スパニング ツリー PortFast の拡張 BPDU ガード

目次

概要

このドキュメントでは、PortFast の Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）ガード機能について説明しています。 この機能は、Cisco が開発した Spanning Tree Protocol（STP; スパンニング ツリー プロトコル）の機能拡張の 1 つです。 この機能は、交換回線ネットワークの信頼性、管理性、およびセキュリティを強化するものです。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

次のソフトウェア バージョンでは、STP PortFast BPDU ガードが導入されています。

- Catalyst 4500/4000（Supervisor Engine II）、5500/5000、6500/6000、2926、2926G、2948G、2980G の各プラットフォーム対応の Catalyst OS（CatOS）ソフトウェア バージョン 5.4.1
- Catalyst 6500/6000 プラットフォームのための Cisco IOS® ソフトウェア リリース 12.0(7)XE
- Catalyst 4500/4000（Supervisor Engine III）では Cisco IOS ソフトウェア リリース

12.1(8a)EW
- Catalyst 4500/4000（Supervisor Engine IV）では Cisco IOS ソフトウェア リリース 12.1(12c)EW
- Catalyst 2900XL および 3500XL シリーズでは Cisco IOS ソフトウェア リリース 12.0(5)WC5
- Catalyst 3750 シリーズ スイッチでは Cisco IOS ソフトウェア リリース 12.1(11)AX
- Catalyst 3750 Metro スイッチでは Cisco IOS ソフトウェア リリース 12.1(14)AX
- Catalyst 3560 シリーズ スイッチでは Cisco IOS ソフトウェア リリース 12.1(19)EA1
- Catalyst 3550 シリーズ スイッチでは Cisco IOS ソフトウェア リリース 12.1(4)EA1
- Catalyst 2970 シリーズ スイッチでは Cisco IOS ソフトウェア リリース 12.1(11)AX
- Catalyst 2955 シリーズ スイッチでは Cisco IOS ソフトウェア リリース 12.1(12c)EA1
- Catalyst 2950 シリーズ スイッチでは Cisco IOS ソフトウェア リリース 12.1(6)EA2
- Catalyst 2950 Long-Reach Ethernet（LRE; 長距離イーサネット）スイッチでは Cisco IOS ソフトウェア リリース 12.1(11)EA1
- Catalyst 2940 シリーズ スイッチでは Cisco IOS ソフトウェア リリース 12.1(13)AY

注: STP PortFast BPDU ガードは、Catalyst 8500 シリーズ、2948G-L3、または 4908G-L3 スイッチには**使用できません**。

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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。

機能説明

STP は、ループのないツリー状のトポロジに、メッシュ トポロジを構成します。 ブリッジ ポート上でリンクがアップすると、そのポートで STP の計算が実行されます。 計算の結果、ポートの状態がフォワーディング状態またはブロッキング状態に遷移します。 この結果は、ネットワーク内でのポートの位置と STP パラメータに左右されます。 通常、この計算と遷移にはおよそ 30 ~ 50 秒の時間がかかります。 この時点では、ユーザ データはポートを通過しません。 ユーザ アプリケーションによっては、この期間中にタイムアウトになる可能性があります。

ポートをただちにフォワーディング状態に遷移できるようにするには、STP PortFast 機能をイネーブルにします。 PortFast を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。 ポートは引き続き STP に参加しています。 したがって、ポートがループの一部になる場合、最終的には STP ブロッキング モードに遷移します。

ポートが STP に参加している限り、一部のデバイスによってルート ブリッジの役割が引き継がれ、アクティブな STP トポロジが影響を受ける可能性があります。 ルート ブリッジの役割を引き継ぐために、デバイスがそのポートに接続され、現在のルート ブリッジよりも低いブリッジ優先度で STP が実行されます。 この方法で別のデバイスによってルート ブリッジが引き継がれると、ネットワークは最適な状態ではなくなります。 これは、ネットワークに対する単純な Denial of Service（DoS; サービス拒否攻撃）です。 ブリッジ優先度の低い（0 の）STP デバイスを一時的に導入し、その後取りはずすと、永続的な STP 再計算が発生します。

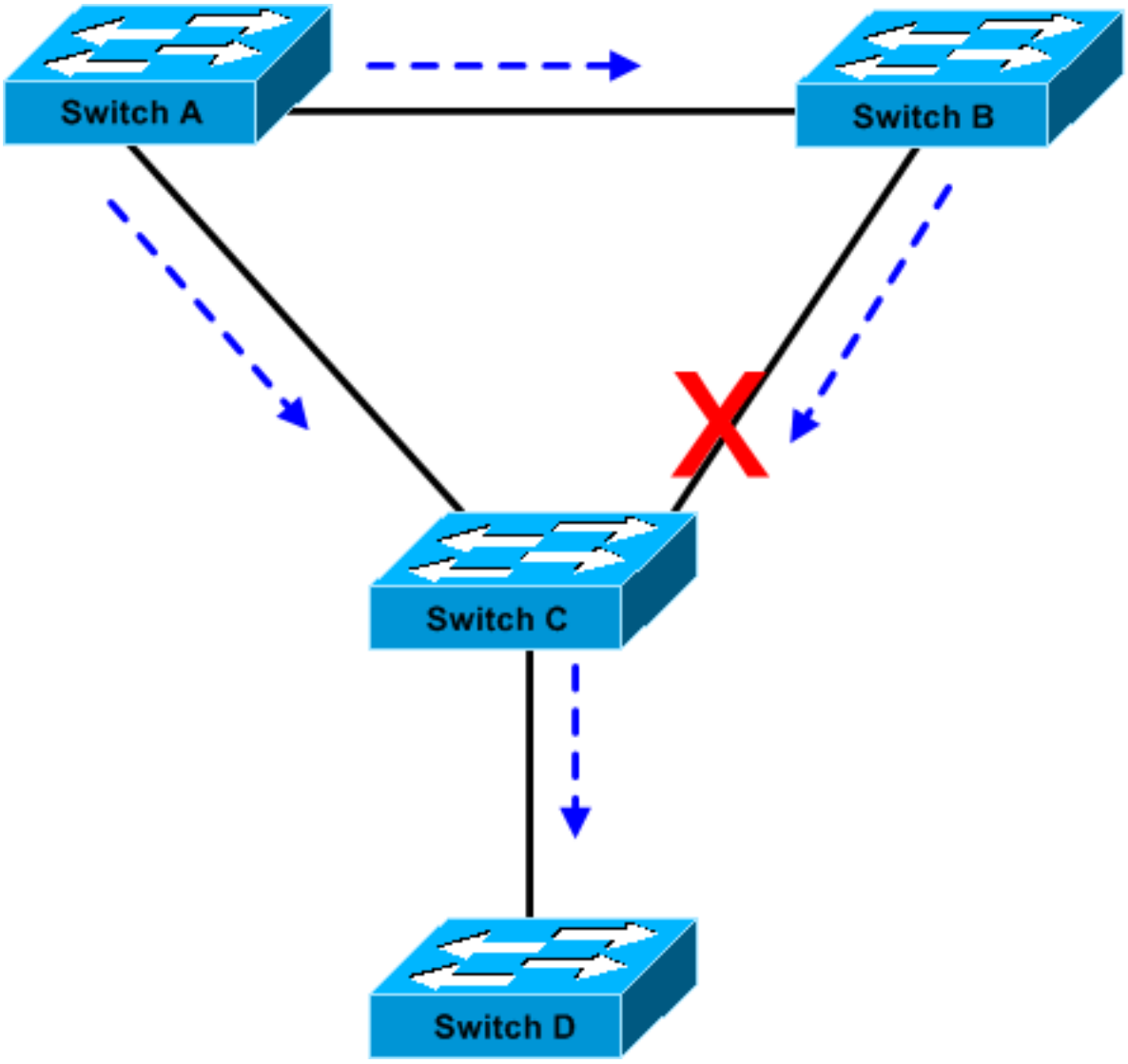
STP PortFast BPDU ガード機能拡張を使用すると、ネットワーク設計者は STP ドメイン境界を強制し、アクティブなトポロジを予測可能な状態に保つことができます。 STP PortFast がイネー

ブルになっているポートの背後にあるデバイスでは、STP トポロジに影響を及ぼすことはできません。 BPDU の受信と同時に、BPDU ガード操作によって PortFast が設定されたポートがディセーブルにされます。 BPDU ガードによって、ポートはエラーディセーブル状態に遷移し、メッセージがコンソールに表示されます。 次にメッセージの例を示します。

```
2000 May 12 15:13:32 %SPANTREE-2-RX_PORTFAST:Received BPDU on PortFast enable port.
Disabling 2/1
2000 May 12 15:13:32 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
```

次の例を検討します。

Figure 1



A を持ち、優先順位 8192 をです VLAN のためのルート繋いで下さい。 ブリッジ B は優先順位が 16384 であり、同じ VLAN のバックアップ ルート ブリッジです。 ブリッジ A とブリッジ B はギガビット イーサネット リンクで接続され、ネットワークの中心部分を構成しています。 ブリッジ C はアクセス スイッチであり、デバイス D に接続しているポートで PortFast が設定されています。 他の STP パラメータがデフォルトの場合、ブリッジ B に接続しているブリッジ C のポートは STP ブロッキング状態です。 デバイス D (PC) は STP に参加していません。 破線の矢印は STP BPDU の流れを示しています。

図 2

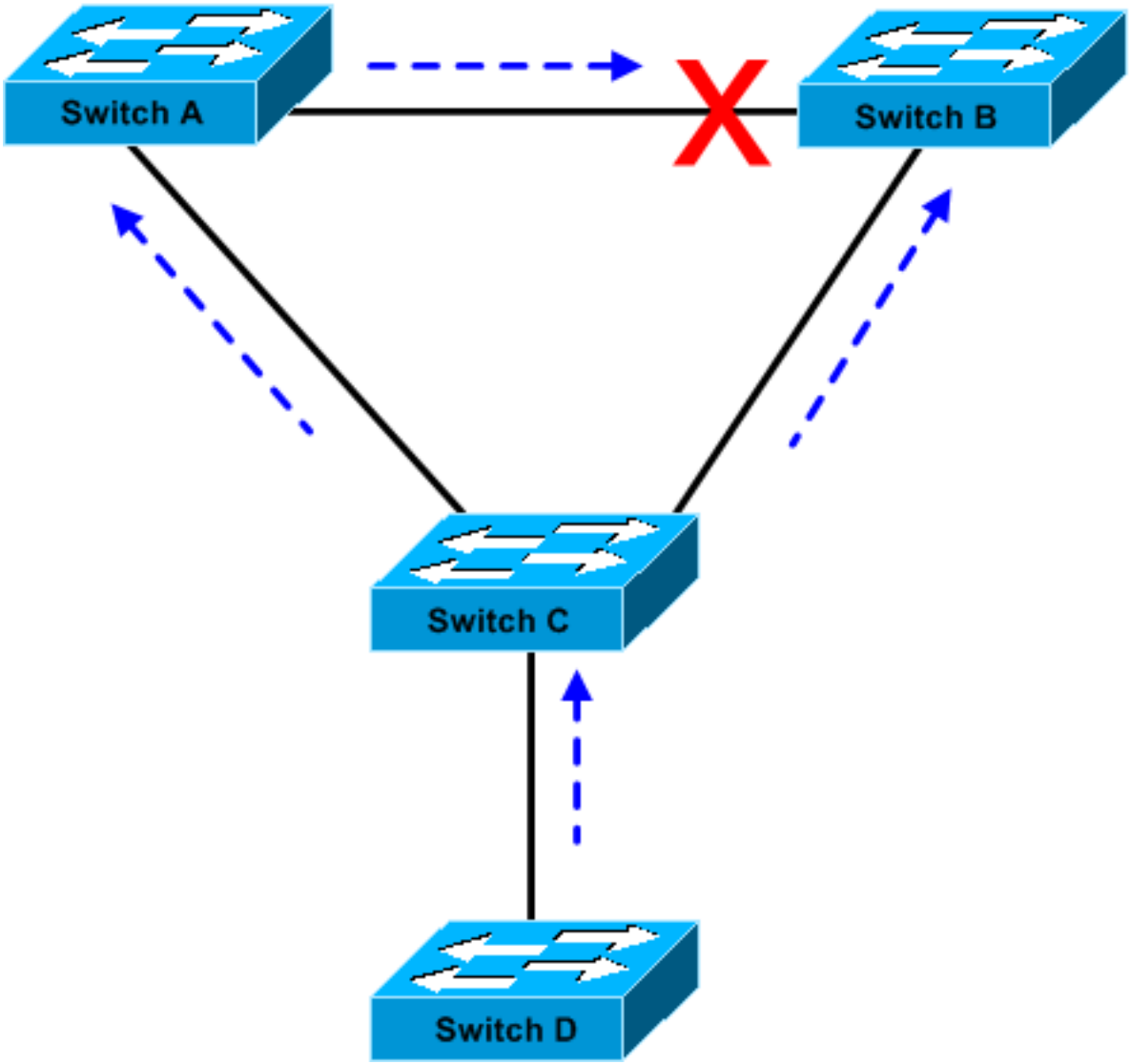


図 2 では、デバイス D による STP への参加が開始されています。 たとえば Linux ベースのブリッジ アプリケーションが PC で起動されます。 ソフトウェア ブリッジのプライオリティが 0 またはルート ブリッジのプライオリティよりも小さい値の場合、ソフトウェア ブリッジによってルート ブリッジの役割が引き継がれます。 2 台のコア スイッチを接続しているギガビット リンクはブロッキング モードに遷移します。 この遷移により、その VLAN 内にあるすべてのデータが、100 Mbps リンクを介して流れるようになります。 このリンクが対応できるよりも多くのデータが、その VLAN のコアを経由して流れた場合、フレームの廃棄が発生します。 フレームの廃棄は、接続停止に至ります。

STP PortFast BPDU ガード機能により、この状況の発生が回避されます。 この機能では、ブリッジ C でデバイス D からの STP BPDU が受信されると同時にポートがディセーブルにされます。

設定

STP PortFast BPDU ガードはグローバル単位でイネーブルまたはディセーブルにでき、この機能は PortFast が設定されたすべてのポートに作用します。 デフォルトでは、STP BPDU ガードは無効になっています。 スイッチで STP PortFast BPDU ガードをイネーブルにするには、次のコマンドを発行します。

CatOS コマンド

```
Console> (enable) set spantree portfast bpdu-guard enable

Spantree portfast bpdu-guard enabled on this switch.

Console> (enable)
```

Cisco IOS ソフトウェア コマンド

```
CatSwitch-IOS(config)# spanning-tree portfast bpduguard
CatSwitch-IOS(config)
```

ポートが STP BPDU ガードによってディセーブルにされている場合は、手動でイネーブルにしない限りこのポートはディセーブル状態のままです。 ポートは、エラーディセーブル状態から自動的に再度イネーブルになるように設定できます。 errdisable-timeout interval を設定し、timeout 機能をイネーブルにする、次のコマンドを発行します。

CatOS コマンド

```
Console> (enable) set errdisable-timeout interval 400

Console> (enable) set errdisable-timeout enable bpdu-guard
```

Cisco IOS ソフトウェア コマンド

```
CatSwitch-IOS(config)# errdisable recovery cause bpduguard

CatSwitch-IOS(config)# errdisable recovery interval 400
```

注: デフォルトでは、タイムアウト間隔は 300 秒に設定されており、タイムアウト機能は無効になっています。

モニタリング

STP BPDU ガード機能がイネーブルになっているか、ディセーブルになっているかを確認するには、次のコマンドを発行します。

コマンド出力

CatOS コマンド

```
Console> (enable) show spantree summary
Root switch for vlans: 3-4.
Portfast bpdu-guard enabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Summary of Connected Spanning Tree Ports By VLAN:

Vlan  Blocking Listening Learning Forwarding STP Active

----- -------- --------- -------- ---------- ----------

   1         0         0        0          1          1

   3         0         0        0          1          1
```

```
   4         0         0         0          1          1

  20         0         0         0          1          1


Blocking Listening Learning Forwarding STP Active

----- -------- --------- -------- ---------- ----------

Total        0         0         0          4          4

Console> (enable)
```

Cisco IOS ソフトウェア コマンド

```
CatSwitch-IOS# show spanning-tree summary totals
Root bridge for: none.
PortFast BPDU Guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Spanning tree default pathcost method used is short


Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
  1 VLAN                0        0         0        1          1

CatSwitch-IOS#
```

関連情報

- LAN 製品に関するサポート ページ
- LAN スイッチングに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems