

Entender os recursos de proteção de loop e UDLD do STP

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Disponibilidade de recursos](#)

[Funções da porta STP](#)

[Guarda de circuito de STP](#)

[Descrição do recurso](#)

[Considerações sobre configuração](#)

[Proteção de loop versus UDLD](#)

[Interoperabilidade de proteção de loop com outros recursos STP](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve os recursos do Spanning Tree Protocol que visam melhorar a estabilidade da rede da Camada 2.

Pré-requisitos

Requisitos

Este documento pressupõe que o leitor está familiarizado com a operação básica do STP. Consulte [Compreender e Configurar o Spanning Tree Protocol \(STP\) em Catalyst Switches](#) para obter mais informações.

Componentes Utilizados

Este documento baseia-se nos switches Catalyst, no entanto, a disponibilidade dos recursos descritos pode depender da versão de software usada.

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

O Spanning Tree Protocol (STP) resolve fisicamente topologias redundantes em topologias em formato de árvores sem loops. O maior problema com o STP é que algumas falhas de hardware podem fazer com que ele falhe.

Esta falha cria loops de encaminhamento (ou loops do STP). As indisponibilidades principais da rede são causadas por loops do STP.

Este documento descreve o recurso STP com proteção de loop que se destina a melhorar a estabilidade das redes de Camada 2.

Este documento também descreve a detecção de desvio da Bridge Protocol Data Unit (BPDU). A detecção de desvio de BPDU é um recurso de diagnóstico que gera mensagens de syslog, quando as BPDUs não são recebidas a tempo.

Disponibilidade de recursos

Cisco IOS

- O recurso de proteção de loop do STP foi introduzido no software Cisco IOS® versão 12.1(12c)EW para switches Catalyst 4500 e no software Cisco IOS versão 12.1(11b)EX para Catalyst 6500.

Funções da porta STP

Internamente, o STP atribui a cada porta de ponte (ou switch) uma função que se baseia em configuração, topologia, posição relativa da porta na topologia e outras considerações.

A função da porta define o comportamento da porta sob o ponto de vista STP. De acordo com a função da porta, a porta envia ou recebe BPDUs do STP e encaminha ou bloqueia o tráfego de dados.

Esta lista fornece um breve resumo de cada função da porta STP:

- Designada – Uma porta designada é eleita por link (segmento). A porta designada é a porta mais próxima da ponte de origem. Essa porta envia as BPDUs no link (segmento) e encaminha o tráfego para a ponte de origem. Em uma rede convergente STP, cada porta designada está no estado de encaminhamento STP.
- Origem – A ponte pode ter apenas uma porta de origem. A porta de origem é a porta que leva à ponte de origem. Em uma rede convergente STP, a porta de origem está no estado

de encaminhamento STP.

- Alternativa – As portas alternativas levam à ponte de origem, mas não são portas de origem. As portas alternadas mantêm o estado de bloqueio de STP.
- Backup – Este é um caso especial, quando duas ou mais portas entre os mesmos switches estão conectadas entre si, diretamente ou por meio de mídia compartilhada. Nesse caso, uma porta é designada, e o restante das portas é bloqueado. A função dessa porta é de backup.

Guarda de circuito de STP

Descrição do recurso

O recurso do protetor de loop STP fornece proteção adicional contra loops de encaminhamento da Camada 2 (laços STP). Um loop STP é criado quando uma porta de bloqueio STP de uma topologia redundante faz a transição erroneamente para o estado de encaminhamento.

Isso costuma acontecer porque uma das portas de uma topologia fisicamente redundante (não necessariamente a porta de bloqueio de STP) não recebe mais BPDUs de STP. Nessa operação, o STP depende da recepção contínua ou da transmissão dos BPDUs com base na função da porta.

A porta designada transmite BPDUs e a porta não designada recebe BPDUs.

Quando uma das portas em uma topologia fisicamente redundante não recebe mais BPDUs, o STP concebe que a topologia está livre de loops. Eventualmente, a porta de bloqueio da porta de backup ou de substituição é designada muda para um estado de encaminhamento. Esta situação cria um loop.

O recurso protetor de loop faz verificações adicionais. Se os BPDUs não são recebidos em uma porta não designada, e o protetor de loop está habilitado, a porta muda para o estado de bloqueio inconsistente de loop de STP, em vez do estado de escuta/aprendizagem/ encaminhamento.

Sem o recurso protetor de loop, a porta assume a função de porta designada. A porta muda para o estado de encaminhamento STP e cria um loop.

Quando a proteção de loop bloqueia uma porta inconsistente, esta mensagem é registrada:

- Cisco IOS

```
%SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port FastEthernet0/24 on VLAN0050.
```

Depois que a BPDUs é recebida em uma porta em um estado de STP inconsistente de loop, a porta muda para outro estado de STP. Para a BPDUs recebida, isso significa que a recuperação é

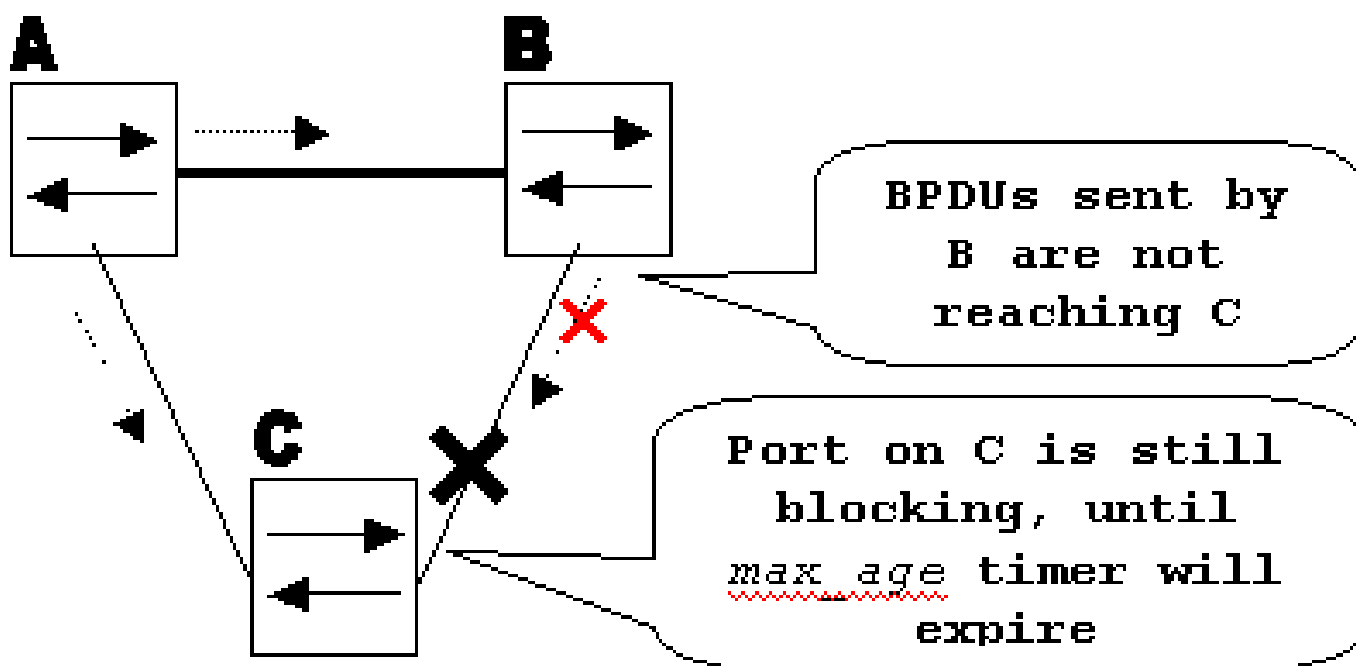
automática e uma intervenção não é necessária. Após a recuperação, esta mensagem é registrada:

- Cisco IOS

```
%SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port FastEthernet0/24 on VLAN0050.
```

Considere este exemplo para ilustrar esse comportamento:

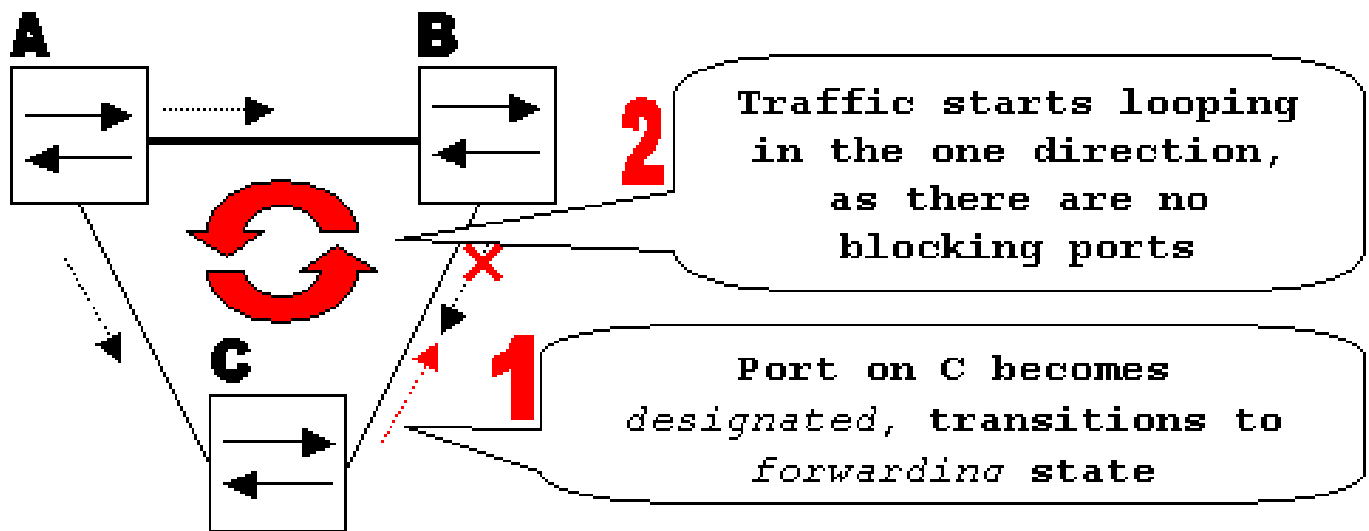
O Switch A é o Switch-raiz. O switch C não recebe BPDUs do switch B devido à falha do link unidirecional no link entre o switch B e o switch C.



Falha no link unidirecional

Sem a proteção de loop, a porta de bloqueio de STP no switch C passa para o estado de escuta de STP quando o temporizador de `max_age` expira e, em seguida, muda para o estado de encaminhamento em duas vezes o tempo de `forward_delay`.

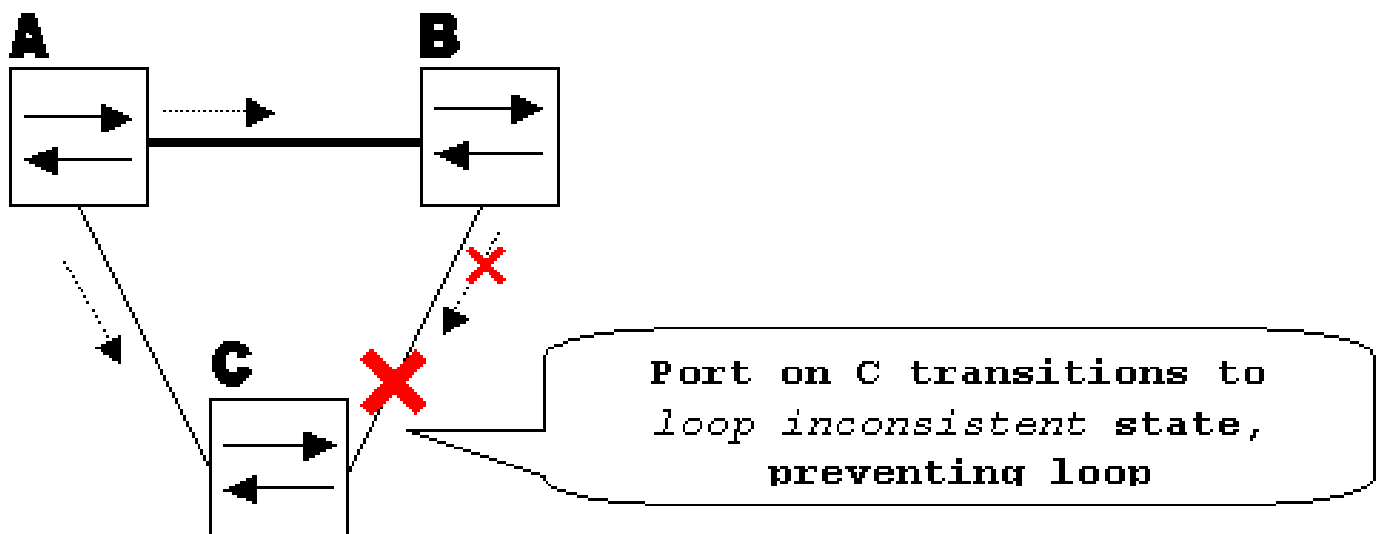
Esta situação cria um loop.



O loop foi criado

Com a proteção de loop ativada, a porta de bloqueio no switch C passa para o estado inconsistente de loop de STP quando o temporizador de max_age expira.

Uma porta no estado inconsistente de loop de STP não passa pelo tráfego de usuário. Portanto, um loop não é criado. (O estado inconsistente de loop é efetivamente igual ao estado de bloqueio.)



A proteção de loop ativada impede o loop

Considerações sobre configuração

O recurso de proteção de loop é ativado por porta. Porém, enquanto bloqueia a porta no nível de STP, a proteção de loop bloqueia portas inconsistentes por VLAN (devido ao STP por VLAN).

Ou seja, se as BPDUs não forem recebidas na porta de tronco para apenas uma VLAN específica, somente essa VLAN será bloqueada (movidada para o estado de STP inconsistente de loop).

Pelo mesmo motivo, se ativado em uma interface EtherChannel, todo o canal será bloqueado para uma VLAN específica, não apenas um link (porque o EtherChannel é considerado uma porta lógica da perspectiva do STP).

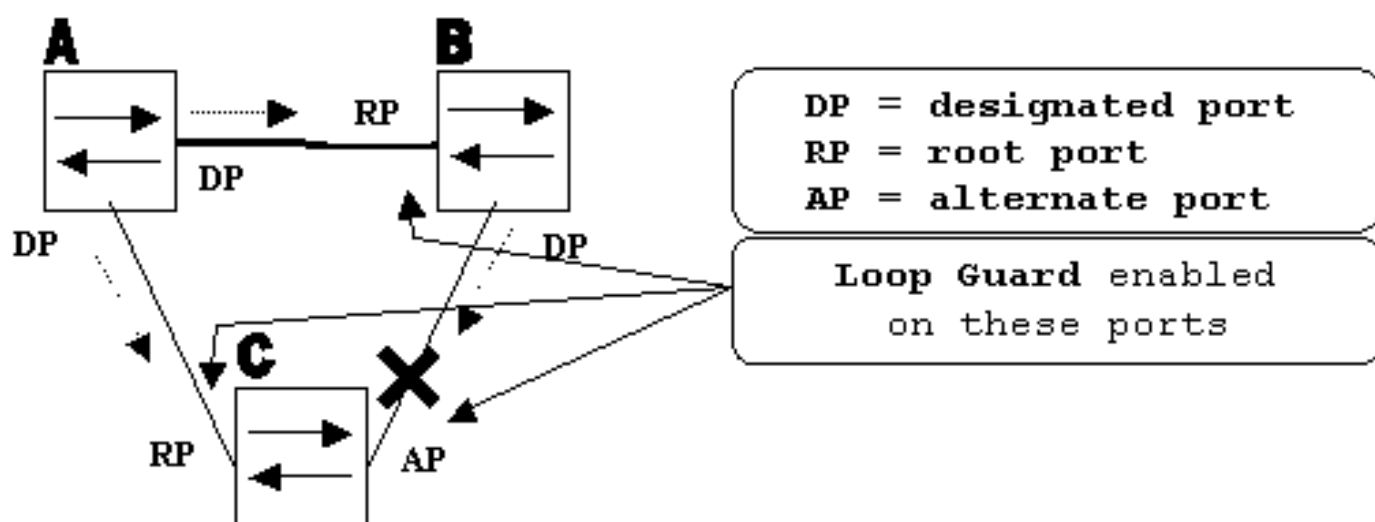
Em quais portas a proteção de loop deve ser ativada? A resposta mais evidente é nas portas de bloqueio. No entanto, isso não está totalmente correto.

A proteção de loop deve ser ativada nas portas não designadas (mais precisamente, nas portas de origem e alternativas) para todas as combinações possíveis de topologias ativas.

Contanto que a proteção de loop não seja um recurso por VLAN, a mesma porta (de tronco) pode ser designada para uma VLAN e não designada para a outra.

Os possíveis cenários de failover também devem ser considerados.

Exemplo



Portas com a proteção de loop ativada

Por padrão, a proteção de loop fica desativada. Este comando é usado para ativar a proteção de loop:

- Cisco IOS

```
<#root>
```

```
spanning-tree guard loop
```

```
Router(config)#
```

```
interface gigabitEthernet 1/1
```

```
Router(config-if)#
```

```
spanning-tree guard loop
```

De forma eficaz, a proteção de loop pode ser ativada em todos os links ponto a ponto. O link ponto a ponto é detectado pelo status duplex do link. Se o duplex estiver cheio, o link será considerado ponto a ponto. Ainda é possível definir ou substituir as configurações globais por porta.

Emita este comando para ativar a proteção de loop globalmente:

- Cisco IOS

```
<#root>  
Router(config)#  
spanning-tree loopguard default
```

Emita este comando para desativar a proteção de loop:

- Cisco IOS

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

Emita este comando para desativar globalmente a proteção de loop:

- Cisco IOS

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

Emita este comando para verificar o status da proteção de loop:

- Cisco IOS

```
<#root>  
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

Proteção de loop versus UDLD

As funcionalidades de proteção de loop e Unidirecional Link Detection (UDLD) são sobrepostas, em parte no sentido de que ambas protegem contra falhas de STP causadas por links unidirecionais. No entanto, esses dois recursos são diferentes quanto à funcionalidade e forma como abordam o problema.

Esta tabela descreve a funcionalidade de proteção de loop e de UDLD:

Funcionalidade	Protetor de loop	UDLD
Configuração	Por porta	Por porta
Granularidade de ação	Por VLAN	Por porta
Recuperação automática	Yes	Sim, com o recurso de limite de tempo err-disable
Proteção contra falhas de STP causadas por links unidirecionais	Sim, quando ativado em todas as portas de origem e alternativas na topologia redundante	Sim, quando ativado em todos os links na topologia redundante
Proteção contra falhas de STP causadas por problemas no software (o switch designado não envia a BPDU)	Yes	No
Proteção contra fiação incorreta.	No	Yes

Com base nas várias considerações de projeto, você pode escolher a UDLD ou o recurso de proteção de loop. Em relação ao STP, a diferença mais perceptível entre os dois recursos é a ausência de proteção na UDLD contra falhas de STP causadas por problemas no software.

Como resultado, o switch designado não envia as BPDUs. No entanto, esse tipo de falha é (por ordem de magnitude) mais raro do que as falhas causadas por links unidirecionais. Em

contrapartida, a UDLD pode ser mais flexível no caso de links unidirecionais no EtherChannel.

Nesse caso, a UDLD desativa apenas os links com falha e o canal pode permanecer funcional com os links que permanecem. Nessa falha, a proteção de loop entra no estado inconsistente de loop para bloquear todo o canal.

Adicionalmente, a proteção de circuito não funciona em enlaces compartilhados ou em situações nas quais o enlace é unidirecional desde a conexão. No último caso, a porta nunca recebe a BPDU e é designada.

Como esse comportamento pode ser normal, a proteção de loop não abrange esse caso específico. A UDLD oferece proteção contra esse cenário.

Conforme descrito, o mais alto nível de proteção é fornecido quando você ativa a UDLD e a proteção de loop.

Interoperabilidade de proteção de loop com outros recursos STP

protetor de raiz

A proteção de origem é mutuamente exclusiva com a proteção de loop. A proteção de origem é usada nas portas designadas e não permite que a porta se torne não designada.

A proteção de loop funciona nas portas não designadas e não permite que a porta seja designada até a expiração de `max_age`. O protetor de raiz não pode estar habilitado na mesma porta da proteção do loop.

Quando a proteção de loop é configurada na porta, ela desativa a proteção de origem configurada na mesma porta.

Uplink fast e backbone fast

Tanto o uplink fast como o backbone fast são transparentes para o protetor do circuito. Quando `max_age` é ignorado pelo backbone fast no momento da reconvergência, ele não aciona a proteção de loop.

Para obter mais informações sobre uplink fast e backbone fast, consulte estes documentos:

- [Entendendo e configurando o recurso Cisco Uplink Fast](#)
- [Entender e configurar o backbone fast nos switches Catalyst](#)

Protetor de BPDU e PortFast e VLAN dinâmica

A proteção de loop não pode ser ativada para portas em que o portfast está ativado. Como a proteção de BPDU funciona em portas ativadas para portfast, algumas restrições se aplicam à proteção de BPDU.

A proteção de loop não pode ser ativada nas portas de VLAN dinâmicas, pois essas portas têm o portfast ativado.

Enlaces compartilhados

A proteção de loop não deve ser ativada em links compartilhados. Se você ativar a proteção de loop em links compartilhados, o tráfego dos hosts conectados aos segmentos compartilhados poderá ser bloqueado.

MST (extensão de árvore múltipla)

A proteção de loop funciona corretamente no ambiente MST.

Informações Relacionadas

- [Aprimorar o Spanning Tree Protocol \(STP\) com a proteção de origem](#)
- [Configurar o recurso do protocolo UDLD](#)
- [Utilização de Portfast e outros comandos para reparar retardos de conectividade da inicialização de estação de trabalho](#)
- [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.