

# Entender o aprimoramento do Spanning Tree PortFast BPDU Guard

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Descrição do recurso](#)

[Figure 1](#)

[Figure 2](#)

[Configuração](#)

[Comando CatOS](#)

[Comando do software Cisco IOS®](#)

[Comandos de CatOS](#)

[Comandos do software Cisco IOS](#)

[Monitor](#)

[Saída do comando](#)

[Comando CatOS](#)

[Comando do Cisco IOS Software](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve o recurso de aprimoramento de proteção BPDU (PortFast Bridge Protocol Data Unit) do STP (Spanning Tree Protocol).

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

### Componentes Utilizados

Estas versões de software introduziram o STP PortFast BPDU guard:

- Software Catalyst OS (CatOS) versão 5.4.1 para as plataformas Catalyst 4500/4000 (Supervisor Engine II), 5500/5000, 6500/6000, 2926, 2926G, 2948G e 2980G

- Software Cisco IOS® versão 12.0(7)XE para as plataformas Catalyst 6500/6000
- Software Cisco IOS versão 12.1(8a)EW para Supervisor Engine III do Catalyst 4500/4000
- Software Cisco IOS versão 12.1(12c)EW para Supervisor Engine IV do Catalyst 4500/4000
- Software Cisco IOS versão 12.0(5)WC5 para as séries Catalyst 2900XL e 3500XL
- Software Cisco IOS versão 12.1(11)AX para Catalyst 3750 Series Switches
- Software Cisco IOS versão 12.1(14)AX para os switches Catalyst 3750 Metro
- Software Cisco IOS versão 12.1(19)EA1 para Catalyst 3560 Series Switches
- Software Cisco IOS versão 12.1(4)EA1 para Catalyst 3550 Series Switches
- Software Cisco IOS versão 12.1(11)AX para Catalyst 2970 Series Switches
- Software Cisco IOS versão 12.1(12c)EA1 para Catalyst 2955 Series Switches
- Software Cisco IOS versão 12.1(6)EA2 para Catalyst 2950 Series Switches
- Software Cisco IOS versão 12.1(11)EA1 para switches Ethernet de longo alcance (LRE) Catalyst 2950
- Software Cisco IOS versão 12.1(13)AY para os switches da série Catalyst 2940



Observação: o STP PortFast BPDU guard não está disponível para os switches da série Catalyst 8500, 2948G-L3 ou 4908G-L3.

---

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Conventions

Consulte as Convenções de dicas técnicas da Cisco para obter mais informações sobre as convenções do documento.

## Informações de Apoio

Este documento explica as características de proteção da Unidade de Dados de Protocolo de Bridge (BPDU) de PortFast. Esta característica é uma das melhorias do Spanning Tree Protocol (STP) que a Cisco criou. Esta característica melhora a confiabilidade, a capacidade de gerenciamento e a segurança da rede de switch.

## Descrição do recurso

O STP configura a topologia em malha em uma topologia em árvore, sem loops. Quando o link em uma porta de bridge fica ativo, ocorre o cálculo de STP nessa porta. O resultado do cálculo é a transição da porta para o estado forwarding ou blocking. O resultado depende da posição da porta na rede e dos parâmetros STP. Esse período de cálculo e transição geralmente leva de 30 a 50 segundos. Nesse momento, nenhum dado do usuário passa pela porta. Alguns aplicativos de usuário podem expirar durante o período.

Para permitir a transição imediata da porta para o estado forwarding, habilite o recurso STP PortFast. O PortFast faz imediatamente a transição da porta para o modo de encaminhamento STP na conexão. A porta ainda participa do STP. Portanto, se a porta for parte do loop, ela finalmente fará a transição para o modo de bloqueio de STP.

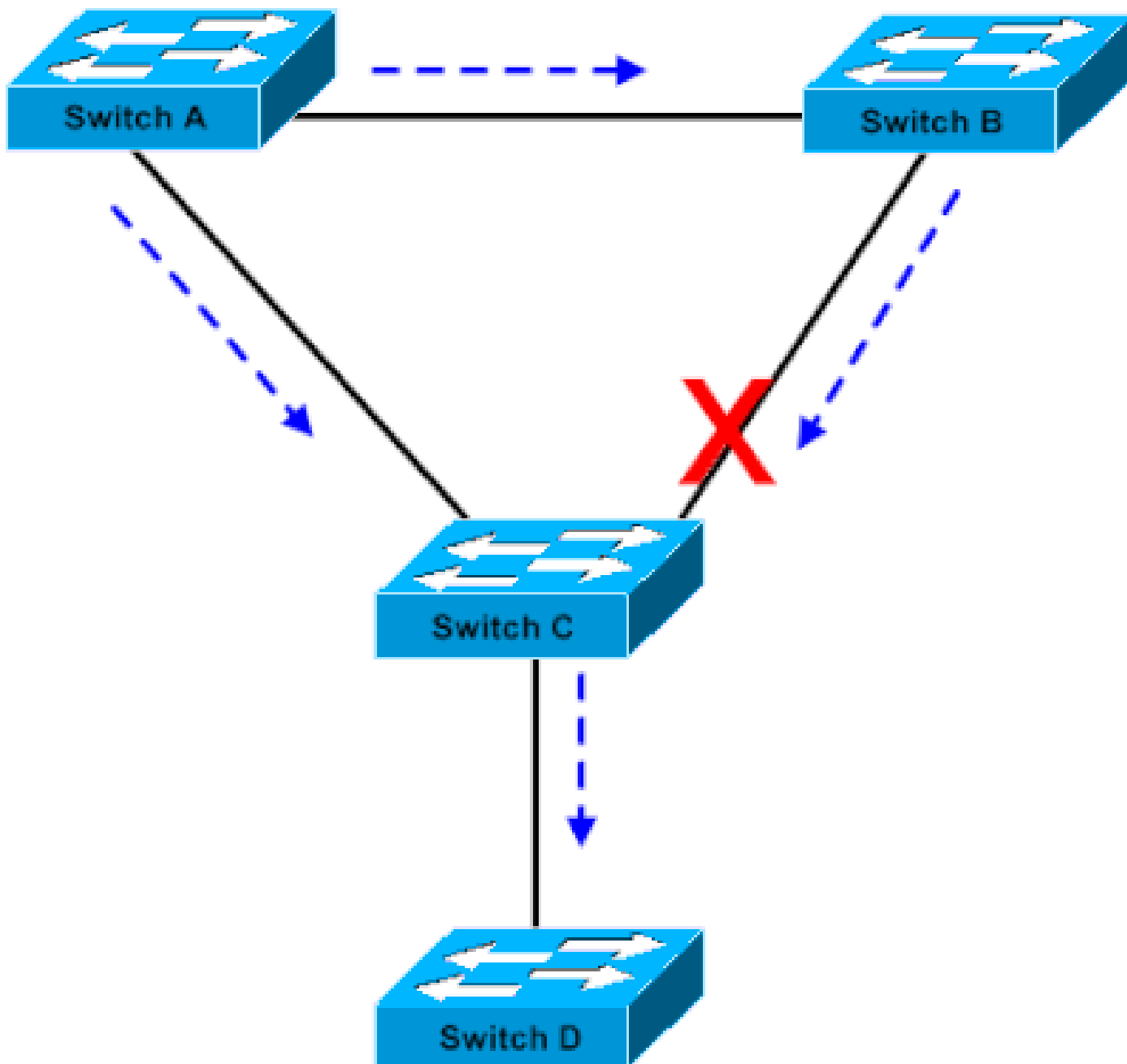
Contanto que a porta participe do STP, algum dispositivo pode assumir a função de bridge raiz e afetar a topologia ativa do STP. Para assumir a função de bridge raiz, o dispositivo seria conectado à porta e executaria o STP com uma prioridade de bridge mais baixa que a da bridge raiz atual. Se outro dispositivo assumir a função de bridge raiz dessa maneira, ele tornará a rede abaixo do ideal. Essa é uma forma simples de ataque de negação de serviço (DoS) na rede. A introdução temporária e a remoção subsequente de dispositivos STP com baixa (0) prioridade de bridge causam um recálculo permanente do STP.

O aprimoramento do protetor de BPDU PortFast de STP permite que os projetistas de rede reforcem as bordas do domínio de STP e mantenham a topologia ativa previsível. Os dispositivos por trás das portas que têm o STP PortFast habilitado não podem influenciar a topologia do STP. Na recepção de BPDUs, a operação de proteção de BPDU desativa a porta que tem PortFast configurado. O BPDU guard faz a transição da porta para o estado errdisable e uma mensagem aparece no console. Esta mensagem é um exemplo:

```
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
```

Considere este exemplo:

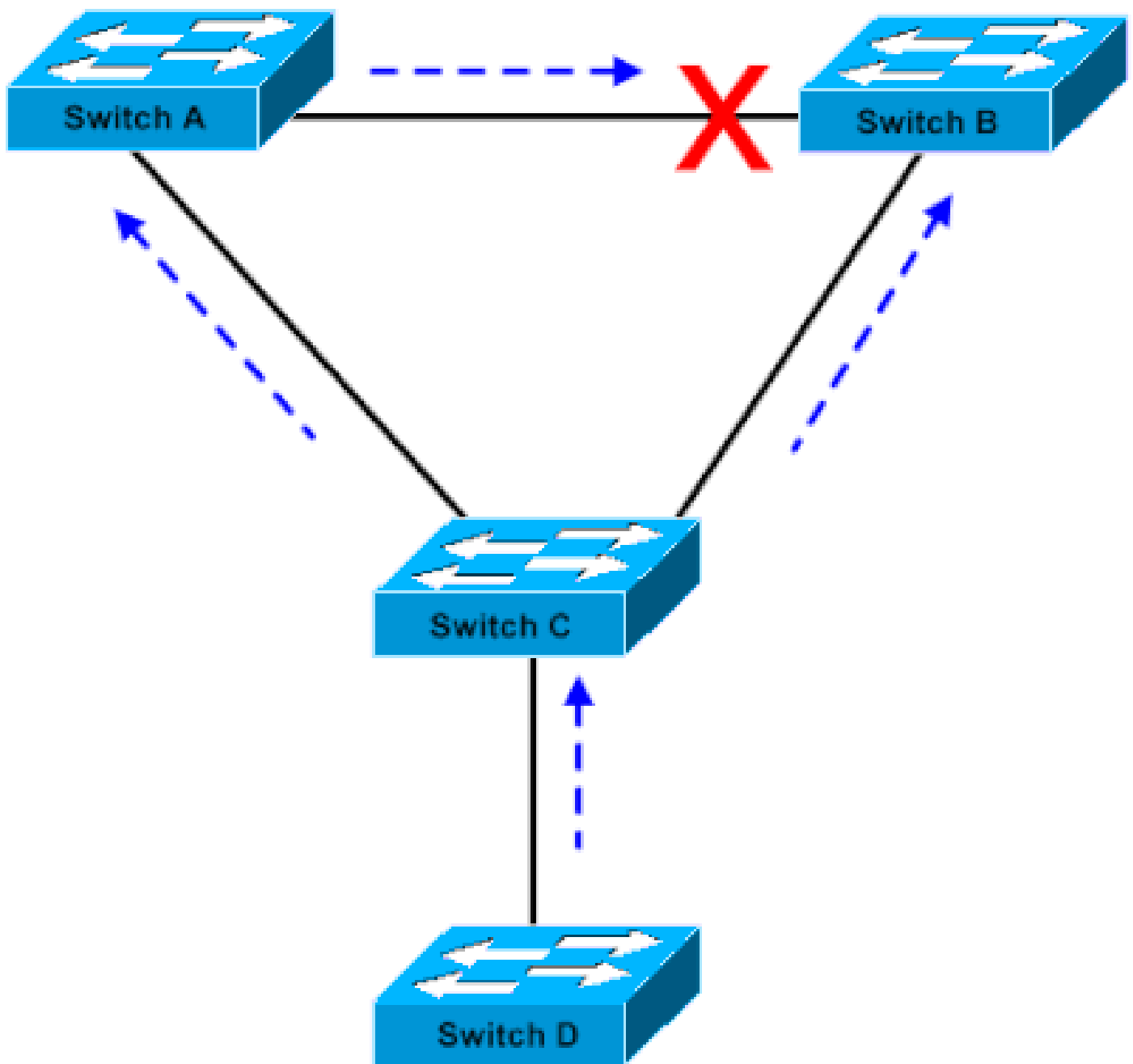
Figure 1



Conexão de Bridge

A ponte A tem prioridade 8192 e é a raiz da VLAN. O Bridge B tem a prioridade 16384 e é o Root Bridge de backup para o mesmo VLAN. As bridges A e B, que são conectadas por um link Gigabit Ethernet, formam um núcleo da rede. A ponte C é um switch de acesso e tem o PortFast configurado na porta que se conecta ao dispositivo D. Se os outros parâmetros de STP forem default, a porta da ponte C que se conecta à ponte B está no estado de bloqueio de STP. O dispositivo D (PC) não participa do STP. As setas tracejadas indicam o fluxo dos BPDUs do STP.

Figure 2



Aplicativo de Bridge baseado em Linux é Iniciado em um PC

Na Figura 2, o dispositivo D começou a participar do STP. Por exemplo, um aplicativo de bridge baseado em Linux é iniciado em um PC. Se a prioridade da bridge do software for 0 ou qualquer valor menor que a prioridade da bridge raiz, a bridge do software assume a função de bridge raiz. O enlace Gigabit Ethernet que conecta os dois switches centrais faz a transição para o modo de bloqueio. A transição faz com que todos os dados naquela VLAN fluam através do link de 100 Mbps. Se houver mais fluxo de dados através do núcleo na VLAN do que o enlace pode acomodar, ocorrerá a queda dos quadros. O descarte de quadros leva a uma interrupção de conectividade.

O recurso protetor de BPDU PortFast de STP evita essa situação. O recurso desabilita a porta assim que a ponte C recebe o STP BPDU do dispositivo D.

# Configuração

Você pode habilitar ou desabilitar o STP PortFast BPDU guard globalmente, o que afeta todas as portas que têm o PortFast configurado. Por padrão, o protetor de BPDU do STP está desabilitado. Execute este comando para habilitar o STP PortFast BPDU guard no switch:

## Comando CatOS

<#root>

Console> (enable)

```
set spantree portfast bpdu-guard enable
```

Spantree portfast bpdu-guard enabled on this switch.

Console> (enable)

## Comando do software Cisco IOS®

<#root>

CatSwitch-IOS(config)#

```
spanning-tree portfast bpduguard
```

CatSwitch-IOS(config)

Quando o STP BPDU guard desativa a porta, a porta permanece no estado disabled, a menos que a porta seja ativada manualmente. Você pode configurar uma porta para reativar-se automaticamente a partir do estado errdisable. Emita estes comandos, que definem o intervalo errdisable-timeout e ativam o recurso timeout :

## Comandos de CatOS

<#root>

Console> (enable)

```
set errdisable-timeout interval 400
```

Console> (enable)

```
set errdisable-timeout enable bpdu-guard
```

## Comandos do software Cisco IOS

```
<#root>
```


```
CatSwitch-IOS(config)#
```

```
errdisable recovery cause bpduguard
```

```
CatSwitch-IOS(config)#
```

```
errdisable recovery interval 400
```

---

 Observação: o intervalo de timeout padrão é de 300 segundos e, por default, o recurso de timeout está desativado.

---

## Monitor

Para verificar se o recurso está habilitado ou desabilitado, emita o próximo comando aplicável.

### Saída do comando

#### Comando CatOS

```
<#root>
```

```
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)

## Comando do Cisco IOS Software

<#root>

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#

## Informações Relacionadas

- [Suporte técnico e downloads da Cisco](#)



## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.