Problemas do protocolo de abrangência de árvore e considerações sobre projetos relacionados

Índice

Introdução

Este documento apresenta uma lista de recomendações que ajudam a executar uma rede segura

no que diz respeito à construção de uma ponte sobre para o Switches do Cisco catalyst que executa o OS do catalizador (Cactos) e o software de Cisco IOS®. Este documento discute alguns dos motivos comuns do Spanning Tree Protocol (STP) poder falhar e quais informações procurar para identificar a origem do problema. O documento também mostra o tipo do projeto que minimiza os problemas relacionados à spanning tree e é simples para resolver problemas.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Informações de Apoio

Este documento não discute a operação de STP básica. Para aprender como o STP trabalha, refira este documento:

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

Este documento não discute STP rápido (RSTP), definido no IEEE 802.1W. Também, este documento não discute o protocolo do Spanning Tree Múltipla (MST), definido no IEEE 802.1S. Para obter mais informações sobre do RSTP e do MST, refira estes documentos:

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

Para um documento mais específico do Troubleshooting de STP para Catalyst Switches que executa o Cisco IOS Software, refira o documento que pesquisa defeitos o STP no Catalyst Switch que executa IO integrados Cisco (modo nativo).

Falha do protocolo de extensão de árvore

A função principal do algoritmo de Spanning Tree (STA) é cortar laços que os enlaces redundantes criam nas redes de Bridge. O STP opera-se na camada 2 do modelo do abrir interconexão do sistema (OSI). Por meio do bridge protocol data units (BPDU) essa troca entre pontes, o STP elege as portas que eventualmente enviam ou obstruem o tráfego. Este protocolo pode falhar em alguns casos específicos, e pesquisar defeitos a situação resultante pode ser muito difícil, que depende do projeto da rede. Nesta área particular, você executa a maioria de parte importante do Troubleshooting antes que o problema ocorra.

Uma falha no STA conduz geralmente a um Loop de Bridging. A maioria de clientes que chamam o Suporte técnico de Cisco para medir - suspeito dos problemas da árvore um erro, mas um erro são raramente a causa. Mesmo se o software é o problema, um Loop de Bridging em um ambiente STP ainda vem de uma porta que deva obstruir, mas pelo contrário trafica para a frente.

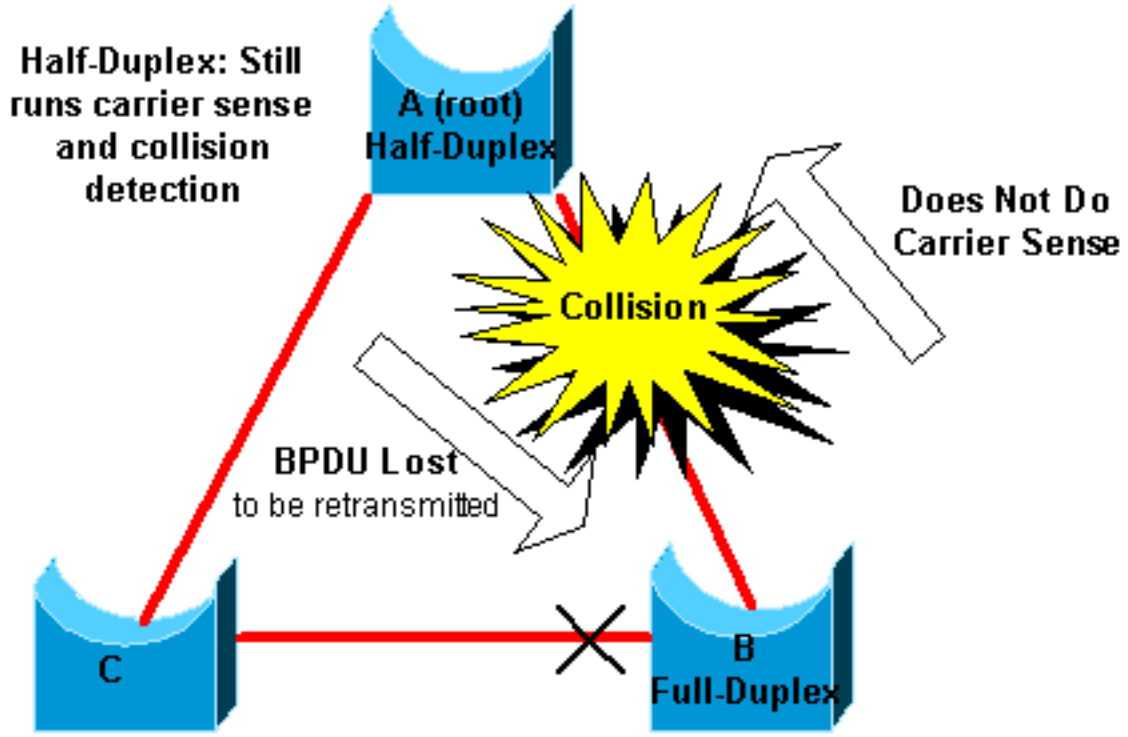
Convergência de árvore de abrangência

Refira - vídeo da árvore para ver um exemplo que explique como a medida - a árvore de medida convirge inicialmente. O exemplo igualmente explica porque um porto bloqueado entra no modo de encaminhamento devido a uma perda excessiva de BPDU, tendo por resultado a falha de STA.

O resto desse documento enumera as diferentes situações que podem provocar a falha do STA. A maioria destas falhas relacionam-se a uma perda grande de BPDU. A perda causa portos bloqueado à transição ao modo de encaminhamento.

Incompatibilidade duplex

A incompatibilidade duplex (bidirecional) em um link de ponto a ponto é muito um erro da configuração comum. Se você ajusta manualmente o modo duplex a completamente em um lado do link e deixa o outro lado no modo de negociação automática, o link termina acima em metade-frente e verso. (A porta A com grupo do modo duplex a completamente já não negocia.)



O cenário de caso pior é quando uma ponte que envie BPDU tem o modo duplex ajustado metade-frente e verso em uma porta, mas a porta de peer na outra extremidade do link tem o modo duplex ajustado FULL-frente e verso. No exemplo acima, o incompatibilidade bidirecional no link entre o Bridge A e B pode levar facilmente a um loop de Bridging. Porque a ponte B tem a configuração para FULL-frente e verso, não executa o carrier sense antes do acesso do link. A ponte B começa enviar quadros mesmo se a ponte A já está usando o link. Esta situação é um problema para A; construa uma ponte sobre A detecta uma colisão e executa o algoritmo de retrocesso antes que a ponte tente uma outra transmissão do quadro. Se há bastante tráfego de B a A, cada pacote que A envia, que inclui os BPDU, submete-se ao adiamento ou à colisão e obtém-se eventualmente deixado cair. De um ponto de vista STP, porque a ponte B não recebe BPDU de A any more, a ponte B perdeu o bridge-raiz. Isto conduz B desbloquear a porta conectada para construir uma ponte sobre o C, que cria o laço.

Sempre que há uma incompatibilidade duplex (bidirecional), estes Mensagens de Erro estão nos

consoles do interruptor dos Catalyst Switches que executam Cactos e Cisco IOS Software:

CatOS

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

Cisco IOS Software

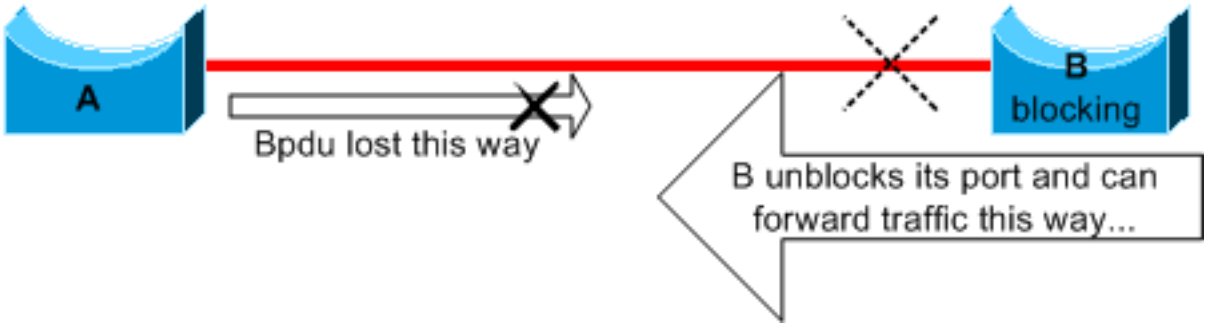
```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half
duplex), with TBA05071417(Cat6K-B) 4/1 (half duplex).
```

Verifique as configurações bidirecional e, se a configuração bidirecional não combina, para ajustar apropriadamente a configuração.

Para obter mais informações sobre de como pesquisar defeitos uma incompatibilidade duplex (bidirecional), refira o documento que configura e pesquisando defeitos o auto-negociação half/full duplex dos Ethernet 10/100/1000Mb.

Link unidirecional

Links unidirecionais são uma causa comum de um Loop de Bridging. Em enlaces de fibra, uma falha que vá sem detecção causa frequentemente enlaces unidirecional. Uma outra causa é um problema com um transceptor. Qualquer coisa que pode conduzir um link para ficar acima e fornecer uma comunicação de sentido único é muito perigoso no que diz respeito ao STP. Este exemplo esclarece:



Aqui, supõe que o link entre A e B é unidirecional. O link deixou cair o tráfego de à B quando o link transmitir o tráfego de B a A. Suposição que constrói uma ponte sobre B estava obstruindo antes que o link se tornou unidirecional. Contudo, uma porta pode somente obstruir se recebe BPDU de uma ponte que tenha uma prioridade mais alta. Desde que, neste caso, todos os BPDU que vêm de A são perdidos, as transições da ponte B eventualmente sua porta para A ao estado de encaminhamento e traficam para a frente. Isto cria um laço. Se esta falha existe na partida, o STP não convirge corretamente. No caso de uma incompatibilidade duplex (bidirecional), uma repartição ajuda temporariamente; mas neste caso, uma repartição das pontes não tem absolutamente nenhum efeito.

A fim detectar os enlaces unidirecional antes da criação do loop de encaminhamento, Cisco projetou e executou o protocolo do UniDirectional Link Detection (UDLD). Esta característica pode detectar a expedição de cabogramas ou enlaces unidirecional impróprios na camada 2 e automaticamente quebrar laços resultantes desabilitando algumas portas. Execute o UDLD na medida do possível em um ambiente interligado.

Para obter mais informações sobre do uso do UDLD, refira o documento que compreende e que configura os Recursos de Protocolo de Detecção de Link Unidirecional.

Corrupção de pacotes

A corrupção do pacote também pode causar o mesmo tipo de falha. Se um link tem um alto índice de erros físicos, você pode perder um determinado número de BPDU consecutivos. Esta perda pode conduzir uma porta de bloqueio à transição ao estado de encaminhamento. Você não vê este caso muito frequentemente porque os parâmetros padrão STP são muito conservadores. A porta de bloqueio precisa de faltar BPDU para 50 pés segundos antes da transição à transmissão. A transmissão bem-sucedida de um único BPDU quebra o laço. Este caso ocorre geralmente com o ajuste sem cuidado dos parâmetros STP. Um exemplo de um ajuste é redução max age.

A incompatibilidade duplex (bidirecional), os cabos ruins, ou o comprimento de cabo incorreto podem causar a corrupção de pacote. Refira a porta de switch do Troubleshooting do documento e conecte problemas para uma explicação saída do contador de erros de Cactos e de Cisco IOS Software.

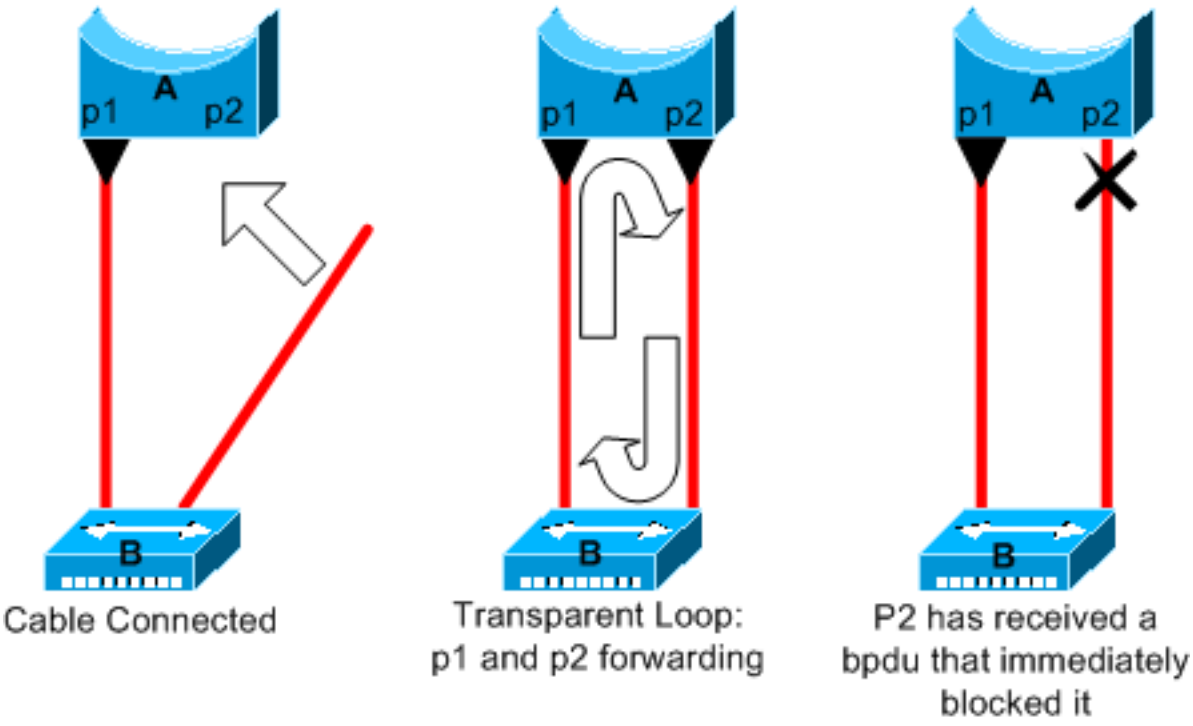
Erros de recursos

O STP é executado no software, mesmo nos switch de produto avançado que executam a maioria das funções de switching no hardware com os circuitos integrados do aplicativo específicos especializados (ASIC). Se por qualquer razão há uma overutilization do CPU da ponte, os recursos podem ser inadequados para a transmissão dos BPDU. O STA não é geralmente recursos intensivos de processador e tem a prioridade sobre outros processos. A seção dos erros de recurso da procura deste documento fornece algumas diretrizes no número de exemplos do STP que uma plataforma particular pode segurar.

Erro de configuração de PortFast

PortFast é uma característica que você permita tipicamente somente para uma porta ou uma relação que conecte a um host. Quando o link vem acima nesta porta, a ponte salta as primeiras fases do STA e diretamente das transições ao modo de encaminhamento.

Caution: Não use os recursos de portfast nas portas de switch ou nas relações que conectam ao outro Switches, Hubs, ou Roteadores. Se não, você pode criar um laço da rede.



Neste exemplo, o dispositivo A é uma ponte com a porta p1 já que envia. O P2 da porta tem uma configuração de Port Fast. O dispositivo B é um hub. Assim que você obstruir o segundo cabo em A, o P2 da porta vai ao modo de encaminhamento e cria um laço entre p1 e P2. Paradas deste laço assim que p1 ou o P2 receberem um BPDU que ponha uma destas duas portas no modo de bloqueio. Mas há um problema com este tipo do loop transitório. Se o tráfego dado laços é muito intensivo, a ponte pode ter o problema com com sucesso a transmissão do BPDU que para o laço. Este problema pode atrasar a convergência consideravelmente ou derrubar a rede em casos extremos.

Para obter mais informações sobre do uso correto de PortFast no Switches que executa Cactos e Cisco IOS Software, refira o documento usando PortFast e outros comandos fixar atrasos da conectividade de inicialização de estação de trabalho.

Mesmo com configuração de Port Fast, a porta ou a relação ainda participam no STP. Se um interruptor com uma prioridade de bridge inferior do que aquele dos diplomatas ativos atuais do bridge-raiz a uma porta ou a uma relação do PortFast configurado, ele pode ser elegido como o bridge-raiz. Esta mudança do bridge-raiz pode adversamente afetar a topologia STP ativa e pode render a rede subótima. Para impedir esta situação, a maioria de Catalyst Switches que executa Cactos e o Cisco IOS Software têm uma característica com o protetor de BPDU do nome. O protetor de BPDU desabilita uma porta ou uma relação do PortFast configurado se a porta ou a relação recebem um BPDU.

Para obter mais informações sobre do uso da característica do protetor de BPDU no Switches que executa Cactos e Cisco IOS Software, refira o realce do protetor de BPDU do portfast de Spanning Tree do documento.

Acordo e problemas de diâmetro inábeis do parâmetro STP

Um valor assertivo para o parâmetro max age e o retardo de encaminhamento pode conduzir a uma topologia STP muito instável. Nesses casos, a perda de alguns BPDU pode fazer com que um laço apareça. O outro problema que não é conhecido relaciona-se ao diâmetro da rede de Bridge. Os valores padrão conservadores para os temporizadores de STP impõem um diâmetro máximo de rede de sete. Este diâmetro máximo de rede restringe como longe de se as pontes na

rede podem ser. Neste caso, duas pontes distintas não podem ser mais de sete saltos longe de se. Parte dessa restrição vem do campo de idade que os BPDUs carregam.

Quando um BPDU propaga do bridge-raiz para as folhas da árvore, o campo idade incrementa cada vez que o BPDU vai embora uma ponte. Eventualmente, a ponte rejeita o BPDU quando o campo idade vai além da idade máxima. Se a raiz é demasiado longe de algumas pontes da rede, esta edição pode ocorrer. Esta edição afeta a convergência da medida - árvore.

Ciao o cuidado especial se você planeia mudar temporizadores de STP do valor padrão. Há um perigo se você tenta obter desta maneira uma reconvergência mais rápida. Uma mudança do temporizador de STP tem um impacto no diâmetro da rede e na estabilidade do STP. Você pode mudar a prioridade de bridge para selecionar o bridge-raiz, e muda os custos de porta ou o parâmetro de prioridade para controlar a Redundância e o Balanceamento de carga.

O Cisco Catalyst Software fornece-o os macro que ajustam finamente os parâmetros STP os mais importantes para você:

- O comando macro do **set spantree root [secondary]** diminui a prioridade de bridge de modo que se transforme raiz (ou raiz alternada). Uma opção adicional está disponível para este comando esse resultados no ajustamento dos temporizadores de STP especificando o diâmetro de sua rede. Mesmo quando feito corretamente, o ajuste de temporizador não melhora significativamente o tempo de convergência e introduz alguns riscos da instabilidade na rede. Também, este tipo do ajustamento tem que ser atualizado cada vez que um dispositivo é adicionado na rede. Mantenha os valores padrão conservadores, que são familiares aos engenheiros de rede.
- **O comando set spantree uplinkfast** para Cactos ou o **comando spanning-tree uplinkfast** para o Cisco IOS Software aumenta a prioridade do interruptor de modo que o interruptor não possa ser raiz. O comando aumenta o tempo da convergência de STP no caso de uma falha do uplink. Use este comando em um switch de distribuição com conexão dupla a alguns switch centrais. Refira o documento que compreende e que configura os recursos uplinkfast de Cisco.
- **O comando set spantree backbonefast enable** para Cactos ou o **comando spanning-tree backbonefast** para o Cisco IOS Software podem aumentar a época da convergência de STP do interruptor no caso de uma falha indireta do link. O BackboneFast é uns recursos proprietários de Cisco. Refira o documento que compreende e que configura o Backbone Fast em Catalyst Switches.

Para obter mais informações sobre dos temporizadores de STP e das regras para ajustá-los quando absolutamente necessário, refira os temporizadores compreensivos e de ajustamentos do documento do Spanning Tree Protocol.

Erros do software

Como mencionado na introdução, o STP é uma das primeiras características que foi executada no Produtos da Cisco. Espera-se que este recurso seja muito estável. Somente a interação com características mais novas, tais como o EtherChannel, fez com que o STP falhe em alguns casos muito específicos que têm sido endereçados agora. Um número de fatores diferentes podem causar um Bug de Software e podem ter um número de efeitos diferentes. Não há nenhuma maneira de descrever adequadamente as edições que um erro pode introduzir. A maioria de situação perigosa que elevara dos erros de software é se você ignora alguns BPDU ou, em linhas gerais, você tem uma transição da porta de bloqueio à transmissão.

Solucionar o problema de uma falha

Infelizmente, não há nenhum procedimento sistemático para pesquisar defeitos uma edição STP. Contudo, esta seção resume algumas das ações que estão disponíveis a você. A maioria das etapas nesta seção aplicam-se ao Troubleshooting dos Loop de Bridging geralmente. Você pode usar uma aproximação mais convencional para identificar outras falhas do STP que conduzem a uma perda de conectividade. Por exemplo, você pode explorar o trajeto esse o tráfego que experimenta tomadas de um problema.

Note: A maioria destes passos de Troubleshooting supõem a Conectividade aos dispositivos diferentes da rede de Bridge. Esta Conectividade significa que você tem o acesso de console. Durante um loop de Bridging, por exemplo, você provavelmente não poderá fazer uma conexão Telnet.

Se você tem a saída de um **comando show-tech support de** seu dispositivo Cisco, você pode usar o analisador do CLI Cisco (clientes registrados somente) para indicar problemas potenciais e reparos.

Utilizar o diagrama da rede

Antes que você pesquise defeitos um Loop de Bridging, você precisa de conhecer estes artigos, pelo menos:

- A topologia da rede de Bridge
- O lugar do bridge-raiz
- O lugar dos portos bloqueado e dos enlaces redundantes

Este conhecimento é essencial no mínimo estas duas razões:

- A fim conhecer o que fixar na rede, você precisa de saber a rede olha quando trabalha corretamente.
- A maior parte das etapas de Troubleshooting simplesmente usa comandos 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

Usou-se para ser que uma tempestade de transmissão poderia ter um efeito desastroso na rede. Hoje, com links de alta velocidade e dispositivos que fornecem o interruptor a nível de hardware, não é provável que um host único, por exemplo, um server, derruba uma rede com as transmissões. A melhor maneira de identificar um Loop de Bridging é capturar o tráfego em um link saturado e certificar-se de você ver tempos similares do múltiplo dos pacotes. Realisticamente, contudo, se todos os usuários em um determinado domínio de Bridge têm problemas de conectividade ao mesmo tempo, você pode já suspeitar um Loop de Bridging.

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

Nos Catalyst Switches que executa Cactos, você pode facilmente verificar o USO de backplane total com o **comando show system**. O comando fornece o uso atual do backplane do interruptor e igualmente especifica o pico de USO e a data do pico de USO. Um pico de utilização incomun

mostra-lhe se houve nunca um Loop de Bridging neste dispositivo.

Restaure a conectividade rapidamente e esteja pronto para outra vez

Portas do desabilitação para quebrar o laço

Os Loop de Bridging têm consequências extremamente sérias em uma rede de Bridge. Os administradores geralmente não têm o tempo procurar a causa do laço e para preferi-la restaurar o mais cedo possível a Conectividade. A maneira fácil para fora é neste caso desabilitar manualmente cada porta que fornece a Redundância na rede. Se você pode identificar parte da rede que está afetada a maioria, comece a desabilitar portas nesta área. Ou, se possível, desabilite inicialmente as portas que devem obstruir. Cada vez que você desabilita uma porta, verifique para ver se você restaurou a Conectividade na rede. Identificando que a porta deficiente para o laço, você igualmente identifica o caminho redundante onde esta porta é encontrada. Se essa porta devia estar sendo bloqueada, é provável que você tenha descoberto o link onde surgiu a falha.

Eventos do log STP nos dispositivos que hospedam portos bloqueado

Se você não pode precisamente identificar a fonte do problema, ou se o problema é transiente, permita o registro de eventos STP nas pontes e no Switches da rede que experimenta a falha. Se você quer limitar o número de dispositivos para configurar, permita pelo menos isto os dispositivos de abertura que hospedam portos bloqueado; a transição de um porto bloqueado é o que cria um laço.

- A questão de software do Cisco IOS o **debug spanning-tree events do** comando exec para permitir o STP debuga a informação. Emita o **registro do** comando general config mode **protegido** para capturar isto debugam a informação nos bufferes do dispositivo.
- O do de Cactos- o **comando set logging level spantree 7 default** aumenta o nível padrão dos eventos que se relacionam ao STP ao nível de debug. Seja certo que você registra um número máximo de mensagens nos bufferes do interruptor com uso do **comando set logging buffer 500**.

Você também pode tentar enviar a saída de depuração para um dispositivo syslog. Infelizmente, quando um Loop de Bridging ocorre, você mantém raramente a Conectividade a um servidor de SYSLOG.

Verificar portas

As portas crítica a investigar primeiramente são as portas de bloqueio. Esta seção fornece uma lista do que procurar nas portas diferentes, com uma descrição rápida dos comandos emitir para o Switches que executa Cactos e Cisco IOS Software.

Certifique-se dos portos bloqueado recebam BPDU

Especialmente em portos bloqueado e em portas de raiz, certifique-se de você receba BPDU periodicamente. Diversas edições podem conduzir a uma falha de porta receber pacotes ou BPDU.

- O Cisco IOS Software-no Cisco IOS Software Release 12.0 ou Mais Recente, saída do

comando show spanning-tree bridge-group - tem um campo `BPDU`. O campo mostra-lhe o número de BPDU recebidos para cada relação. Emita o comando uma ou dois épocas adicionais determinar se o dispositivo recebe BPDU.Se você não tem o campo `BPDU na` saída do **comando show spanning-tree**, você pode permitir o STP debuga com o **comando debug spanning-tree** verificar o recibo dos BPDU.

- **O comando show mac module/port de** Cactos-The diz-lhe os números de pacote multicast que uma porta específica recebe. Mas o comando o mais simples usar-se é o **comando show spantree statistics module-/port- vlan-**. Este comando indica o número exato de bpdus de configuração que uma porta específica recebeu, em um VLAN específico. Uma porta pode pertencer a diversos VLAN, se entroncamento. Veja uma seção de comando cactos adicional deste documento.

Verifique para ver se há uma incompatibilidade duplex (bidirecional)

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

- Questão de software do Cisco IOS o **comando show interfaces [interface interface-number] status** verificar o estado da velocidade e duplexação da porta específica.
- As primeiras linhas de Cactos-The muito da saída do **comando show port module-/port-** dão-lhe a velocidade e duplexação de acordo com a configuração de porta.

Verifique a Utilização da Porta

Uma relação com sobrecarga do tráfego pode não transmite bpdus vital. Uma sobrecarga do link igualmente indica um Loop de Bridging possível.

- Software-uso do Cisco IOS o comando show interfaces **determinar a utilização em uma relação.** Diversos campos ajudam-no com esta determinação, tal como a `carga` e o `entrada/saída dos pacotes`. Refira a porta de switch do Troubleshooting do documento e conecte problemas para uma explicação da saída do **comando show interfaces**.
- **O comando show mac module-/port- de** Cactos-The indica estatísticas sobre os pacotes que uma porta recebe e envia. **O comando show top** avalia automaticamente a utilização de porta durante um período 30-second e indica o resultado. O comando classifica os resultados pela utilização da largura de banda da porcentagem, embora as outras opções para a classificação dos resultados estejam disponíveis. Também, o **comando show system** dá uma indicação da utilização de backplane, mesmo que o comando não aponte a uma porta específica.

Check Packet Corruption

- O Software-olhar do Cisco IOS para o erro incrementa no contador de `erros de entrada do` **comando show interfaces**. Os contadores de erros incluem `runts, gigantes, sem buffer, CRC, quadro, overrun`, e `contagens ignorada`.Refira a porta de switch do Troubleshooting do documento e conecte problemas para uma explicação da saída do **comando show interfaces**.
- O comando show port module-/port- de Cactos-The **dá-lhe alguns detalhes com** `Erro Align, Erro FCS, Erro Xmit, o RCV-ERR,` e campos `subdesenvolvidos`. **O comando show counters module-/port-** fornece estatísticas em ainda mais detalhe.

Um comando CatOS adicional

O comando show spantree statistics module-/port- vlan- *dá muito a informação precisa sobre uma porta específica.* Emita este comando nas portas que você suspeita e paga a atenção especial a estes campos:

- `Dianteiro contagem-este` contador `transporte` recorda quantas vezes transições de porta da aprendizagem à transmissão. Em uma topologia estável, este contador mostra sempre 1. Este as reinicializações do contador a 0 como a porta vão para baixo e levantam. Assim, um valor que seja mais alto de 1 indica que a transição experimentada pela porta é o resultado de um recálculo de STP. A transição não é o resultado de uma falha de link direto.
- `A expiração do max age contagem-este` contador segue o número de vezes que o max age expirou neste link. Basicamente, uma porta que espere esperas BPDU para o max age antes que a porta considerar o bridge designada ser perdida. O padrão do max age é 20 segundos. Cada vez que este evento ocorre, o contador incrementa. Quando o valor não é 0, indica que o bridge designada para este LAN é instável ou tem um problema com a transmissão dos BPDU.

Procurar erros de recurso

Uma utilização elevada da CPU pode ser perigosa para um sistema que execute o STA. Use este método para certificar-se dos recursos do CPU sejam adequados para um dispositivo:

- Questão de software do Cisco IOS o **comando show processes cpu**. Verifique se a utilização da CPU não está muito elevada. Para o Switches do 4500/4000 Series do catalizador que executa Cactos ou Cisco IOS Software, refira a utilização CPU do documento no catalizador 4500/4000, 2948G, 2980G, e 4912G Switch.
- Cactos-edição o **comando show proc cpu** indicar a informação da utilização CPU. Verifique se a utilização da CPU não está muito elevada.

Há uma limitação no número de exemplos diferentes do STP que um Supervisor Engine pode segurar. 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.

Emita o **comando show spantree summary** para o Switches que executa Cactos ou o **comando show spanning-tree summary totals** para o Switches que executa o Cisco IOS Software. Estes comandos display o número de portas lógica ou de relações pelo VLAN na `coluna de STP Ativo`. O total aparece na parte inferior desta coluna. O total representa a soma de todas as portas lógica através de todos os exemplos do STP para os VLAN diferentes. Certifique-se de que este número não excede o número máximo apoiado para cada tipo de Supervisor Engine.

Note: A fórmula para computar a soma das portas lógica no interruptor 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 um sumário das limitações para o STP que se aplicam aos Catalyst Switches, refira estes documentos:

Plataforma	Restrições de STP de	Restrições de STP do Cisco IOS

	Cactos	Software
Supervisor Engine I e II do Catalyst 6500/6000	Troubleshooting de STP	
Supervisor Engine 720 do Catalyst 6500/6000	Troubleshooting de STP	Troubleshooting de Spanning Tre
Catalyst 4500/4000	Spanning Tree	Medida de pesquisa de defeitos - árvore
Catalyst 3750		Configurando o STP

Características desnecessárias do desabilitação

O Troubleshooting é uma matéria de identificar o que está atualmente erradamente na rede. Desabilite tantas como características como possíveis. As ajudas da incapacidade simplificam a estrutura de rede e facilitam a identificação do problema. Por exemplo, EtherChanneling é uma característica que exija o STP empacotar logicamente diversos links diferentes em um link único; a incapacidade desta característica durante o Troubleshooting faz o sentido. Em regra geral, fazer a configuração facilita tão simples quanto possível pesquisando defeitos o problema.

Comandos úteis

Comandos do Cisco IOS Software

- show interfaces
- show spanning-tree
- mostre a ponte
- show processes cpu
- debugar a medir-árvore
- registro colocado em buffer

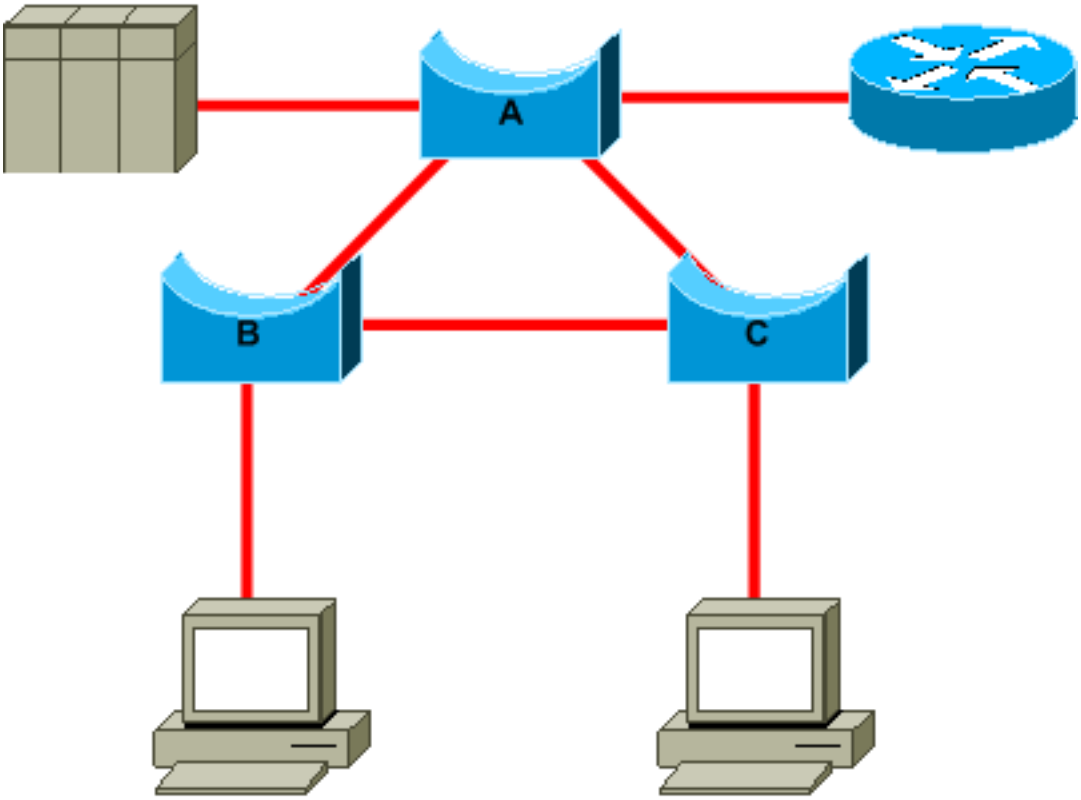
Comandos de CatOS

- show port
- show mac
- show spantree
- mostre estatísticas de árvore de abrangência
- mostre blockedports do spantree
- show spantree summary
- show top
- show proc cpu
- show system
- show counters
- set spantree root [secondary]
- set spantree uplinkfast
- definir nível de registro
- ajuste o registro protegido

STP de projeto para evasiva de problema

Saber onde está a raiz

Muito frequentemente, a informação sobre o lugar da raiz não está disponível no tempo de Troubleshooting. Não deixe o STP para decidir que ponte é raiz. Para cada VLAN, você pode geralmente identificar que o interruptor pode o melhor saque como a raiz. Isto depende do projeto da rede. Geralmente, escolha um bridge forte no meio da rede. Se você põe o bridge-raiz no centro da rede com a conexão direta aos server e ao Roteadores, você reduz geralmente a distância média dos clientes aos server e ao Roteadores.



Este diagrama mostra:

- Se a ponte B é raiz, ligue A ao C está obstruído na ponte A ou na ponte C. neste caso, os anfitriões que conectam ao switch B podem alcançar o server e o roteador em dois saltos. Os anfitriões que conectam para construir uma ponte sobre o C podem alcançar o server e o roteador em três saltos. A distância média é dois e um meio dos saltos.
- Se a ponte A é raiz, o roteador e o server são alcançáveis em dois saltos para ambos os anfitriões que conectam em B e em C. A distância média é agora dois saltos.

A lógica atrás de transferências deste exemplo simples a mais topologias complexas.

Nota importante: Para cada VLAN, código duro o bridge-raiz e o root bridge de backup com uma redução no valor do parâmetro de prioridade do STP. Ou você pode usar set spantree root macro.

Saiba onde está a redundância

Planeie a organização de seus enlaces redundantes. Esqueça sobre os recursos de plugue-and-play do STP. Ajuste o parâmetro de custo STP para decidir que portas obstruem. Isto que ajusta não é geralmente necessário se você tem um projeto hierárquico e um bridge-raiz em um bom lugar.

Nota importante: Para cada VLAN, saiba que portas devem obstruir na rede estável. Tenha um

diagrama da rede que mostrem claramente cada laço físico na rede e os que portos bloqueado quebrem os laços.

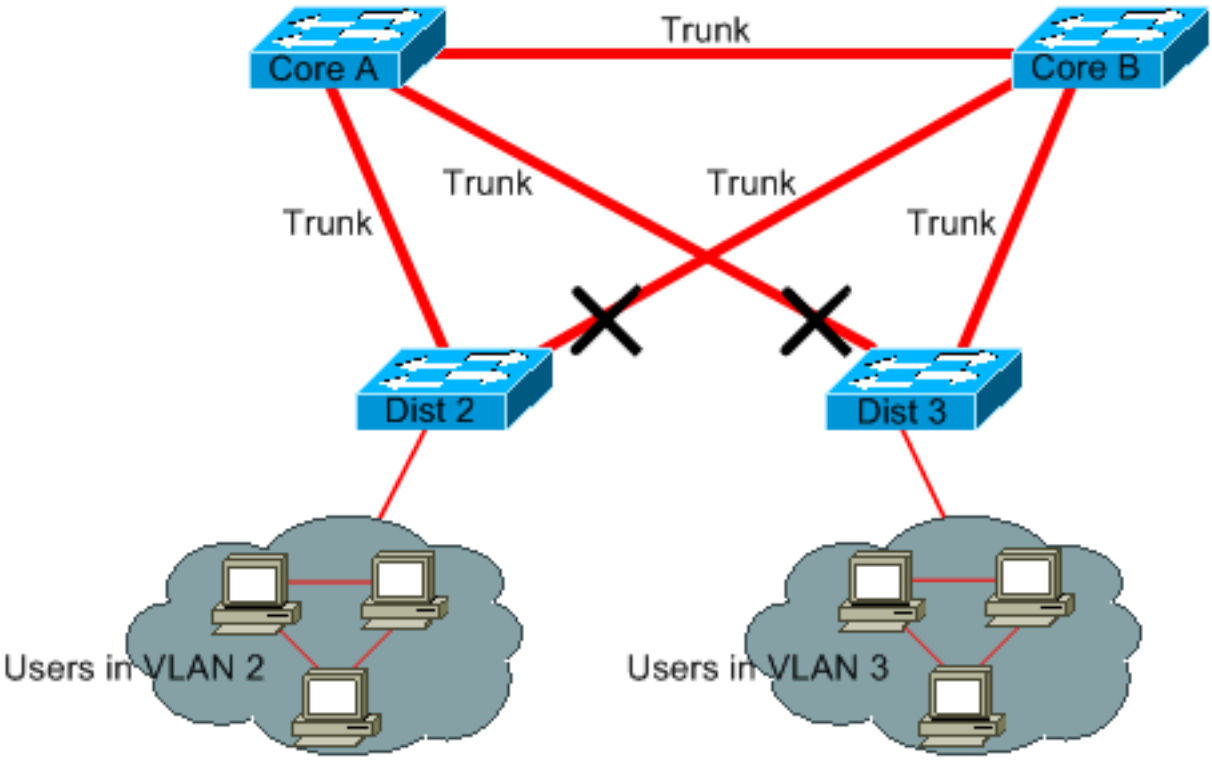
O conhecimento do lugar dos enlaces redundantes ajuda-o a identificar um Loop de Bridging acidental e a causa. Também, o conhecimento do lugar dos portos bloqueado permite que você determine o lugar do erro.

Minimizar o número de portas bloqueadas

A única ação crítica que o STP toma é a obstrução das portas. Uma única porta de bloqueio que equivocadamente as transições à transmissão podem se derreter um grande parte da rede. Uma boa maneira de limitar o risco inerente no uso do STP é reduzir tanto quanto possível o número de portos bloqueado.

Ameixa seca VLAN que você não usa

Você não precisa mais de dois enlaces redundantes entre dois Nós em uma rede de Bridge. Contudo, este tipo de configuração é comum:



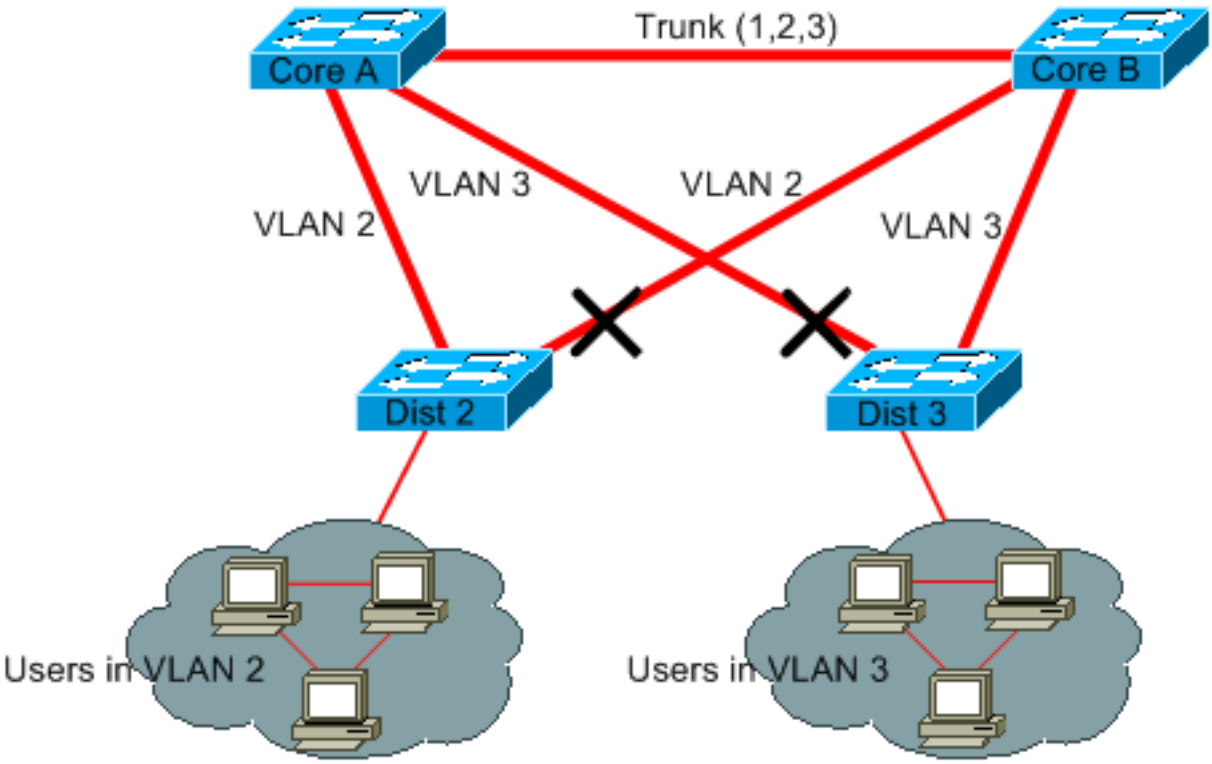
Os switch de distribuição são dual anexo a dois switch centrais. Os usuários que conectam em switch de distribuição estão somente em um subconjunto dos VLAN disponíveis na rede. Neste exemplo, os usuários que conectam em Dist 2 são todos no VLAN2; Dist 3 conecta somente usuários em VLAN 3. à revelia, troncos leva todos os VLAN definidos no domínio do protocolo VLAN Trunk (VTP). Somente Dist 2 recebe o broadcast desnecessária e o tráfego multicast para o VLAN3, mas igualmente está obstruindo uma de suas portas para o VLAN3. O resultado é três caminhos redundantes entre o núcleo A e o núcleo B. Esta Redundância conduz a mais portos bloqueado e a uma semelhança mais elevada de um laço.

Nota importante: Pode todo o VLAN que você não precisar fora de seus troncos.

A poda de VTP pode ajudar, mas este tipo dos recursos de plugue-and-play não é necessário no

núcleo da rede.

Neste exemplo, somente um acesso VLAN é usado para conectar os switch de distribuição ao núcleo:



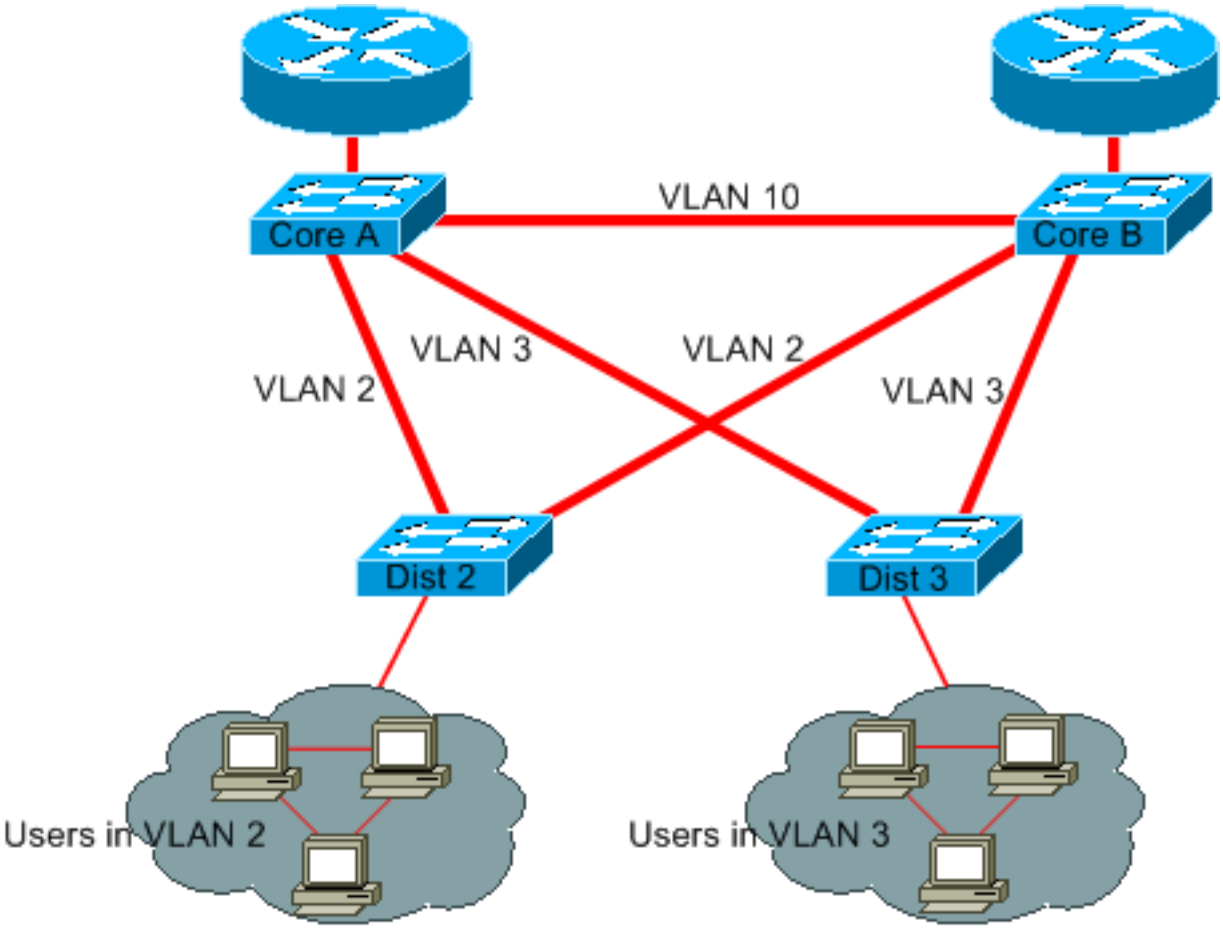
Neste design apenas uma porta está bloqueada por VLAN. Também, com este projeto, você pode remover todos os enlaces redundantes em apenas uma etapa se você fecha o núcleo A ou o núcleo B.

Use switching da camada 3

O switching da camada 3 significa a distribuição aproximadamente na velocidade do interruptor. Um roteador realiza duas funções principais:

- Um roteador constrói uma tabela do forwarding. O roteador troca geralmente a informação com os pares por protocolos de roteamento.
- Um roteador recebe-os pacotes e para a frente à relação correta baseada no endereço de destino.

Os switch de camada 3 de Cisco da extremidade alta podem agora executar esta segunda função, na mesma velocidade que a função de switching de Camada 2. Se você introduz um salto do roteamento e cria uma segmentação adicional da rede, não há nenhuma pena da velocidade. Este diagrama usa o exemplo na ameixa seca VLAN da seção que você não usa como base:



Retire o núcleo de A e de núcleo B são agora alguns switch de camada 3. O VLAN2 e o VLAN3 não são construídos uma ponte sobre já não entre o núcleo A e o núcleo B, tão lá são nenhuma possibilidade para um STP loop.

- A Redundância está ainda atual, com uma confiança em protocolos de roteamento da camada 3. O projeto assegura uma reconvergência que seja mesmo mais rápida do que a reconvergência com STP.
- Há já não toda a porta única que o STP obstruir. Consequentemente, não há nenhum potencial para um Loop de Bridging.
- Não existe penalidade de velocidade, como deixar a VLAN através da Layer 3 Switching ser tão rápido quanto interligar dentro da VLAN.

Há um único inconveniente com este projeto. A migração a este tipo do projeto implica geralmente um rework do método de endereçamento.

Mantenha o STP mesmo se é desnecessário

Mesmo se você sucedeu com a remoção de todos os portos bloqueado de sua rede e você não tem nenhuma redundância física, não desabilite o STP. O STP não é geralmente muito recursos intensivos de processador; o packet switching não envolve o CPU na maioria de switch Cisco. Também, poucos BPDU que são enviados em cada link não reduzem significativamente a largura de banda disponível. Contudo, uma rede de Bridge sem STP pode derreter-se em uma fração de um segundo se um operador faz um erro em um painel de correção, por exemplo. Geralmente, desabilitar o STP em uma rede de Bridge não é valor o risco.

Mantenha o tráfego fora do VLAN administrativo e não tenha um único período VLAN a toda a rede

Um switch Cisco tem tipicamente um único endereço IP de Um ou Mais Servidores Cisco ICM NT que ligue a um VLAN, conhecido como o VLAN administrativo. Neste VLAN, o interruptor comporta-se como um host IP genérico. Em particular, cada transmissão ou pacote de transmissão múltipla são enviados ao CPU. Uma taxa alta a transmissão ou o tráfego multicast no VLAN administrativo pode adversamente impactar do CPU e da capacidade de CPU processar bpdus vital. , Mantenha consequentemente o tráfego de usuário fora do VLAN administrativo.

Até recentemente, não havia nenhuma maneira de remover o VLAN1 de um tronco na implementação Cisco. O VLAN1 serve geralmente como um VLAN administrativo, onde todo o Switches seja acessível na mesma sub-rede IP. Embora útil, esta instalação pode ser perigosa porque um Loop de Bridging no VLAN1 afeta todos os troncos, que podem derrubar a rede inteira. Naturalmente, o mesmo problema existe nenhuma matéria que o VLAN você usa. Tente segmentar os domínios de Bridging com uso de 3 Switch da camada de alta velocidade.

Épossível remover VLAN 1 de troncos desde a Versão do Software Cisco IOS 12.1(11b)E e a versão 5.4 do CatOS. O VLAN1 ainda existe, mas obstrui o tráfego, que impede toda a possibilidade do laço.

Informações Relacionadas

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