# Solucionar problemas de STP e considerações de design relacionadas

## Contents

# Introdução

Este documento descreve recomendações para implementar uma rede segura sobre como fazer bridging de switches Cisco Catalyst que executam o Catalyst OS/Cisco IOS® Software.

# Pré-requisitos

## Requisitos

Não existem requisitos específicos para este documento.

## Componentes Utilizados

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

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.

## Informações de Apoio

Este documento discute alguns dos motivos comuns do Spanning Tree Protocol (STP) poder falhar e quais informações procurar para identificar a origem do problema. Ele também mostra o tipo de design que minimiza problemas relacionados ao spanning tree e é fácil de solucionar problemas.

Este documento não aborda a operação básica do STP. Para saber como funciona o STP, consulte este documento:

- Entendendo e configurando o protocolo de árvore de abrangência (STP) em Switches Catalyst

Este documento não aborda o Rapid STP (RSTP), definido no IEEE 802.1w. Além disso, este documento não aborda o protocolo Multiple Spanning Tree (MST), definido no IEEE 802.1s. Para obter mais informações sobre RSTP e MST, consulte estes documentos:

- Compreendendo o protocolo múltiplo de extensão de árvore (802.1s)
- Compreendendo o protocolo de abrangência de árvore rápida (802.1w)

Para obter um documento de solução de problemas de STP mais específico para switches Catalyst que executam o software Cisco IOS, consulte o documento Solução de problemas de

STP no switch Catalyst que executa o Cisco IOS integrado (modo nativo).

# Falha do Spanning Tree Protocol

A função principal do algoritmo Spanning-Tree (STA) é eliminar os loops criados por links redundantes nas redes de ponte. O STP opera na Camada 2 do modelo OSI. Por meio das BPDUs (bridge protocol data units, unidades de dados do protocolo de ponte) trocadas entre pontes, o STP escolhe as portas que eventualmente encaminham ou bloqueiam o tráfego. Esse protocolo pode falhar em alguns casos específicos e solucionar problemas da situação que pode ser muito difícil, o que depende do projeto da rede. Nessa área específica, você executa a parte mais importante do processo de solução de problemas antes que o problema ocorra.

Geralmente, uma falha no STA leva a um loop de ponte. A maioria dos clientes que acionam o Suporte técnico da Cisco para problemas de Spanning Tree suspeita de bug, mas raramente um bug é a causa. Mesmo que o software seja o problema, um Loop de Bridging em um ambiente STP ainda virá de uma porta que pode bloquear, mas encaminha o tráfego.

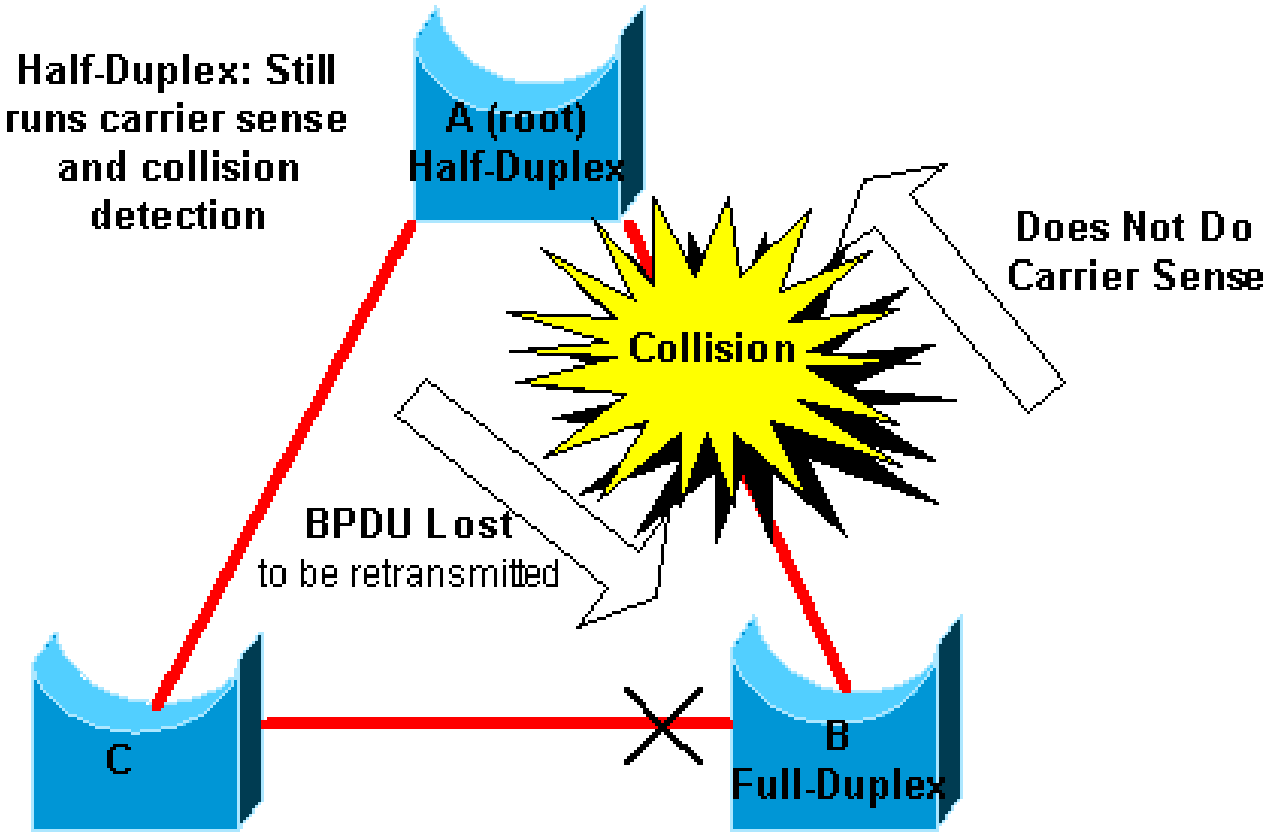
## Convergência de árvore de abrangência

Consulte o vídeo do Spanning Tree para ver um exemplo que explica a convergência inicial do Spanning Tree. O exemplo também explica por que uma porta bloqueada entra no modo de encaminhamento devido a uma perda excessiva de BPDUs, resultando em falha de STA.

O resto desse documento enumera as diferentes situações que podem provocar a falha do STA. A maioria dessas falhas está relacionada a uma perda considerável de BPDUs. A perda faz com que as portas bloqueadas migrem para o modo de encaminhamento.

## Incompatibilidade duplex

A incompatibilidade de duplex em um link ponto a ponto é um erro de configuração muito comum. Se você definir manualmente o modo duplex como Full em um lado do link e deixar o outro lado no modo de negociação automática, o link terminará em half-duplex. (Uma porta com o modo duplex definido como Full não negocia mais.)




O cenário do pior caso é quando o modo duplex de uma ponte que envia BPDUs é definido como half-duplex em uma porta, mas o modo duplex da porta do par em outra extremidade do link é definido como full-duplex. No exemplo anterior, a incompatibilidade bidirecional no link entre as pontes A e B pode facilmente levar a um loop de Bridging. Como a ponte B foi configurada para full-duplex, ela não realiza a verificação de operadora antes do acesso ao link. A ponte B começa a enviar quadros mesmo que a ponte A já use o link. Essa situação é um problema para A; a bridge A detecta uma colisão e executa o algoritmo de backoff antes que a bridge tente outra transmissão do quadro. Se houver tráfego suficiente de B para A, cada pacote que A enviar, que inclui as BPDUs, passará por adiamento ou colisão e eventualmente será descartado. Do ponto de vista do STP, como a ponte B não recebe mais as BPDUs da ponte A, a ponte B perdeu a ponte de origem. Isso faz com que a ponte B desbloqueie a porta conectada à ponte C, que cria o loop.

Sempre que existe uma incompatibilidade de duplex, essas mensagens de erro aparecem nos consoles dos switches Catalyst que executam o CatOs e o software Cisco IOS:

CatOS

```
CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port [mod]/[port]
```

Cisco IOS Software

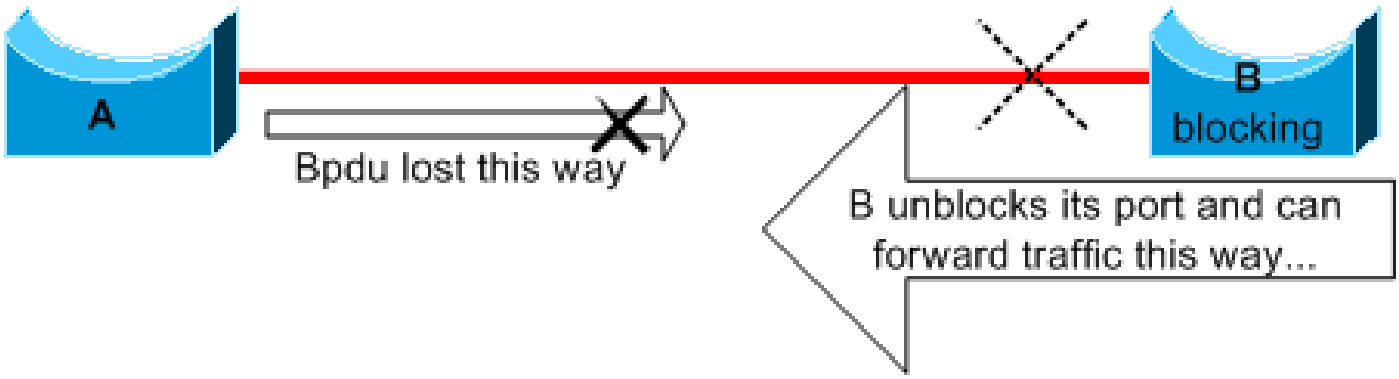
```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half
duplex), with TBA05071417(Cat6K-B) 4/1 (half duplex).
```

Verifique as configurações de duplex e, se houver incompatibilidade na configuração de duplex, defina a configuração corretamente.

Para obter mais informações sobre como solucionar os problemas de incompatibilidade de duplex, consulte o documento Configuração e solução de problemas da negociação automática Half/Full Duplex 10/100/1000Mb Ethernet.

## Link unidirecional

Links unidirecionais são uma causa comum de um Loop de Bridging. Nos links de fibra, uma falha sem detecção geralmente causa links unidirecionais. Outra causa é um problema em um transceptor. Tudo o que pode levar um link a ficar ativo e fornecer uma comunicação unidirecional é muito perigoso em relação ao STP. Este exemplo esclarece:




Suponha que o link entre A e B seja unidirecional. O link descarta o tráfego de A para B, enquanto o link transmite o tráfego de B para A. Imagine que a ponte B seja bloqueada antes que o link se torne unidirecional. No entanto, uma porta só poderá ser bloqueada se receber as BPDUs de uma ponte com prioridade mais alta. Como, nesse caso, todas as BPDUs provenientes de A são perdidas, a porta da ponte B eventualmente migra para A para o estado de encaminhamento e encaminha o tráfego. Isso cria um loop. Se essa falha existir na inicialização, a convergência de STP não ocorrerá corretamente. No caso de uma incompatibilidade bidirecional, uma reinicialização ajuda temporariamente; mas, nesse caso, uma reinicialização das pontes não tem efeito algum.

Para detectar os links unidirecionais antes da criação do loop de encaminhamento, a Cisco desenvolveu e implementou o protocolo UDLD (UniDirectional Link Detection ). Esse recurso pode detectar cabeamento incorreto ou links unidirecionais na Camada 2 e interromper automaticamente os loops resultantes ao desativar algumas portas. Execute o UDLD sempre que possível em um ambiente de ponte.

Para obter mais informações sobre o uso do UDLD, consulte o documento Noções básicas e configuração do recurso do protocolo UDLD.

## Corrupção de pacotes

A corrupção do pacote também pode causar o mesmo tipo de falha. Se um link tiver uma taxa alta de erros físicos, você poderá perder um determinado número de BPDUs consecutivas. Essa perda pode levar uma porta de bloqueio a migrar para o estado de encaminhamento. Você não vê esse caso com muita frequência, pois os parâmetros padrão do STP são muito conservadores. A porta de bloqueio precisa perder as BPDUs por 50 segundos, antes da transição para o encaminhamento. A transmissão bem-sucedida de uma única BPDU interrompe o loop. Esse caso normalmente ocorre com o ajuste descuidado dos parâmetros de STP. Um exemplo de ajuste é a redução da idade máxima.

Incompatibilidade de duplex, cabos danificados ou comprimento de cabo incorreto pode corromper os pacotes. Consulte o documento Solução de problemas da porta do switch e problemas de interface para obter uma explicação sobre a saída do contador de erros do CatOS e do software Cisco IOS.

## Erros de recursos

O STP é implementado no software, até mesmo nos switches avançados que realizam a maioria das funções de switching no hardware com circuitos integrados específicos de aplicação (ASICs). Se por alguma razão houver uma superutilização da CPU da ponte, os recursos poderão ser inadequados para a transmissão das BPDUs. Geralmente, o STA não apresenta processamento intenso e tem prioridade sobre outros processos. A seção Procurar erros de recurso deste documento fornece algumas diretrizes sobre o número de instâncias de STP que podem ser resolvidas por uma plataforma específica.

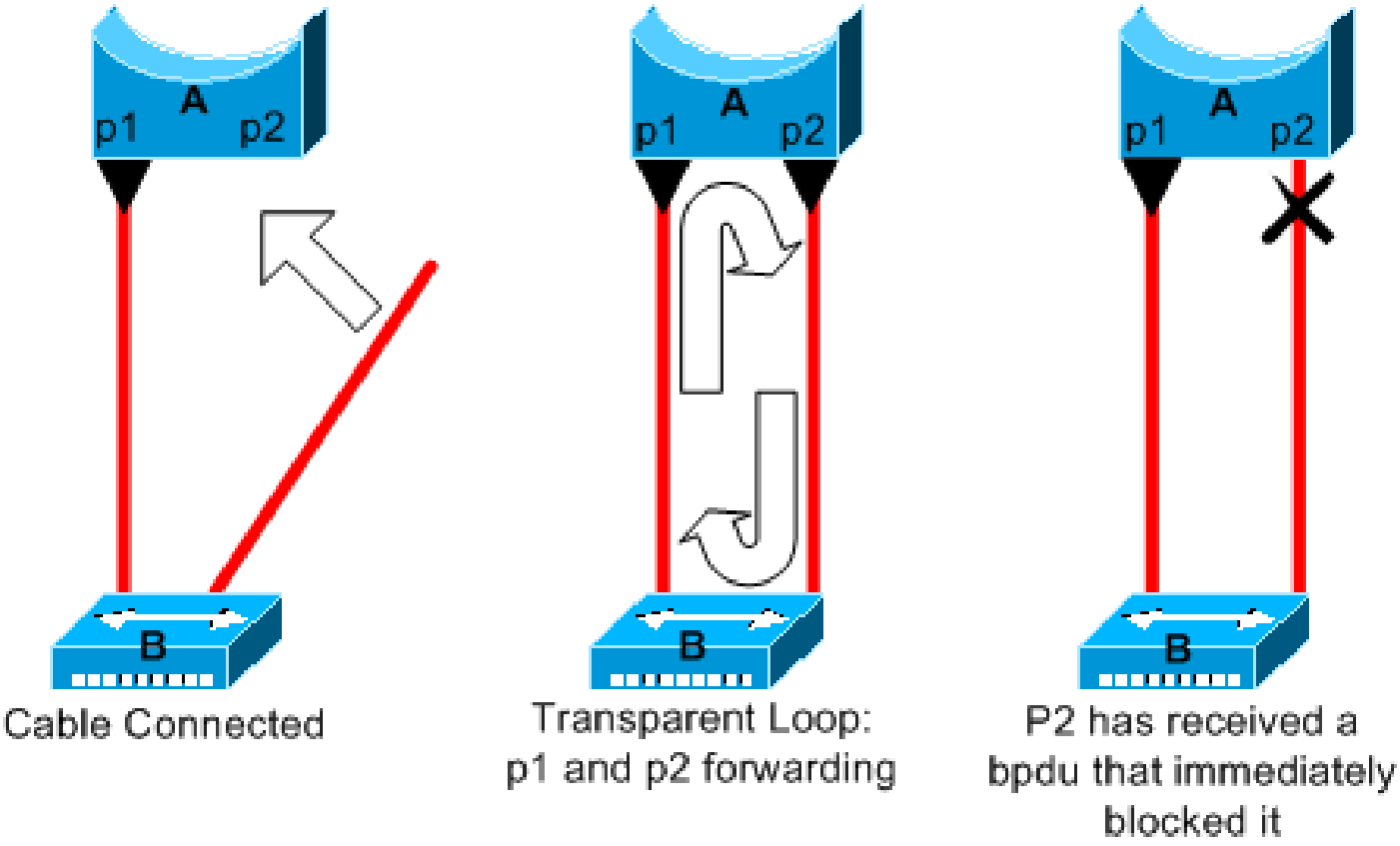
## Erro de configuração de PortFast

PortFast é um recurso que você normalmente ativa apenas para uma porta ou interface que é conectada a um host. Quando o link se torna ativo nesta porta, a ponte ignora os primeiros estágios do STA e migra diretamente para o modo de encaminhamento.

---

> Cuidado: não use o recurso PortFast em portas de switch ou interfaces que se conectam a outros switches, hubs ou roteadores. Caso contrário, você pode criar um loop de rede.

---




Neste exemplo, o dispositivo A é uma ponte com a porta p1 já no estado de encaminhamento. A porta p2 tem uma configuração PortFast. O dispositivo B é um hub. Assim que você conecta o segundo cabo à porta A, a porta p2 entra no modo de encaminhamento e cria um loop entre p1 e p2. Esse loop é interrompido assim que p1 ou p2 recebe uma BPDU que coloca uma dessas duas portas no modo de bloqueio. Mas há um problema nesse tipo de loop transitório. Se o tráfego em loop é muito intenso, a ponte pode ter problemas na transmissão bem-sucedida da BPDU que interrompe o loop. Esse problema pode atrasar consideravelmente a convergência ou derrubar a rede em casos extremos.

Para obter mais informações sobre o uso correto do PortFast em switches que executam o CatOs e o software Cisco IOS, consulte o documento Uso de PortFast e outros comandos para corrigir os atrasos de conectividade na inicialização do local de trabalho.

Mesmo com a configuração PortFast, a porta ou a interface ainda participa do STP. Se um switch com uma ponte de menor prioridade do que a ponte de origem ativa no momento for conectado a uma porta ou interface configurada com PortFast, ele poderá ser eleito como a ponte de origem. Essa alteração da ponte de origem pode afetar adversamente a topologia do STP ativo e fazer com que a rede fique abaixo do ideal. Para evitar essa situação, a maioria dos switches Catalyst que executam o CatOs e o software Cisco IOS tem um recurso chamado BPDU Guard. O BPDU Guard desativa uma porta ou interface configurada com PortFast, se a porta ou interface recebe uma BPDU.

Para obter mais informações sobre o uso do recurso BPDU Guard nos switches que executam o CatOs e o software Cisco IOS, consulte o documento Aprimoramento do BPDU Guard PortFast do Spanning Tree.

## Problemas de ajuste e diâmetro de parâmetros de STP inadequados

Um valor agressivo para o parâmetro de idade máxima e o atraso de encaminhamento podem causar uma topologia de STP muito instável. Nesses casos, a perda de algumas BPDUs pode causar um loop. Outro problema que não é bem conhecido está relacionado ao diâmetro da rede de ponte. Os valores padrão conservadores dos temporizadores de STP impõem um diâmetro máximo de rede igual a sete. Esse diâmetro máximo de rede restringe a distância entre as outras pontes na rede. Nesse caso, duas pontes diferentes não podem estar a mais de sete saltos de distância uma da outra. Parte dessa restrição vem do campo de idade que os BPDUs carregam.

Quando uma BPDU é propagada da ponte de origem em direção às folhas da árvore, o campo de idade aumenta cada vez que a BPDU passa por uma ponte. Eventualmente, a ponte descarta a BPDU quando o campo de idade excede a idade máxima. Se a raiz estiver muito longe de algumas pontes da rede, esse problema poderá ocorrer. Esse problema afeta a convergência do Spanning Tree.

Tome muito cuidado se estiver planejando alterar o valor padrão dos temporizadores do STP. É perigoso tentar obter uma convergência mais rápida dessa forma. Uma alteração no temporizador de STP tem um impacto no diâmetro da rede e na estabilidade do STP. Você pode alterar a prioridade da ponte para selecionar a ponte de origem e mudar o custo da porta ou o parâmetro de prioridade para controlar a redundância e o balanceamento de carga.

O software Cisco Catalyst fornece macros que ajustam perfeitamente os parâmetros de STP mais importantes para você:

- O **set spantree root [secondary]** macro diminui a prioridade da bridge para que ela se torne raiz (ou raiz alternativa). Uma opção adicional está disponível para esse comando que resulta no ajuste dos temporizadores de STP, especificando o diâmetro da rede. Mesmo quando realizado de forma correta, o ajuste do temporizador não melhora significativamente o tempo de convergência e apresenta alguns riscos de instabilidade na rede. Além disso, esse tipo de ajuste deve ser atualizado toda vez que um dispositivo for adicionado à rede. Mantenha os valores padrão conservadores, que são familiares para os engenheiros de rede.

- O **set spantree uplinkfast** para CatOS ou o **spanning-tree uplinkfast** para o Cisco IOS Software aumenta a prioridade do switch para que o switch não possa ser raiz. O comando aumenta o tempo de convergência do STP no caso de uma falha de uplink. Use esse comando em um switch de distribuição com conexão dupla para alguns switches de núcleo. Consulte o documento Noções básicas e configuração do recurso UplinkFast da Cisco.

- O **set spantree backbonefast enable** para CatOS ou o **spanning-tree backbonefast** para o Cisco IOS Software pode aumentar o tempo de convergência de STP do switch no caso de uma falha indireta de link. BackboneFast é um recurso proprietário da Cisco. Consulte o documento Noções básicas e configuração do Backbone Fast nos switches Catalyst.

Para obter mais informações sobre os temporizadores de STP e as regras para ajustá-los quando absolutamente necessário, consulte o documento Noções básicas e ajuste dos temporizadores do protocolo do Spanning Tree.

### Erros do software

Como mencionado na Introdução, o STP é um dos primeiros recursos implementados nos produtos da Cisco. Espera-se que este recurso seja muito estável. Somente a interação com os recursos mais recentes, como EtherChannel, causou a falha do STP em alguns casos muito específicos, que agora foram resolvidos. Uma série de fatores diferentes pode causar um bug de software e ter diversos efeitos. Não há como descrever corretamente os problemas que um bug pode apresentar. A situação mais perigosa que surge dos erros de software é se você ignorar algumas BPDUs ou se tiver uma transição de porta de bloqueio para encaminhamento.

## Solucionar o problema de uma falha

Infelizmente, não há um procedimento sistemático para solucionar um problema de STP. No entanto, esta seção resume algumas das ações disponíveis para você. A maioria das etapas nesta seção se aplica à solução de problemas de loops de ponte em geral. Você pode usar uma abordagem mais convencional para identificar outras falhas do STP que levam a uma perda de conectividade. Por exemplo, você pode explorar o caminho percorrido pelo tráfego que apresenta um problema.

---

> Observação: a maioria dessas etapas para solucionar problemas pressupõe a conectividade com os diferentes dispositivos da rede de bridge. Essa conectividade significa que você tem acesso ao console. Durante um loop de Bridging, por exemplo, você provavelmente não poderá fazer uma conexão Telnet.

---

Se você tiver a saída de um **show-tech support** do seu dispositivo Cisco, você pode usar o Cisco CLI Analyzer (somente clientes registrados) para exibir problemas potenciais e correções.

### Utilizar o diagrama da rede

Antes de solucionar os problemas de um loop de ponte, você precisa conhecer esses itens, no mínimo:

- A topologia da rede de ponte
- O local da ponte de origem
- O local das portas bloqueadas e os links redundantes

No mínimo, esse conhecimento é essencial pelos dois motivos a seguir:

- Para saber o que corrigir na rede, você precisa saber a aparência da rede quando ela funciona corretamente.
- A maioria das etapas para solucionar problemas é usar **show** para tentar identificar condições de erro. O conhecimento sobre a rede ajuda você a dar ênfase às portas principais dos dispositivos-chave.

## Identificar um Loop de Bridging

Anteriormente, um congestionamento de transmissões poderia ter um efeito desastroso na rede. Hoje, com os links e dispositivos de alta velocidade que fornecem switching no nível de hardware, não é provável que um único host (por exemplo, um servidor) derrube uma rede por meio de transmissões. A melhor maneira de identificar um loop de ponte é capturar o tráfego em um link saturado e verificar se você vê pacotes semelhantes várias vezes. Realisticamente, no entanto, se todos os usuários de determinado domínio da ponte tiverem problemas de conectividade ao mesmo tempo, você já pode suspeitar de um loop de ponte.

Verifique a utilização de portas nos dispositivos e procure valores anormais. Consulte a seção Verificar a utilização da porta deste documento.

Nos Catalyst Switches que executam CatOS, você pode verificar facilmente o uso geral do painel traseiro com o comando **show system** comando. O comando fornece o uso atual do painel traseiro do switch e também especifica o uso máximo e o uso da data de pico. Uma utilização de pico incomum mostra se já houve um loop de ponte neste dispositivo.

## Restaure a conectividade rapidamente e esteja pronto para outra vez

### Desativar as portas para interromper o loop

Os loops de ponte têm consequências extremamente graves em uma rede de ponte. Os administradores geralmente não têm tempo para procurar a causa do loop e preferem restaurar a conectividade assim que possível. A maneira mais fácil nesse caso é desativar manualmente cada porta que fornece redundância na rede. Se você puder identificar uma parte da rede que está afetada, comece a desativar as portas nessa área. Ou, se possível, desabilite inicialmente as portas que podem estar bloqueadas. Toda vez que você desativar uma porta, verifique se você restaurou a conectividade na rede. Ao identificar a porta desativada que interrompe o loop, você também identifica o caminho redundante em que essa porta se encontra. Se essa porta estiver sendo bloqueada, você provavelmente encontrou o link no qual a falha apareceu.

### Registrar eventos de STP em dispositivos que hospedam portas bloqueadas

Se você não puder identificar com precisão a origem do problema ou se o problema for transitório, ative o registro de eventos de STP nas pontes e nos switches da rede que apresenta a falha. Se você quiser limitar o número de dispositivos a serem configurados, habilite pelo menos esse registro nos dispositivos que hospedam portas bloqueadas; a transição de uma porta bloqueada é o que cria um loop.

- Software Cisco IOS - Emita o comando exec **debug spanning-tree events** para habilitar as informações de depuração do STP. Emita o comando do modo de configuração geral **logging buffered** para capturar essas informações de depuração nos buffers do dispositivo.
- CatOS-O **set logging level spantree 7 default** aumenta o nível padrão de eventos relacionados ao STP para o nível de depuração. Certifique-se de registrar um número máximo de mensagens nos buffers do switch usando o comando **set logging buffer 500** comando.

Você também pode tentar enviar a saída de depuração para um dispositivo syslog. Infelizmente, quando ocorre um loop de ponte, você raramente mantém a conectividade com um servidor syslog.

## Verificar portas

As portas vitais a serem investigadas primeiro são as portas de bloqueio. Esta seção fornece uma lista do que procurar nas diferentes portas, com uma rápida descrição dos comandos a serem executados para os switches que executam o CatOs e o software Cisco IOS.

### Verificar se as portas bloqueadas recebem BPDUs

Especialmente nas portas bloqueadas e portas de origem, verifique se você recebe BPDUs periodicamente. Vários problemas podem fazer com que uma porta não receba pacotes ou BPDUs.

- Cisco IOS Software - No Cisco IOS Software Release 12.0 ou posterior, a saída do comando **show spanning-tree bridge-group #** tem um campo `BPDU`. O campo mostra o número de BPDUs recebidas para cada interface. Execute o comando mais uma ou duas vezes para determinar se o dispositivo recebe BPDUs.

  Se você não tiver o campo `BPDU` na saída de **show spanning-tree** você pode habilitar a depuração do STP com o comando **debug spanning-tree** para verificar o recebimento de BPDUs.

- CatOS-O **show mac module/port** informa o número de pacotes multicast que uma porta específica recebe. Mas o comando mais simples de usar é o comando **show spantree statistics module#/port# vlan#** comando. Esse comando exibe o número exato de BPDUs de configuração recebidas por uma porta específica, em uma VLAN específica. Uma porta pode pertencer a várias VLANs, se houver entroncamento. Consulte a seção Um comando adicional do CatOS deste documento.

### Procurar uma incompatibilidade de duplex

Para procurar uma incompatibilidade de duplex, você deve verificar cada lado do link ponto a ponto.

- Cisco IOS Software-Emita o comando **show interfaces [interface interface-number] status** para verificar o status da velocidade e do duplex da porta específica.

- CatOS - As primeiras linhas da saída do comando **show port module#/port#** fornece a velocidade e o duplex de acordo com a configuração da porta.

### Verifique a Utilização da Porta

Uma interface com sobrecarga de tráfego pode não transmitir BPDUs essenciais. Uma sobrecarga de link também indica um possível loop de ponte.

- Software Cisco IOS - Use o comando **show interfaces** para determinar a utilização em uma interface. Vários campos ajudam você nessa determinação, como `carga e entrada/saída de pacotes`. Consulte o documento Troubleshooting de Porta de Switch e Problemas de Interface para obter uma explicação do **show interfaces** Saída do comando.

- CatOS-O **show mac module#/port#** exibe estatísticas sobre os pacotes que uma porta recebe e envia. O **show top** avalia automaticamente a utilização da porta em um período de 30 segundos e exibe o resultado. O comando classifica os resultados pela porcentagem de utilização da largura de banda, embora haja outras opções para classificação de resultados disponíveis. Além disso, o **show system** fornece uma indicação da utilização do painel traseiro, mesmo que o comando não aponte para uma porta específica.

Check Packet Corruption

- Software Cisco IOS - Procure incrementos de erro no contador de `erros de entrada` do **show interfaces** comando. O contador de erros inclui as contagens de runts, giants, no buffer, CRC, frame, overrun e ignored.

  Consulte o documento Troubleshooting de Porta de Switch e Problemas de Interface para obter uma explicação do **show interfaces** command output.

- CatOS - O comando **show port module#/port#** O fornece alguns detalhes com os campos `Align-Err, FCS-Err, Xmit-Err, Rcv-Err` e `Undersize`. O **show counters module#/port#** fornece estatísticas com ainda mais detalhes.

Um comando CatOS adicional

O comando **show spantree statistics module#/port# vlan#** fornece informações muito precisas sobre uma porta específica. Execute este comando nas portas suspeitas e preste atenção especial a estes campos:

- `Forward trans count-este contador lembra quantas vezes uma porta migra de aprendizado para encaminhamento`. Em uma topologia estável, esse contador sempre mostra 1. Esse contador é redefinido como 0, pois a porta fica inativa e ativa. Portanto, um valor maior que 1 indica que a transição realizada pela porta é o resultado de um recálculo de STP. A transição não é o resultado de uma falha de link direto.

- `Max age expiry count-este contador rastreia o número de vezes que a idade máxima expirou neste link`. Basicamente, uma porta que espera receber BPDUs aguarda a idade máxima, antes de considerar que a ponte designada foi perdida. O padrão de idade máxima é de 20 segundos. Toda vez que esse evento ocorrer, o contador aumenta. Quando o valor não é 0, isso indica que a ponte designada para essa LAN está instável ou tem um problema na transmissão de BPDUs.

## Procurar erros de recurso

Uma alta utilização da CPU pode ser perigosa para um sistema que executa o STA. Use este

método para verificar se o recurso da CPU é adequado para um dispositivo:

- Software Cisco IOS - execute o comando show processes cpu. Verifique se a utilização da CPU não está muito elevada. Nos switches Catalyst 4500/4000 Series que executam o CatOs ou o software Cisco IOS, consulte o documento Utilização da CPU nos switches Catalyst 4500/4000, 2948G, 2980G e 4912G.
- CatOS - Emita o comando **show proc cpu** command to display CPU utilization information. Check that the CPU utilization is not too high.

Há uma limitação no número de instâncias diferentes de STP que um mecanismo de supervisão pode suportar. Verifique se o número total de portas lógicas em todas as instâncias de STP para diferentes VLANs não excede o número máximo suportado para cada tipo de Supervisor Engine e configuração de memória.

Execute o **show spantree summary** para switches que executam CatOS ou o **show spanning-tree summary totals** para switches que executam o software Cisco IOS. Esses comandos exibem o número de portas lógicas ou interfaces de acordo com a VLAN na `coluna ativa do STP`. O total é exibido na parte inferior dessa coluna. O total representa a soma de todas as portas lógicas em todas as instâncias de STP para as diferentes VLANs. Assegure que esse número não exceda o número máximo suportado para cada tipo de mecanismo de supervisão.

---

Observação: a fórmula para calcular a soma das portas lógicas no switch é:

---

```
(number of non-ATM trunks * number of active Vlans on that trunk)
+ 2*(number of ATM trunks * number of active Vlans on that trunk)
+ number of non-trunking ports
```

Para obter um resumo das restrições do STP que se aplicam aos switches Catalyst, consulte estes documentos:

| Platform | Restrições de STP do CatOs | Restrições de STP do software Cisco IOS |
|---|---|---|
| Mecanismo de supervisão I e II do Catalyst 6500/6000 | Solução de problemas do STP | |
| Mecanismo de supervisão 720 do Catalyst 6500/6000 | Solução de problemas do STP | Troubleshooting de Spanning Tree |
| Catalyst 4500/4000 | Spanning Tree | Solução de problemas de Spanning Tree |
| Catalyst 3750 | | Configuração do STP |

## Desativar recursos desnecessários

Ao solucionar problemas, você tenta identificar o que está errado na rede no momento. Desative

o maior número de recursos possível. A desativação ajuda a simplificar a estrutura de rede e facilita a identificação do problema. Por exemplo, o EtherChanneling é um recurso que requer que o STP empacote logicamente vários links diferentes em um único link; a desabilitação desse recurso durante o processo de solução de problemas faz sentido. Como regra geral, tornar a configuração o mais simples possível torna o processo de solução de problemas muito mais fácil.

## Comandos úteis

### Comandos do software Cisco IOS

- **show interfaces**
- **show spanning-tree**
- **show bridge**
- **show processes cpu**
- **debug spanning-tree**
- **logging buffered**

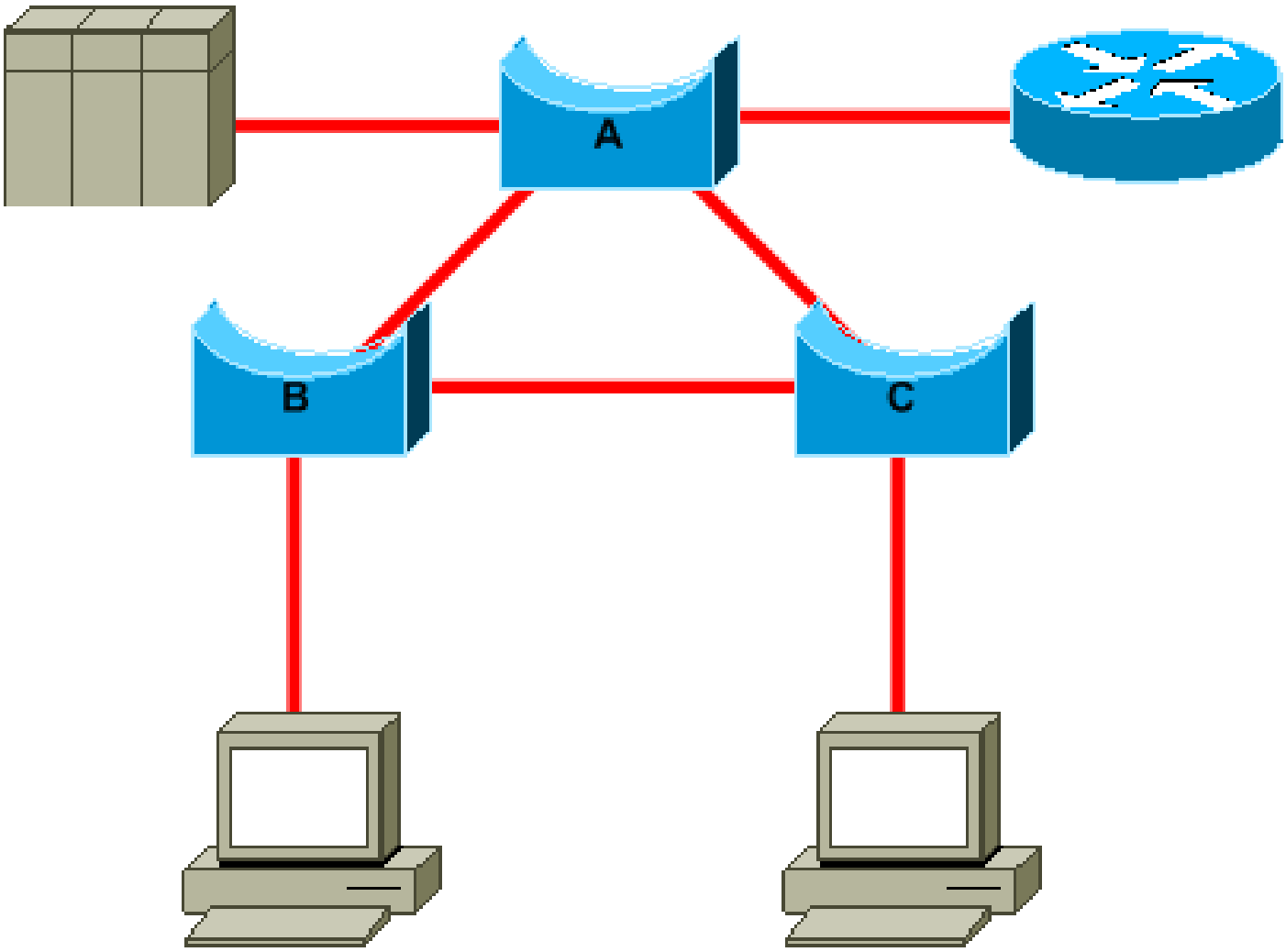
### Comandos de CatOS

- **show port**
- **show mac**
- **show spantree**
- **show spantree statistics**
- **show spantree blockedports**
- **show spantree summary**
- **show top**
- **show proc cpu**
- **show system**
- **show counters**
- **set spantree root [secondary]**
- **set spantree uplinkfast**
- **set logging level**
- **set logging buffered**

# STP de projeto para evasiva de problema

## Saber onde está a raiz

Muitas vezes, as informações sobre o local da causa do problema não estão disponíveis no momento da solução de problemas. Não deixe o STP decidir qual ponte é a causa do problema. Para cada VLAN, geralmente você pode identificar qual switch pode servir melhor como origem. Isso depende do projeto da rede. Em geral, escolha uma ponte eficaz no meio da rede. Se colocar a ponte de origem no centro da rede, com conexão direta com os servidores e roteadores, geralmente você reduz a distância média dos clientes para os servidores e roteadores.




Este diagrama mostra:

- Se a ponte B for a raiz, o link A para C será bloqueado na ponte A ou na ponte C. Nesse caso, os hosts que se conectam ao switch B podem acessar o servidor e o roteador em dois saltos. Os hosts conectados à ponte C podem acessar o servidor e o roteador em três saltos. A distância média é de dois saltos e meio.
- Se a ponte A for a origem, o roteador e o servidor estarão acessíveis em dois saltos para os dois hosts conectados a B e C. A distância média agora é de dois saltos.

A lógica por trás desse exemplo simples é transferida para topologias mais complexas.

---

> Observação: para cada VLAN, codifique a bridge raiz e a bridge raiz de backup com uma redução no valor do parâmetro de prioridade STP. Ou então, você pode usar set spantree root macro.

---

## Saiba onde está a redundância

Planeje a organização dos links redundantes. Esqueça o recurso plug-and-play do STP. Ajuste o parâmetro de custo do STP para decidir quais portas bloquear. Geralmente, esse ajuste não é necessário se você tiver um projeto hierárquico e uma ponte de origem em um local adequado.

---

> Observação: para cada VLAN, saiba quais portas podem estar bloqueadas na rede estável. Tenha um diagrama de rede que mostre claramente cada loop físico na rede e que as portas bloqueadas interrompam os loops.

---

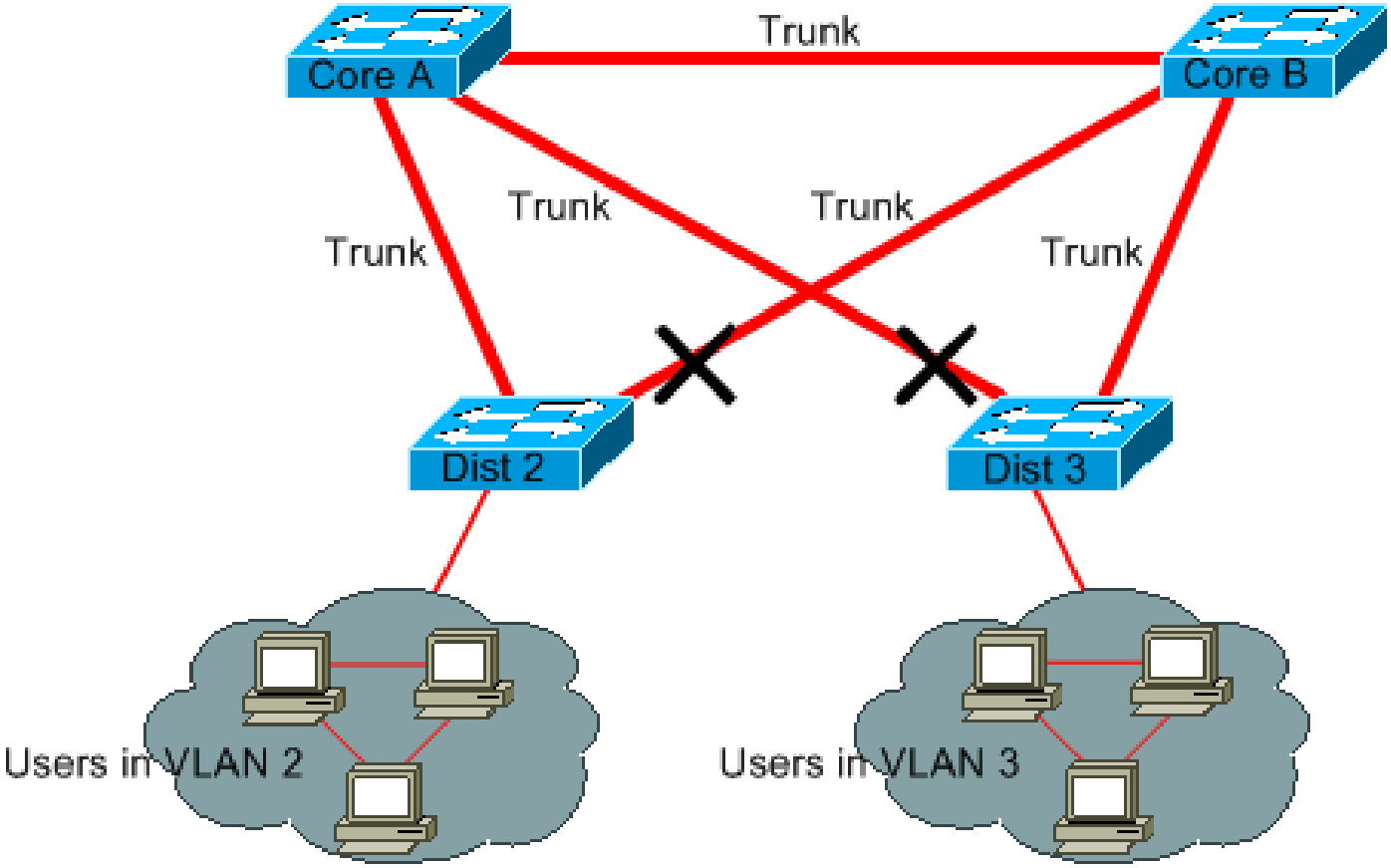
O conhecimento do local dos links redundantes ajuda a identificar um loop de ponte acidental e a causa. Além disso, o conhecimento do local das portas bloqueadas permite determinar o local do erro.

## Minimizar o número de portas bloqueadas

A única ação crítica que o STP realiza é o bloqueio das portas. Uma única porta de bloqueio que migrar equivocadamente para o encaminhamento pode destruir uma grande parte da rede. Uma boa maneira de limitar o risco inerente ao uso do STP é reduzir o número de portas bloqueadas o máximo possível.

Remova as VLANs que você não usa

Você não precisa de mais de dois links redundantes entre dois nós em uma rede de ponte. No entanto, esse tipo de configuração é comum:




Os switches de distribuição fazem uma conexão dupla com dois switches de núcleo. Os usuários conectados aos switches de distribuição estão apenas em um subconjunto das VLANs disponíveis na rede. Neste exemplo, todos os usuários que se conectam no Distribuidor 2 estão na VLAN 2; o Distribuidor 3 só conecta os usuários no Distribuidor 3. Por padrão, os troncos transportam todas as VLANs definidas no domínio do VLAN Trunk Protocol (VTP). Somente o Dist 2 recebe tráfego desnecessário de broadcast e multicast para VLAN 3, mas também está bloqueando uma de suas portas para VLAN 3. O resultado consiste em três caminhos redundantes entre o Núcleo A e o Núcleo B. Essa redundância resulta em mais portas bloqueadas e em uma maior probabilidade de loop.

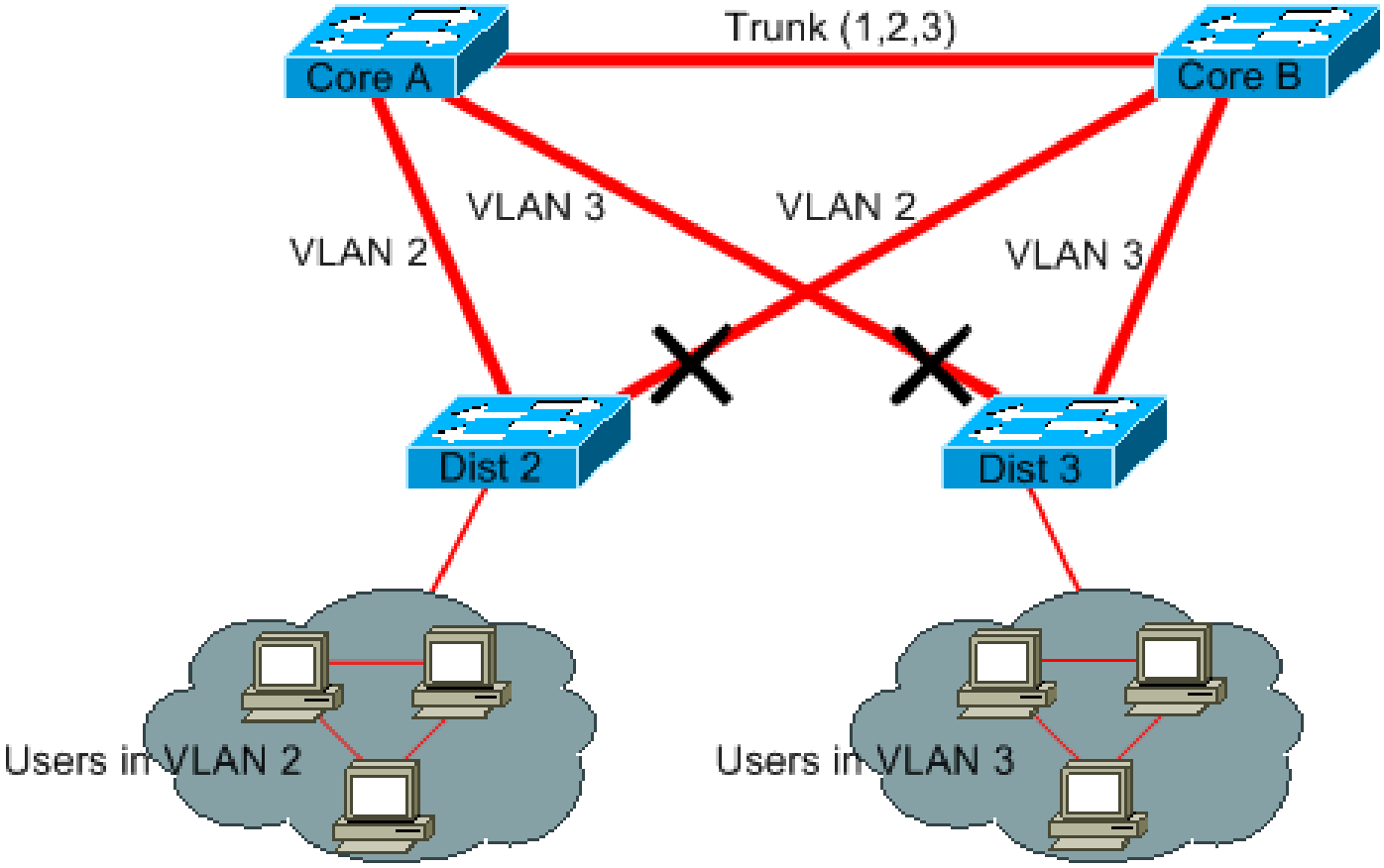
---

Observação: remova todas as VLANs de que você não precisa em seus troncos.

---

A remoção do VTP pode ajudar, mas esse tipo de recurso plug-and-play não é necessário no núcleo da rede.

Neste exemplo, somente uma VLAN de acesso é usada para conectar os switches de distribuição ao núcleo:



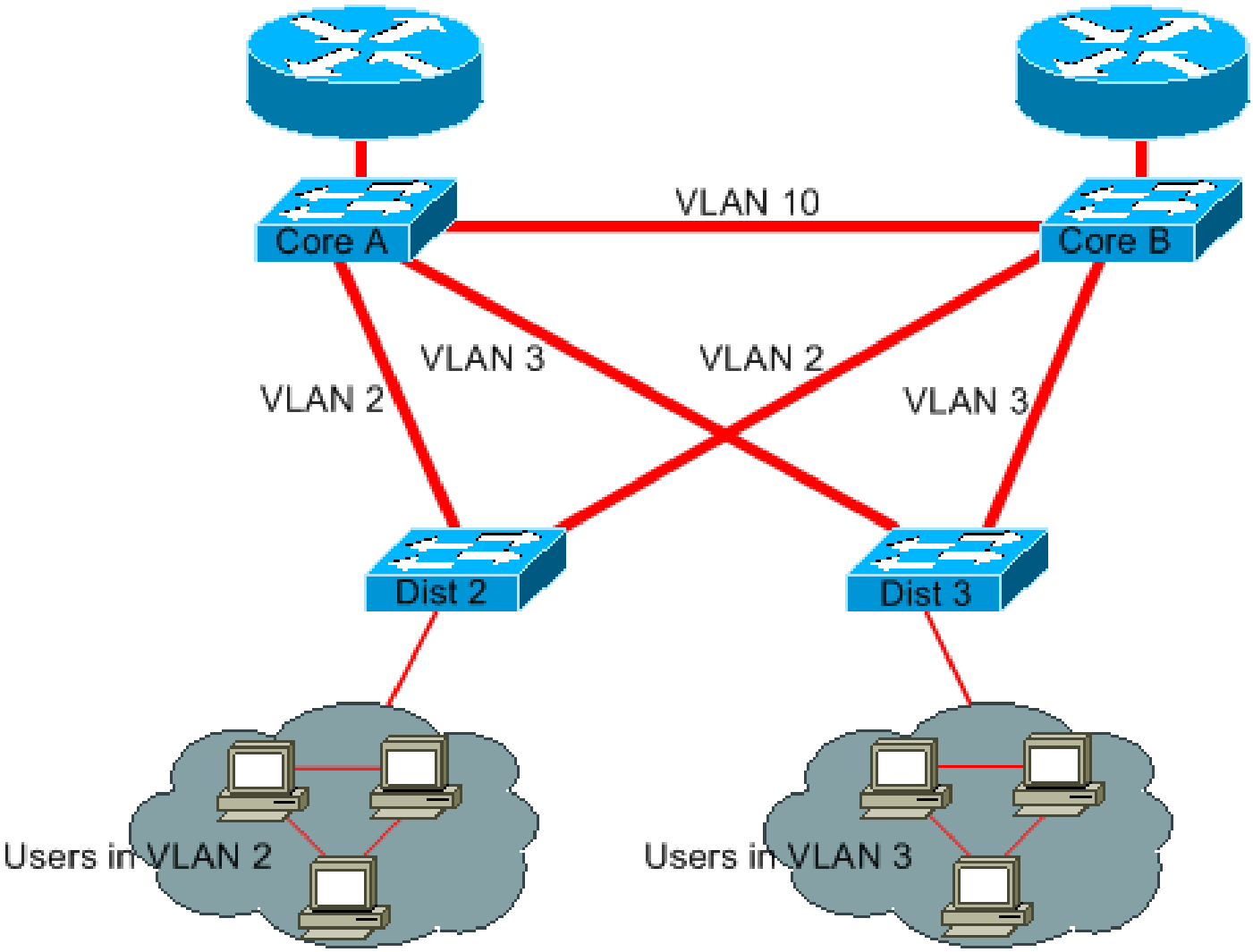

Neste design apenas uma porta está bloqueada por VLAN. Além disso, com esse projeto, você pode remover todos os links redundantes em apenas uma etapa, se desligar o Núcleo A ou o Núcleo B.

Use switching da camada 3

O switching da Camada 3 significa roteamento aproximadamente na velocidade de switching. Um roteador realiza duas funções principais:

- Um roteador cria uma tabela de encaminhamento. O roteador geralmente troca informações com pares por meio dos protocolos de roteamento.
- Um roteador recebe pacotes e os encaminha para a interface correta com base no endereço de destino.

Agora os switches avançados da Camada 3 da Cisco podem realizar essa segunda função, na mesma velocidade que a função de switching da Camada 2. Se você introduzir um salto de roteamento e criar uma segmentação adicional da rede, a velocidade não será prejudicada. Este diagrama usa o exemplo na seção Remova as VLANs que você não usa como base:




O Núcleo A e o Núcleo B agora são alguns switches da Camada 3. A VLAN 2 e a VLAN 3 não estão mais conectadas entre o Núcleo A e o Núcleo B, então não há possibilidade de um loop de STP.

- Ainda há redundância, com uma dependência nos protocolos de roteamento da Camada 3. O projeto garante uma reconvergência que é ainda mais rápida do que a reconvergência com o STP.
- Não existe mais nenhuma porta bloqueada pelo STP. Portanto, não há potencial para um loop de ponte.
- Não há penalidade de velocidade, pois deixar a VLAN pela Camada 3 o switching é tão rápido quanto o bridging dentro da VLAN.

Há uma única desvantagem nesse projeto. A migração para esse tipo de projeto geralmente implica um retrabalho do esquema de endereçamento.

## Manter o STP mesmo se for desnecessário

Mesmo se você tiver êxito com a remoção de todas as portas bloqueadas da rede e não tiver nenhuma redundância física, não desative o STP. O STP geralmente não exige muito do

processador; a comutação de pacotes não envolve a CPU na maioria dos switches Cisco. Além disso, as poucas BPDUs enviadas em cada link não reduzem significativamente a largura de banda disponível. No entanto, uma rede de ponte sem STP pode ser destruída em uma fração de segundos, se um operador cometer um erro em um painel de correção, por exemplo. Geralmente, a desativação do STP em uma rede de ponte não vale o risco.

### Mantenha o tráfego fora da VLAN administrativa e não tenha uma única VLAN em toda a rede

Um switch Cisco normalmente tem um único endereço IP vinculado a uma VLAN, conhecida como a VLAN administrativa. Nessa VLAN, o switch atua como um host IP genérico. Especificamente, cada pacote de broadcast ou multicast é encaminhado para a CPU. Uma alta taxa de tráfego de broadcast ou multicast na VLAN administrativa pode afetar adversamente a CPU e a capacidade da CPU de processar BPDUs essenciais. Portanto, mantenha o tráfego de usuário fora da VLAN administrativa.

Até recentemente, não havia uma maneira de remover a VLAN 1 de um tronco na implementação da Cisco. A VLAN 1 geralmente atua como uma VLAN administrativa, onde todos os switches estão acessíveis na mesma sub-rede IP. Embora útil, essa configuração pode ser perigosa porque um loop de ponte na VLAN 1 afeta todos os troncos, o que pode derrubar toda a rede. É claro que o mesmo problema ocorre independentemente da VLAN que você usa. Tente segmentar os domínios de ponte com o uso de switches de alta velocidade da Camada 3.

A partir do CatOS versão 5.4 e do Cisco IOS Software Release 12.1(11b)E, você pode remover a VLAN 1 dos troncos. A VLAN 1 ainda existe, mas bloqueia o tráfego, o que evita qualquer possibilidade de loop.

## Informações Relacionadas

- Ferramentas e recursos - suporte técnico e documentação
- Suporte Técnico e Documentação - Cisco Systems

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.