

Aprimore o Spanning Tree Protocol com o Root Guard

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Descrição do recurso](#)

[Disponibilidade](#)

[Configuração](#)

[Configuração do Cisco IOS Software para Catalyst 6500/6000 e Catalyst 4500/4000](#)

[Configuração do Cisco IOS Software para Catalyst 2900XL/3500XL, 2950 e 3550](#)

[Qual a diferença entre o protetor de BPDU STP e o protetor de raiz de STP?](#)

[O protetor de raiz ajuda com o problema de duas raízes?](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve os recursos aprimorados do protetor de raiz do STP que melhoram a confiabilidade, gerenciabilidade e segurança da rede comutada.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. 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 convenções de documentos.

Descrição do recurso

O STP padrão não fornece nenhum meio para que o administrador de rede aplique com segurança a topologia da rede da Camada 2 (L2) comutada. Um meio de aplicar a topologia pode ser especialmente importante em redes com controle administrativo compartilhado, onde diferentes entidades administrativas ou empresas controlam uma rede comutada.

A topologia de encaminhamento da rede comutada é calculada. O cálculo é baseado na posição da bridge raiz, entre outros parâmetros. Qualquer switch pode ser a bridge raiz em uma rede. Mas uma topologia de encaminhamento mais ideal coloca a bridge raiz em um local predeterminado específico. Com o STP padrão, qualquer bridge na rede com um ID de bridge mais baixo assume a função de bridge raiz. O administrador não pode impor a posição da bridge raiz.

Observação: o administrador pode definir a prioridade da bridge raiz como 0 em um esforço para proteger a posição da bridge raiz. Mas não há garantia contra uma bridge com prioridade 0 e um endereço MAC mais baixo.

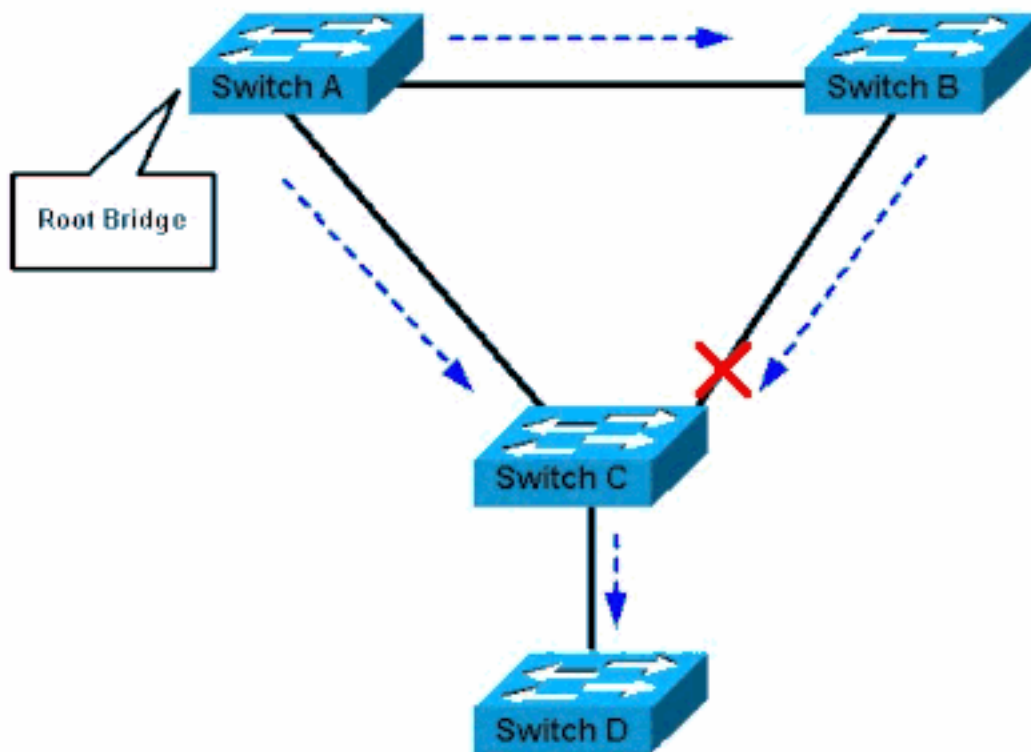
O recurso de protetor de raiz fornece uma maneira de aplicar a colocação da bridge raiz na rede.

O protetor de raiz garante que a porta na qual o protetor de raiz está habilitado seja a porta designada. Normalmente, as portas da bridge raiz são todas as portas designadas, a menos que duas ou mais portas da bridge raiz estejam conectadas juntas. Se a ponte receber Unidades de Dados de Protocolo de Ponte (BPDUs - Bridge Protocol Data Units) STP superiores em uma porta habilitada para protetor de raiz, o protetor de raiz moverá essa porta para um estado de STP de raiz inconsistente. Esse estado de raiz inconsistente é efetivamente igual a um estado de escuta. Nenhum tráfego é encaminhado através dessa porta. Dessa forma, o protetor de raiz reforça a posição da bridge raiz.

O exemplo nesta seção demonstra como uma bridge raiz invasora pode causar problemas na rede e como o protetor de raiz pode ajudar.

Na figura 1, os Switches A e B compõem o núcleo da rede e A é a bridge raiz de uma VLAN. Switch C is an access layer Switch. O link entre B e C está bloqueado no lado C. As setas mostram o fluxo de STP BPDUs.

Figure 1

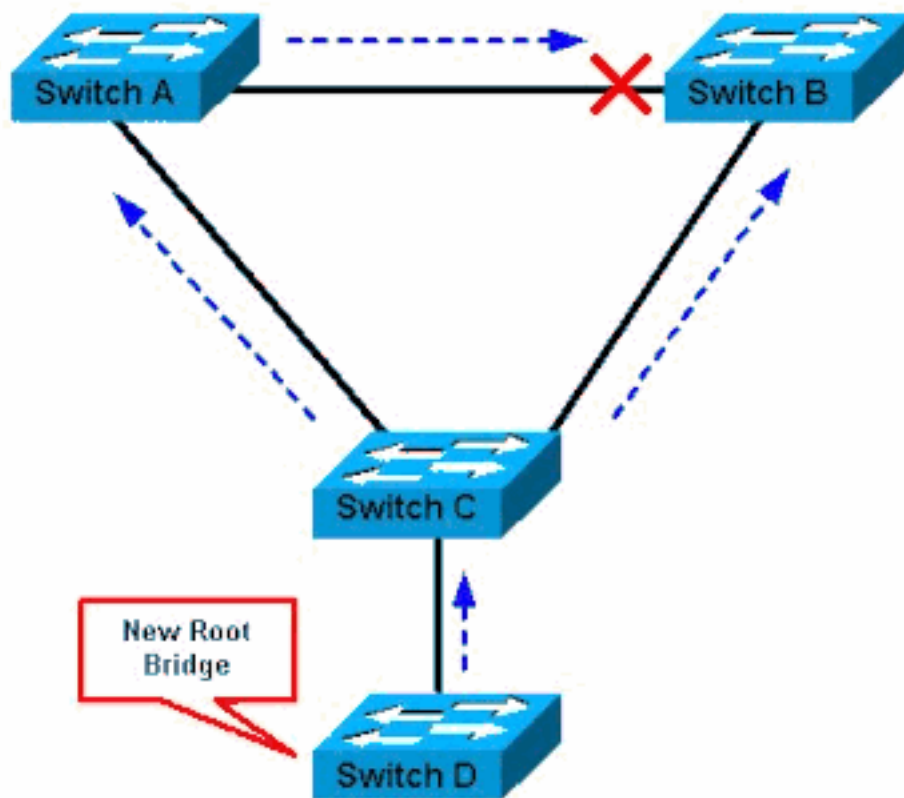


O switch A é a bridge raiz

Na Figura 2, o dispositivo D começa a participar do STP. Por exemplo, aplicativos de ponte baseados em software são iniciados em PCs ou outros switches que você conecta a uma rede de provedor de serviços. Se a prioridade da bridge D for 0 ou qualquer valor inferior à prioridade da bridge raiz, o dispositivo D será escolhido como bridge raiz para essa VLAN. Se o link entre os dispositivos A e B for de 1 gigabit e os links entre A e C, bem como entre B e C, forem de 100 Mbps, a escolha de D como raiz fará com que o link Gigabit Ethernet que conecta os dois switches centrais seja bloqueado.

Esse bloco faz com que todos os dados nessa VLAN fluam através de um link de 100 Mbps através da camada de acesso. Se mais dados fluem pelo núcleo nessa VLAN do que esse link pode acomodar, ocorre a queda de alguns quadros. O descarte de quadros leva a uma perda de desempenho ou a uma interrupção de conectividade.

Figure 2



O switch D é a nova bridge

raiz

O recurso de protetor de raiz protege a rede contra esses problemas.

A configuração do protetor de raiz é feita por porta. O protetor de raiz não permite que a porta se torne uma porta de raiz STP, portanto, a porta é sempre designada pelo STP. Se um BPDU melhor chegar a essa porta, o protetor de raiz não leva em conta o BPDU e elege uma nova raiz de STP. Em vez disso, o protetor de raiz coloca a porta no estado STP de raiz inconsistente. Você deve habilitar o protetor de raiz em todas as portas em que a bridge raiz não deve aparecer. De certa forma, você pode configurar um perímetro ao redor da parte da rede onde a raiz do STP pode ser localizada.

[Na Figura 2](#), ative o protetor de raiz na porta do Switch C que se conecta ao Switch D.

O Switch C [na Figura 2](#) bloqueia a porta que se conecta ao Switch D, depois que o switch recebe um BPDU superior. O protetor de raiz coloca a porta no estado STP de raiz inconsistente. Nenhum tráfego passa pela porta nesse estado. Depois que o dispositivo D deixar de enviar BPDUs superiores, a porta será desbloqueada novamente. Através do STP, a porta passa do estado de escuta para o estado de aprendizagem e, eventualmente, passa para o estado de encaminhamento. A recuperação é automática; nenhuma intervenção humana é necessária.

Esta mensagem aparece depois que o protetor de raiz bloqueia uma porta:

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in VLAN 77.
Moved to root-inconsistent state
```

Disponibilidade

O protetor de raiz está disponível no Catalyst 6500/6000 que executa o software do sistema Cisco

IOS®. Esse recurso foi introduzido pela primeira vez no Cisco IOS Software Release 12.0(7)XE. Para o Catalyst 4500/4000 que executa o software do sistema Cisco IOS, esse recurso está disponível em todas as versões.

Para os switches Catalyst 2900XL e 3500XL, o protetor de raiz está disponível no Cisco IOS Software Release 12.0(5)XU e posterior. Os switches da série Catalyst 2950 suportam o recurso de protetor de raiz no Cisco IOS Software Release 12.0(5.2)WC(1) e posterior. Os Catalyst 3550 Series Switches suportam o recurso de protetor de raiz no Cisco IOS Software Release 12.1(4)EA1 e posterior.

Esse recurso também está disponível nos switches Cisco Catalyst Series mais recentes.

Configuração

Configuração do Cisco IOS Software para Catalyst 6500/6000 e Catalyst 4500/4000

Nos Catalyst 6500/6000 ou Catalyst 4500/4000 Switches com Cisco IOS System Software, execute este conjunto de comandos para configurar o protetor de raiz STP:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
!
Switch#(config)#interface fastethernet 3/1
Switch#(config-if)#spanning-tree guard root
!
```

Observação: o Cisco IOS Software Release 12.1(3a)E3 para o Catalyst 6500/6000 que executa o Cisco IOS System Software alterou esse comando de **spanning-tree rootguard** para **spanning-tree guard root**. O Catalyst 4500/4000 que executa o software de sistema Cisco IOS usa o comando **spanning-tree guard root** em todas as versões.

Configuração do Cisco IOS Software para Catalyst 2900XL/3500XL, 2950 e 3550

No Catalyst 2900XL, 3500XL, 2950 e 3550, configure switches com protetor de raiz no modo de configuração de interface, como mostra este exemplo:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 0/8
Switch(config-if)# spanning-tree rootguard
Switch(config-if)# ^Z
*Mar 15 20:15:16: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Rootguard enabled on
port FastEthernet0/8 VLAN 1.
Switch#
```

Qual a diferença entre o protetor de BPDU STP e o protetor de raiz de STP?

A guarda BPDU e a guarda de raiz são semelhantes, mas seu impacto é diferente. O protetor de BPDU desabilitará a porta, após a recepção do BPDU, se portfast estiver habilitado na porta. A desativação impede efetivamente que os dispositivos por trás dessas portas participem do STP.

Você deve reabilitar manualmente a porta que é colocada no estado errdisable ou configurar **errdisable-timeout** .

O protetor de raiz permite que o dispositivo participe do STP desde que o dispositivo não tente se tornar a raiz. Se o protetor de raiz bloquear a porta, a recuperação subsequente será automática. A recuperação ocorre assim que o dispositivo desviante deixa de enviar BPDUs superiores.

Para obter mais informações sobre o BPDU guard, consulte [Melhoria do Spanning Tree PortFast BPDU Guard](#).

O protetor de raiz ajuda com o problema de duas raízes?

Pode haver uma falha de link unidirecional entre duas bridges em uma rede. Devido à falha, uma ponte não recebe as BPDUs da ponte raiz. Com tal falha, o switch raiz recebe quadros que outros switches enviam, mas os outros switches não recebem as BPDUs que o switch raiz envia. Isso pode levar a um loop de STP. Como os outros switches não recebem BPDUs da raiz, eles acreditam que são a raiz e começam a enviar BPDUs.

Quando a bridge raiz real começa a receber BPDUs, a raiz descarta os BPDUs porque eles não são superiores. A bridge raiz não muda. Portanto, o protetor de raiz não ajuda a resolver esse problema. Os recursos UniDirectional Link Detection (UDLD) e loop guard tratam desse problema.

Para obter mais informações sobre cenários de falha de STP e como solucioná-los, consulte [Problemas do Spanning Tree Protocol e Considerações de Projeto Relacionadas](#).

Informações Relacionadas

- [Entender e configurar o recurso de protocolo UDLD](#)
- [Recuperar o Estado da Porta Errdisable nas Plataformas Cisco IOS](#)
- [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.