達したことがある（つまりスキューが発生した）すべてのポートについて、スキュー検出は、最新のスキューと、そのスキューの期間（遅延）を報告します。また、特定のポートでの最長の BPDU 遅延も報告されます。

ブリッジの CPU が過負荷状態にならないようにするため、BPDU スキューイングが発生しても、そのたびに syslog メッセージが生成されるわけではありません。60 秒ごとに 1 つのメッセージが生成されるようレート制限されています。ただし、BPDUの遅延がmax_ageを2で割った値（デフォルトでは10秒）を超えると、メッセージはすぐに出力されます。

> **注**:BPDUスキュー検出は診断機能です。BPDU スキューイングが検出されても syslog メッセージが送信されるだけで、BPDU スキュー検出では修正措置は行われません。

> **注**:BPDUスキュー検出機能は、Cisco IOSシステムソフトウェアが稼働するCatalystスイッチではサポートされていません

BPDU スキュー検出によって生成された syslog メッセージの例を次に示します。

```
%SPANTREE-2-BPDU_SKEWING: BPDU skewed with a delay of 10 secs (max_age/2)
```

設定に関する考慮事項

BPDU スキュー検出はスイッチ単位で設定されます。デフォルト設定は「無効」です。BPDU スキュー検出を有効にするには、次のコマンドを発行します。

```
Cat6k> (enable) set spantree bpdu-skewing enable
   Spantree bpdu-skewing enabled on this switch.
```

BPDUスキューイング情報を表示するには、次の例に示すように、**show spantree bpdu-skewing <vlan>|<mod/port>** コマンドを使用します。

```
Cat6k> (enable) show spantree bpdu-skewing 1
Bpdu skewing statistics for vlan 1
Port Last Skew (ms) Worst Skew (ms) Worst Skew Time
-------------- --------------- --------------- -------------------------
```

関連情報

- スパニングツリー プロトコル ルート ガード拡張機能
- スパニング ツリー PortFast BPDU ガード機能拡張
- 単方向リンク検出プロトコル(UDLD)機能の説明と設定
- PortFast と他のコマンドを使用したワークステーションの接続始動遅延の修復
- テクニカルサポートとダウンロード – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。