Solucionar problemas de ambientes de LAN switching

Introduction

Este documento descreve os recursos comuns do switch LAN e como solucionar quaisquer problemas de switching LAN.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

As seções neste capítulo descrevem os recursos comuns do switch LAN e as soluções para alguns dos problemas mais comuns de switching LAN. Estes tópicos são abordados:

- Introdução à switching de LAN
- Sugestões para solucionar problemas do switch geral
- Solucionar problemas de conectividade de porta
- Solucionar problemas de autonegociação half/full duplex da Ethernet 10/100Mb
- Entroncamento ISL nos switches da família Catalyst 5000 e 6000
- Configurar e solucionar problemas do switch EtherChannel para o switch
- Usar o Portfast e outros comandos para corrigir problemas de conectividade na inicialização da estação final
- Configurar e solucionar problemas de comutação multicamada

Introdução à switching de LAN

Se você não tiver experiência com switching de LAN, estas seções o orientam por alguns dos principais conceitos relacionados aos switches. Um dos pré-requisitos para solucionar problemas de qualquer dispositivo é conhecer as regras sob as quais ele opera. Os switches se tornaram muito mais complexos nos últimos anos, pois eles ganharam em popularidade e sofisticação. Esses parágrafos descrevem alguns dos principais conceitos para conhecer os switches.

Concentradores e Switches

Devido à grande demanda colocada nas redes locais, houve uma mudança de uma rede de largura de banda compartilhada, com hubs e cabo coaxial, para uma rede de largura de banda dedicada, com switches. Um hub permite que vários dispositivos sejam conectados ao mesmo segmento de rede. Os dispositivos nesse segmento compartilham a largura de banda entre si. Se for um hub de 10 MB e houver 6 dispositivos conectados a 6 portas diferentes no hub, todos os seis dispositivos vão compartilhar 10 MB de largura de banda entre si. Um hub de 100 MB compartilha 100 MB de largura de banda entre os dispositivos conectados. Em termos de modelo OSI, um hub é considerado um dispositivo de camada um (camada física). Ele ouve um sinal elétrico no fio e o passa para as outras portas.

Um switch pode substituir fisicamente um hub na rede. Um switch permite que vários dispositivos sejam conectados à mesma rede, assim como um hub faz, mas a semelhança termina aí. Um switch permite que cada dispositivo conectado tenha largura de banda dedicada em vez de compartilhada. A largura de banda entre o switch e o dispositivo é reservada para a comunicação de entrada e saída desse dispositivo apenas. Seis dispositivos conectados a seis portas diferentes em um switch de 10 MB têm 10 MB de largura de banda para operar, em vez de largura de banda compartilhada com outros dispositivos. Um switch pode aumentar muito a largura de banda disponível na rede, o que pode levar ao melhor desempenho da rede.

Ligações e Switches

Um switch básico é considerado um dispositivo de camada dois. Ao usar a palavra camada, você se refere ao modelo OSI de 7 camadas. Um switch não apenas transmite sinais elétricos, como um hub faz; em vez disso, ele monta os sinais em um quadro (camada dois) e decide o que fazer com o quadro. Um switch determina o que fazer com um quadro quando toma emprestado um algoritmo de outro dispositivo de rede comum: uma bridge transparente. Logicamente, um switch atua exatamente como uma ponte transparente, mas pode manipular os quadros muito mais rápido do que ela (devido a um hardware e uma arquitetura especiais). Quando um switch decide para onde o quadro é enviado, ele passa o quadro pela porta (ou portas) apropriada (s). Você pode imaginar um switch como um dispositivo que cria conexões instantâneas entre várias portas, em uma base quadro a quadro.

VLANs

Como o switch decide, a cada quadro, quais portas trocam dados, é natural posicionar a lógica dentro do switch para permitir que ele escolha as portas para agrupamentos especiais. Este agrupamento de portas é chamado de Rede de área local virtual (VLAN). O switch garante que o tráfego de um grupo de portas nunca seja enviado para outros grupos de portas (que seria roteamento). Esses grupos de portas (VLANs) podem ser considerados um segmento de LAN individual.

As VLANs também são descritas como domínios de transmissão. Isso ocorre devido ao algoritmo de transição transparente, que indica que os pacotes de transmissão (pacotes destinados *a todos os endereços de dispositivos) são enviados por todas as portas que estão no mesmo grupo (ou seja, na mesma VLAN).* Todas as portas na mesma VLAN também estão no mesmo domínio de

transmissão.

Algoritmo de Transparent Bridging

O algoritmo de Transparent Bridging e o spanning tree são abordados com mais detalhes em outro lugar (Capítulo 20: Identificação e Solução de Problemas de Ambientes de Transparent Bridging). Quando um switch recebe um quadro, ele deve decidir o que fazer com esse quadro. Ele pode ignorar o quadro; ele pode passar o quadro por outra porta ou pode passar o quadro por muitas outras portas.

Para saber o que fazer com o quadro, o switch aprende o local de todos os dispositivos no segmento. Essas informações de local são colocadas em uma tabela de memória endereçável por conteúdo (CAM - nomeada devido ao tipo de memória usada para armazenar essas tabelas). A tabela CAM mostra, para cada dispositivo, o endereço MAC do dispositivo, a porta em que o endereço MAC pode ser encontrado e à qual VLAN essa porta está associada. O switch aprende continuamente à medida que os quadros são recebidos no switch. A tabela CAM do switch é atualizada continuamente.

Essas informações na tabela CAM são usadas para decidir como é tratado um quadro recebido. Para decidir onde enviar um quadro, o switch examina o endereço MAC de destino em um quadro recebido e pesquisa esse endereço MAC de destino na tabela CAM. A tabela CAM mostra para qual porta o quadro deve ser enviado para que ele alcance o endereço MAC de destino especificado. Estas são as regras básicas que um switch usa para executar a responsabilidade de encaminhamento de quadros:

Se o endereço MAC de destino for encontrado na tabela CAM, o switch envia o quadro para a porta que está associada a esse endereço MAC de destino na tabela CAM. Isso se chama encaminhamento.

Se a porta associada para envio do quadro para saída for a mesma porta em que o quadro veio originalmente, ele será ignorado porque não há necessidade de enviá-lo de volta para a mesma porta. Isso é chamado de filtragem.

Se o endereço MAC de destino não estiver na tabela CAM (o endereço é *desconhecido), o switch envia o quadro para todas as outras portas que estão na mesma VLAN que o quadro recebido.* Isso é chamado de inundação. Ele não inunda o quadro para fora da mesma porta que o quadro foi recebido.

Se o endereço MAC de destino do quadro recebido for o endereço de transmissão (FFFF. FFFF. FFFF), o quadro será enviado para todas as portas que estão na mesma VLAN que o quadro recebido. Isso também é chamado de inundação. O quadro não é enviado para a mesma porta em que o quadro foi recebido.

Spanning Tree Protocol

Como você viu, o algoritmo de Transparent Bridging inunda quadros desconhecidos e de broadcast de todas as portas que estão na mesma VLAN que o quadro recebido. Isso causa um problema potencial. Se os dispositivos de rede que executam esse algoritmo estiverem conectados em um loop físico, os quadros inundados (como difusões) serão transmitidos de switch a switch para sempre e pelo loop. Dependendo das conexões físicas envolvidas, os

quadros podem, na verdade, ser multiplicados exponencialmente devido ao algoritmo de inundação, e isso pode causar sérios problemas de rede.

Há uma vantagem em um loop físico na rede: ele pode fornecer redundância. Se um link falhar, ainda haverá outra maneira de o tráfego poder atingir seu destino. Para permitir os benefícios derivados da redundância, e não quebrar a rede devido à inundação, um protocolo chamado spanning tree foi criado. A abrangência de árvore foi padronizada na especificação IEEE 802.1d.

A finalidade do Spanning Tree Protocol (STP) é identificar e bloquear temporariamente os loops em um segmento de rede ou uma VLAN. Os switches executam o STP e elegem uma bridge raiz ou um switch. Os outros switches medem a distância em relação ao switch raiz. Se existe mais de uma forma de chegar ao switch raiz, há um loop. Os switches rastreiam o algoritmo para determinar quais portas devem ser bloqueadas para quebrar o loop. O STP é dinâmico; se um link no segmento falhar, as portas que estavam originalmente bloqueadas podem ser alteradas para o modo de encaminhamento.

Entroncamento

O entroncamento é um mecanismo usado com mais frequência para permitir que várias VLANs funcionem de forma independente em vários switches. Os roteadores e os servidores também podem usar o entroncamento, o que permite que eles fiquem ativos simultaneamente em várias VLANs. Se sua rede tiver apenas uma VLAN, você não precisará necessariamente de entroncamento; mas se sua rede tiver mais de uma VLAN, você provavelmente desejará aproveitar os benefícios do entroncamento.

Uma porta em um switch normalmente pertence a apenas uma VLAN; presume-se que todo o tráfego recebido ou enviado nessa porta pertença à VLAN configurada. Uma porta de tronco, por outro lado, é uma porta que pode ser configurada para enviar e receber tráfego para muitas VLANs. Isso é feito ao anexar informações de VLAN a cada quadro, um processo chamado *marcação do quadro.* Além disso, o entroncamento deve estar ativo em ambos os lados do link; o outro lado deve esperar quadros que incluam informações de VLAN para que ocorra a comunicação apropriada.

Existem diferentes métodos de entroncamento dependentes da mídia usada. Os métodos de truncamento de Fast Ethernet ou de Gigabit Ethernet são ISL (Link InterSwitch) ou 802.1q. O truncamento via ATM usa LANE. O entroncamento sobre a FDDI usa 802.10.

EtherChannel

EtherChannel é uma técnica usada quando há várias conexões com o mesmo dispositivo. Em vez de cada função de link de forma independente, o EtherChannel agrupa as portas para trabalhar como uma única unidade. Ele distribui o tráfego em todos os links e fornecerá redundância se um ou mais links falharem. As configurações do EtherChannel devem ser iguais em ambos os lados dos enlaces envolvidos no canal. Normalmente, o spanning tree bloquearia todas essas conexões paralelas entre dispositivos, porque são loops, mas o EtherChannel é executado *abaixo do Spanning Tree, para que o spanning tree pense que todas as portas em um determinado EtherChannel são apenas uma única porta.*

Switching Multicamadas (MLS)

O switching multicamada (MLS) é a capacidade de um switch encaminhar quadros com base nas informações do cabeçalho da camada três e, às vezes, da camada quatro. Isso geralmente se aplica a pacotes IP, mas agora também pode ocorrer em pacotes IPX. O switch aprende como

lidar com esses pacotes quando ele se comunica com um ou mais roteadores. Com uma explicação simplificada, o switch observa como o roteador processa um pacote e, em seguida, ele processa futuros pacotes nesse mesmo fluxo. Tradicionalmente, os switches foram muito mais rápidos em quadros de switching que os roteadores, portanto, fazer com que eles aliviem o tráfego do roteador, pode resultar em melhorias significativas na velocidade. Se algo mudar na rede, o roteador pode dizer ao switch para apagar o cache de camada três e compilá-lo do zero novamente conforme a situação evolui. O protocolo utilizado para comunicar com os roteadores é chamado de Protocolo de switching de multicamada (MLSP).

Como aprender sobre esses recursos

Esses são apenas alguns dos recursos básicos dos switches. A cada dia, mais são adicionados. É importante entender como os switches funcionam, quais recursos você usa e como esses recursos precisam funcionar. Um dos melhores lugares para aprender essas informações sobre os switches da Cisco está no site da Cisco. Vá para a seção *Serviço e suporte, escolha Documentos técnicos.* Aqui, escolha a *Página inicial da documentação.* Os conjuntos de documentação para todos os produtos da Cisco podem ser encontrados aqui. O link *Multilayer LAN Switches* leva você à documentação de todos os switches LAN da Cisco. Para aprender sobre os recursos de um switch, leia o *Guia de configuração de software para obter a versão específica do software que você usa.* Os guias de configuração de software fornecem informações detalhadas sobre o que a função do recurso e quais comandos usar para configurá-lo no switch. Todas essas informações estão disponibilizadas gratuitamente na Web. Você nem precisa de uma conta para esta documentação; ela está disponível para qualquer pessoa. Alguns desses guias de configuração podem ser lidos em uma tarde e valem o tempo gasto.

Outra parte do site da Cisco é preenchida pelo site de Suporte e documentação da Cisco. Ele inclui informações projetadas para ajudá-lo a implementar, manter e solucionar problemas da rede. Acesse o site de Suporte e documentação para obter informações detalhadas de suporte por produtos ou tecnologias específicas.

Sugestão para Troubleshooting de Switch Geral

Há muitas maneiras de solucionar problemas de um switch. À medida que os recursos dos switches crescem, também aumenta a possibilidade de falhas. Para solucionar problemas com eficiência, desenvolva uma abordagem ou um plano de teste em vez de uma abordagem de erro. Aqui estão algumas sugestões gerais:

Reserve um tempo para se familiarizar com a operação normal do switch. O site da Cisco tem uma quantidade enorme de informações técnicas que descreve como os switches funcionam, conforme mencionado na seção anterior. Os manuais de configuração são particularmente muito úteis. Muitos casos abertos podem ser resolvidos com informações dos guias de configuração do produto.

- Para as situações mais complexas, tenha um mapa físico e lógico preciso da rede. Um mapa físico mostra como os dispositivos e os cabos estão conectados. Um mapa lógico mostra quais segmentos (VLANs) existem na rede e quais roteadores fornecem serviços de roteamento para esses segmentos. Um mapa de spanning tree é muito útil para solucionar problemas complexos. Devido à capacidade de um switch de criar segmentos diferentes com a implementação de VLANs, as conexões físicas sozinhas não contam toda a história; é preciso saber como os switches são configurados para determinar quais segmentos (VLANs) existem e saber como eles estão logicamente conectados.

Tenha um plano. Alguns problemas e soluções são óbvios; outros não. Os sintomas que você vê na rede podem ser o resultado de problemas em outra área ou camada. Antes chegar a conclusões precipitadas, tente verificar de forma estruturada o que funciona ou não. Como as redes podem ser complexas, é útil isolar possíveis domínios de problema. Uma maneira de fazer isso é usar o modelo OSI de sete camadas. Por exemplo: verifique as conexões físicas envolvidas (camada 1); verifique os problemas de conectividade na VLAN (camada 2) e verifique os problemas de conectividade em diferentes VLANs (camada 3) e assim por diante. Se houver uma configuração correta no switch, muitos dos problemas encontrados estarão relacionados aos problemas da camada física (portas e cabos físicos). Atualmente, os switches estão envolvidos na camada três e quatro apresentam problemas, que incorporam a inteligência para pacotes de switch com base nas informações derivadas dos roteadores ou que realmente têm roteadores que vivem no switch (switching de camada três ou camada quatro).

Não suponha que um componente funcione, você deve primeiro verificá-lo. Isso pode economizar um longo período de tempo. Por exemplo, se um PC não pode fazer login em um servidor na rede, há muitas coisas que podem estar erradas. Não ignore as coisas básicas e assuma que algo funciona; alguém pode ter alterado algo e não ter lhe contado. Leva apenas um minuto para verificar algo básico (por exemplo, se as portas envolvidas estão conectadas ao local correto e ativas), o que pode economizar muitas horas desperdiçadas.

Solucionar problemas de conectividade de porta

Se a porta não funcionar, nada funcionará! As portas são a base da sua rede de switching. Algumas portas têm relevância especial devido à localização na rede e à quantidade de tráfego que carregam. Essas portas incluem conexões com outros switches, roteadores e servidores. Os problemas nessas portas podem ser mais complicados de resolver, pois elas sempre utilizam recursos especiais, como truncamento e EtherChannel. O restante das portas também é significativo, pois conecta os usuários reais da rede.

Muitas coisas podem fazer com que uma porta não funcione: problemas de hardware, problemas de configuração e problemas de tráfego. Essas categorias são exploradas com um pouco mais de profundidade.

Problemas de hardware

General

A funcionalidade de porta requer duas portas ativas conectadas por um cabo ativo (do tipo correto). O padrão da maioria dos switches Cisco é ter uma porta no estado *notconnect* , o que significa que ela não está conectada a nada, mas deseja se conectar. Se você conectar um cabo adequado a duas portas de switch no *notconnect state (estado não conectado), a luz de link se tornará verde para ambas as portas, e o status da porta indicará connected (conectado), o que significa que a porta estará ativa na camada um.* Esses parágrafos destacam os itens que devem ser verificados se a camada um não estiver ativa.

Verifique o status das duas portas envolvidas. Assegure-se de que nenhuma porta envolvida no enlace esteja fechada. Possivelmente, o administrador desativou uma ou ambas as portas. O software dentro do switch pode ter encerrado a porta devido a condições de erro de configuração. Se um lado estiver desligado e o outro não, o status no lado habilitado será *notconnect* (porque ele não detecta um vizinho no outro lado do fio). O status no lado de desligamento indica algo

como *disable (desativado) ou errDisable (dependendo do que realmente desligou a porta).* O link não aparecerá, a menos que ambas as portas estejam ativadas.

Quando você conecta um cabo adequado (novamente, se for do tipo correto) entre duas portas ativadas, elas mostram uma luz de link verde em alguns segundos. Além disso, o estado da porta mostra *connected (conectado) na interface de linha de comando (CLI).* Nesse ponto, se você não tiver um link, seu problema será limitado a três coisas: a porta em um lado, a porta no outro lado ou o cabo no meio. Em alguns casos, há outros dispositivos envolvidos: conversores de mídia (fibra para cobre e assim por diante), ou em links Gigabit você pode ter conectores de interface de gigabit (GBICs). Ainda assim, essa é uma área razoavelmente limitada de pesquisa.

Os conversores de mídia poderão adicionar ruído a uma conexão ou diminuir o sinal se não funcionarem corretamente. Eles também colocam conectores extras que podem causar problemas, sendo outro componente a ser analisado.

Verifique se existem conexões soltas. Às vezes, um cabo parece estar assentado no conector, mas na verdade não está; desconecte o cabo e insira-o novamente. Você também deve procurar sujeira, pinos perdidos ou quebrados. Faça isso para as duas portas envolvidas na conexão.

O cabo pode estar conectado à porta errada, o que normalmente acontece. Certifique-se de que ambas as extremidades do cabo estejam conectadas às portas no local desejado.

Você pode ter um enlace em um lado e não ter no outro. Verifique o link em ambos os lados. Um único cabo quebrado pode provocar esse tipo de problema.

Uma luz de link não garante que o cabo esteja funcionando adequadamente. Pode ter havido estresse físico, que faz com que seja funcional em um nível marginal. Geralmente, você observa isso pela porta que tem muitos erros de pacote.

Para determinar se o cabo é o problema, troque-o por um cabo em bom estado. Não apenas troque-o por qualquer outro cabo; certifique-se de trocá-lo por um cabo que você saiba que é bom e que é do tipo correto.

Caso seja um cabo de execução muito longo (subterrâneo, em um campus grande, por exemplo), é bom ter um testador de cabos sofisticado. Se você não tiver um testador de cabos, considere o seguinte:

- Tente portas diferentes para ver se elas ficam ativas com esse cabo longo.
- Conecte a porta em questão a outra porta no mesmo switch, apenas para ver se a porta está vinculada localmente.
- Realoque temporariamente os switches próximos um do outro, para que você possa experimentar com um cabo ideal e conhecido.

Cobre

Verifique se você tem o cabo correto para o tipo de conexão feita. O cabo categoria 3 pode ser usado para conexões UTP de 10 MB, mas a categoria 5 deve ser usada para conexões 10/100.

Um cabo de conexão direta via RJ-45 é usado em estações finais, roteadores ou servidores para conexão a um switch ou hub. Um cabo Ethernet do tipo Philips é usado para conexões entre

switches ou hup a switch. Este é o pino de um cabo Ethernet do tipo Philips. As distâncias máximas para os fios de cobre Ethernet ou Fast Ethernet são de 100 metros. Uma boa regra geral é que quando você cruza uma camada OSI, como entre um switch e um roteador, use um cabo direto; quando você conecta dois dispositivos na mesma camada OSI, como entre dois roteadores ou dois switches, use um cabo cruzado. Somente para a finalidade desta regra, trate uma estação de trabalho como se fosse um roteador.

Esses dois gráficos mostram os pinos necessários para um cabo cruzado switch a switch.

Fibra

Para fibra, certifique-se de que você tenha o cabo correto para as distâncias envolvidas e o tipo de portas de fibra que é usado (monomodo, multimodo). Verifique se as portas conectadas juntas são de modo único e de vários modos. A fibra monomodo geralmente alcança 10 quilômetros, e a fibra multimodo pode geralmente atingir 2 quilômetros, mas há o caso especial do multimodo 100BaseFX usado no modo half-duplex, que pode ir apenas 400 metros.

Para conexões de fibra, certifique-se de que o condutor de transmissão de uma porta esteja conectado ao condutor de recepção da outra porta e vice-versa; transmitir para transmitir, receber para receber, não funciona.

Com relação a conexões de gigabit, os GBICs precisam ser correspondentes em cada lado da conexão. Há diferentes tipos de GBICs dependentes do cabo e das distâncias envolvidas: comprimento de onda curto (SX), comprimento de onda longo/longo alcance (LX/LH) e distância estendida (ZX).

Um SX GBIC precisa se conectar a um SX GBIC; um SX GBIC não se conecta a um LX GBIC. Além disso, algumas conexões Gigabit exigem cabos de condicionamento dependentes dos tamanhos envolvidos. Consulte as notas de instalação do GBIC.

Se o link de gigabit não for ativado, verifique se as configurações de controle de fluxo e negociação de porta estão consistentes em ambos os lados do link. Poderá haver incompatibilidade na implementação desses recursos, se os switches conectados forem de fornecedores diferentes. Em caso de dúvida, desative esses recursos nos dois switches.

Problemas de configuração

Outra causa de problemas de conectividade de porta é a configuração de software incorreta do switch. Se uma porta tiver uma luz laranja sólida, isso significa que o software dentro do switch desligará a porta, seja por meio da interface do usuário ou por processos internos.

Certifique-se de que o administrador não tenha desligado as portas envolvidas (como mencionado). O administrador pode desativar manualmente a porta em um lado do link ou no outro. Esse link não é ativado até que você reative a porta; verifique o status da porta.

Alguns switches, como o Catalyst 4000/5000/6000, poderão desativar a porta se os processos de software dentro do switch detectarem um erro. Quando você observa o status da porta, ele indica errdisable. Você deve corrigir o problema de configuração e levar a porta para fora do estado de errDisable manualmente. Algumas versões de software mais recentes (CatOS 5.4(1) e posteriores) têm a capacidade de reabilitar automaticamente uma porta após uma quantidade configurável de tempo gasta no estado errDisable. Estas são algumas das causas do estado errDisable:

- **Configuração incorreta do EtherChannel**: se um lado estiver configurado para EtherChannel e

o outro não, isso poderá fazer com que o processo de spanning tree desative a porta no lado configurado para EtherChannel. Se você tentar configurar o EtherChannel, mas as portas envolvidas não tiverem as mesmas configurações (velocidade, duplex, modo de entroncamento e assim por diante) que suas portas vizinhas no link, isso poderá causar o estado errDisable. É melhor definir cada lado como o *modo desejado do EtherChannel, caso você queira usar EtherChannel.* Posteriormente, veremos seções sobre como configurar o EtherChannel.

Incompatibilidade duplex: se a porta do switch receber muitas colisões atrasadas, isso geralmente indica um problema de incompatibilidade duplex. Há outras causas para colisões tardias: uma placa de rede ruim, segmentos de cabo muito longos, mas o motivo mais comum hoje é uma incompatibilidade bidirecional. O lado full-duplex acha que pode enviar sempre que quiser. O lado half-duplex espera apenas pacotes em determinados momentos - não em "qualquer" momento.

BPDU Port-guard: algumas versões mais recentes do software do switch podem monitorar se o portfast está habilitado em uma porta. Uma porta que usa PortFast deve estar conectada a uma estação final, não a dispositivos que geram pacotes de spanning tree chamados BPDUs. Caso o switch observe um BPDU em uma porta com PortFast habilitado, ele coloca a porta no modo errDisable.

UDLD: Unidirectional Link Detection é um protocolo em algumas novas versões de software que descobre se a comunicação em um link é apenas unidirecional. Um cabo de fibra quebrado ou outros problemas de cabo/porta podem causar essa comunicação apenas unidirecional. Esses links parcialmente funcionais podem causar problemas quando os switches envolvidos não sabem que o link foi parcialmente interrompido. Podem ocorrer circuitos de árvore de abrangência com esse problema. O UDLD pode ser configurado para incluir uma porta no estado errDisable, quando detecta um link unidirecional.

Incompatibilidade de VLAN nativa: antes de uma porta ter o entroncamento ativado, ela pertence a uma única VLAN. Se o truncamento estiver ativado, a porta poderá suportar tráfego para vários VLANs. A porta ainda se lembra da VLAN em que estava antes de o entroncamento ter sido ativado, chamada de VLAN nativa. A VLAN nativa é central para o truncamento 802.1q Se a VLAN nativa em cada extremidade do link não corresponder, uma porta entrará no estado errDisable.

Outro: qualquer processo no switch que reconheça um problema com a porta pode colocá-la no estado *errDisable*.

Outra causa de portas inativas é quando o VLAN a que pertencem desaparece. Cada porta em um switch pertence a uma VLAN. Se essa VLAN for excluída, a porta se tornará inativa. Alguns switches mostram uma luz laranja estável em cada porta que isso aconteceu. Se você vir trabalhar um dia e ver centenas de luzes laranja, não entre em pânico; pode ser que todas as portas pertençam à mesma VLAN e alguém acidentalmente excluiu a VLAN à qual as portas pertenciam. Quando você adiciona a VLAN de volta na tabela de VLAN, as portas se tornam ativas novamente. Uma porta se lembra da VLAN atribuída.

Se você tiver um link e as portas parecerem conectadas, mas não for possível estabelecer comunicações com outro dispositivo, isso pode ser particularmente complicado. Geralmente

indica um problema maior que a camada física: camada 2 ou camada 3. Experimente estas coisas.

Verifique o modo de entroncamento em cada lado do enlace. Certifique-se de que ambos os lados estejam no mesmo modo. Se você ativar o modo de entroncamento para "on" (ao contrário de "auto" ou "desirable") para uma porta e a outra porta tiver o entroncamento

definido como "desligado", eles não conseguem se comunicar. O entroncamento altera o formato do pacote; as portas precisam concordar com o formato que usam no link ou não se entendem.

Verifique se todos os dispositivos estão na mesma VLAN. Caso não estejam na mesma VLAN, um roteador deve ser configurado para permitir que os dispositivos se comuniquem.

Certifique-se de que o endereçamento de camada três esteja corretamente configurado.

Problemas de tráfego

Nesta seção, você descreve algumas das coisas que pode aprender ao examinar as informações de tráfego de uma porta. A maioria dos switches tem alguma maneira de rastrear os pacotes quando entram e saem de uma porta. Os comandos que geram esse tipo de saída nos switches Catalyst 4000/5000/6000 são **show portandshow mac**. A saída desses comandos nos switches 4000/5000/6000 é descrita nas referências do comando de switch.

Alguns desses campos de tráfego de porta mostram a quantidade de dados transmitida e recebida na porta. Outros campos mostram quantos quadros de erro são encontrados na porta. Se você tiver uma grande quantidade de erros de alinhamento, erros de FCS ou colisões atrasadas, isso poderá indicar uma incompatibilidade de duplex no fio. Outras causas para esses tipos de erros podem ser problemas de placas de interface de rede ou de cabo incorretos. Se você tiver um grande número de quadros adiados, é um sinal de que seu segmento tem muito tráfego; o switch não é capaz de enviar tráfego suficiente no fio para esvaziar seus buffers. Considere a remoção de alguns dispositivos em outro segmento.

Falha do Hardware do Switch

Se você tentou tudo o que podia imaginar e a porta não funciona, pode haver falha de hardware.

Às vezes, as portas são danificadas pela descarga eletrostática (ESD). Você pode ou não ver qualquer indicação disso.

Veja os resultados do POST (Power-On Self-Test) do switch para ver se houve alguma falha indicada para qualquer parte do switch.

Se você vir um comportamento que possa ser considerado "estranho", isso poderá indicar problemas de hardware ou software. Normalmente, é mais fácil recarregar o software do que obter um novo hardware. Tente trabalhar primeiro com o software do switch.

O sistema operacional pode ter um bug. Caso você carregue um sistema operacional mais recente, ele pode corrigir isso. Você poderá pesquisar bugs conhecidos se ler as notas de da versão do código ou usar o Kit de ferramentas para correção de problemas da Cisco.

O sistema operacional pode ter sido corrompido. Se você recarregar a mesma versão do sistema operacional, poderá corrigir o problema.

Caso a luz de status no switch pisque na cor laranja, isso normalmente significa que há algum tipo de problema de hardware com a porta, o módulo ou o switch. O mesmo ocorre se a porta ou o status do módulo indicafaulty (falha).

Antes de trocar o hardware do switch, você pode tentar alguns procedimentos:

Recoloque o módulo no switch. Se você fizer isso com o equipamento ligado, verifique se o módulo pode trocado ou removido em operação. Em caso de dúvida, desligue o switch antes de recolocar o módulo ou consulte o guia de instalação de hardware. Se a porta for incorporada ao switch, ignore esta etapa.

Reinicializar o switch. Às vezes, isso faz com que o problema desapareça; essa é uma solução alternativa, não uma correção.

Verifique o software do switch. Se essa for uma nova instalação, lembre-se de que alguns componentes só podem funcionar com determinadas versões do software. Verifique as notas de versão ou o guia de instalação e configuração de hardware para o componente que você instalou.

Se estiver razoavelmente certo de que você tem um problema de hardware, substitua o componente defeituoso.

Identificar E Solucionar Problemas De Autonegociação Half/Full Duplex Da Ethernet 10/100Mb

Objetivos

Esta seção apresenta informações gerais usadas para solucionar problemas e uma discussão de técnicas para solucionar problemas de autonegociação da Ethernet.

Esta seção mostra como determinar o comportamento atual de um enlace. Mostra como os usuários podem controlar o comportamento, bem como explicações sobre situações de falha na autonegociação.

Muitos Cisco Catalyst Switches e muitos Cisco Routers suporte negociação automática. Esta seção se concentra na autonegociação entre switches Catalyst 5000. Os conceitos explicados aqui também podem ser aplicados a outros tipos de dispositivos.

Introduction

A negociação automática é uma função opcional do padrão IEEE 802.3u Fast Ethernet que habilita dispositivos para trocar informações automaticamente em um link sobre habilidades de velocidade e dúplex.

A auto-negociação é destinada às portas, que são alocadas a áreas pelas quais os dispositivos ou usuários transitórios se conectam a uma rede. Por exemplo, várias empresas oferecem escritórios ou cubos compartilhados para os gerentes financeiros e os engenheiros de sistema usarem quando estão no escritório e não fora dele. Cada escritório ou cubo tem uma porta Ethernet permanentemente conectada à rede do escritório. Como não é possível garantir que cada usuário tenha 10 MB, uma Ethernet de 100 MB ou uma placa de 10/100 MB no notebook, as portas do switch que lidam com essas conexões devem ser capazes de negociar a velocidade e o modo duplex. A alternativa é capaz de fornecer uma porta de 10 MB e 100 MB em cada escritório ou cubo e rotulá-las da maneira apropriada.

A autonegociação não deve ser usada para portas que aceitam dispositivos de infraestrutura de rede, como switches e roteadores, ou outros sistemas finais não transitórios, como servidores e impressoras. Embora a autonegociação para velocidade e duplex seja normalmente o comportamento padrão nas portas de switch compatíveis, as portas conectadas a dispositivos fixos devem sempre ser configuradas para o comportamento correto, em vez de permitirem a negociação. Isso elimina qualquer possível problema de negociação e garante que você sempre saiba exatamente como as portas precisam operar. Por exemplo, um link de switch a switch Ethernet de 10/100BaseTX configurado para 100 MB full-duplex só funciona nessa velocidade e nesse modo. As portas não podem fazer o downgrade do link para uma velocidade mais lenta dentro de uma redefinição de porta ou de switch. Caso as portas não possam operar como configuradas, elas não devem ter tráfego. Por outro lado, um enlace switch a switch que recebeu permissão para negociar seu comportamento pode operar em half-duplex de 10 Mb. Geralmente, um link não funcional é mais fácil de descobrir que um link funcional mas que não opera na velocidade ou no modo esperado.

Uma das causas mais comuns de problemas de desempenho em links Ethernet 10/100Mb é quando uma porta no link opera em half-duplex, enquanto a outra porta opera em full-duplex. Às vezes, isso acontece quando uma das portas de um link ou ambas são reiniciadas e o processo de autonegociação não resulta na mesma configuração para os dois parceiros do link. Isso também ocorre quando usuários reconfiguram um lado de um enlace e esquecem de configurar o outro. Muitas chamadas de suporte relacionadas ao desempenho serão evitadas se você criar uma política que exija que as portas de todos os dispositivos não transitórios sejam configuradas para o comportamento necessário, além de impor a política com medidas adequadas de controle de alterações.

Identificar e Solucionar Problemas de Autonegociação Ethernet Entre Dispositivos de Infraestrutura de Rede

Procedimentos e/ou cenários

Cenário 1. Cat 5K com Fast Ethernet

Tabela 22-2: Problemas de conectividade da negociação automática

Possível problema	Solução
O comportamento atual do link é negociado automaticamente?	1. Use o comando **show port mod_num/port**_number para determinar o comportamento atual do link. Se os dois parceiros de link (interfaces em cada extremidade do link) indicarem ter um prefixo "a-" nos campos de status de duplex e velocidade, a autonegociação provavelmente foi bem-sucedida.
autonegociação não suportada.	2. Emita o comando **show port capabilities mod_num/port**_number para verificar se seus módulos

a autonegociação não funciona nos switches Catalyst.	suportam autonegociação. 3. Use o comando automático **set port speed mod_num/port_num** em um Catalyst para configurar a negociação automática. 4. Experimente portas ou módulos diferentes. 5. Tente redefinir as portas. 6. Tente diferentes cabos de correção. 7. Desligue e ligue os dispositivos novamente.
a autonegociação não funciona em roteadores Cisco.	8. Emita o comando Cisco IOS correto para ativar a autonegociação (se disponível) 9. Tente interfaces diferentes. 10. Tente redefinir as interfaces. 11. Tente diferentes cabos de correção. 12. Desligue e ligue os dispositivos novamente.

Exemplo de Autonegociação de Configuração e Troubleshooting de Ethernet 10/100Mb

Esta seção passa por um exame do comportamento de uma porta Ethernet 10/100Mb que suporta autonegociação. Também mostra como fazer alterações no comportamento padrão e como restaurá-lo para o comportamento padrão.

Tarefas a executar

Analisar as capacidades das portas.

Configurar a auto-negociação para a porta 1/1 em ambos os interruptores.

Determine se a velocidade e o modo duplex estão definidos para negociação automática.

Altere a velocidade na porta 1/1 no switch A para 10 MB.

Entendendo o significado do prefixo "a-" nos campos de status de duplex e velocidade.

Visualize o status duplex da porta 1/1 no Switch B.

Compreenda o erro de incompatibilidade bidirecional.

Compreenda as mensagens de erro de spanning tree.

Mude o modo duplex para half na porta 1/1 no interruptor A.

Ajuste o modo duplex e a velocidade da porta 1/1 no switch B.

Restaure o modo duplex padrão e a velocidade às portas 1/1 em ambos os interruptores.

Veja as mudanças do status de porta em ambos os interruptores.

Passo a passo

Execute estas etapas:

O comando show port capabilities 1/1 exibe os recursos de uma porta de Ethernet 10/100BaseTX 1/1 no Switch A.

Digite este comando para as duas portas que você solucionar os problemas. Ambas as portas devem suportar as capacidades de velocidade e duplex mostradas se elas devem usar autonegociação.

```
Switch-A> (enable) show port capabilities 1/1
Model WS-X5530
Port 1/1
Type 10/100BaseTX
Speed auto,10,100
Duplex half, full
```

A autonegociação é configurada para o modo de velocidade e duplex na porta 1/1 de ambos os switches se você inserir o comando **set port speed 1/1 auto** (auto é o padrão para portas que suportam autonegociação).

```
Switch-A> (enable) set port speed 1/1 auto
Port(s) 1/1 speed set to auto detect.
Switch-A (enable)
```

Observação: o **comando set port speed {mod_num/port_num} auto** também define o modo duplex como auto. Não há comando automático {mod_num/port_num} para ajuste da porta bidirecional.

O comando **show port 1/1** exibe o status das portas 1/1 nos Switches A e B.

```
Switch-A> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- -----
 1/1               connected  1          normal a-full a-100 10/100BaseTX

Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- -----
 1/1               connected  1          normal a-full a-100 10/100BaseTX
```

Observe que a maior parte da saída normal do comando show port {num_mod/num_port} foi omitida.

Os prefixos "a-" em "full" e "100" indicam que essa porta não foi codificada por hardware

(configurada) para um modo ou velocidade duplex específico. Portanto, ele pode negociar automaticamente o modo duplex e a velocidade se o dispositivo ao qual está conectado (seu parceiro de link) também puder negociar automaticamente o modo duplex e a velocidade. Observe também que o status é "conectado" em ambas as portas, o que significa que um pulso de enlace foi detectado na outra porta. O status pode ser “connected” (conectado), mesmo se o dúplex tiver sido negociado ou configurado de forma incorreta.

Para demonstrar o que acontece quando um parceiro de link negocia automaticamente e o outro parceiro de link não negocia, a velocidade na porta 1/1 no Switch A é definida como 10Mb com o comando **set port speed 1/1 10**.

```
Switch-A> (enable) set port speed 1/1 10
Port(s) 1/1 speed set to 10Mbps.
Switch-A> (enable)
```

Observação: se você codificar a velocidade em uma porta, ela desativará toda a funcionalidade de autonegociação na porta para velocidade e duplex.

Quando uma porta tiver sido configurada para uma velocidade, seu modo duplex será automaticamente configurado para o modo negociado anteriormente. Nesse caso, full-duplex. Quando você inseriu o comando set port speed 1/1 10, isso fez com que o modo duplex na porta 1/1 fosse configurado como se o comando set port duplex 1/1 full também tivesse sido inserido. Isso é explicado em seguida.

Compreenda o significado do prefixo "a-" nos campos de status duplex e velocidade.

A ausência do prefixo "a-" nos campos de status da saída do comando **show port 1/1** no Switch A mostra que o modo duplex agora está configurado para "full" e a velocidade agora está configurada para "10".

```
Switch-A> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal  full  10    10/100BaseTX
```

O comando **show port 1/1** no Switch B indica que a porta agora opera em half-duplex e 10Mb.

```
Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal a-half a-10  10/100BaseTX
```

Esta etapa mostra que é possível para um parceiro de enlace detectar a velocidade em que o outro parceiro de enlace opera, mesmo que o outro parceiro de enlace não seja configurado para a auto-negociação. Detectar o tipo de sinal elétrico que chega para descobrir se é 10Mb ou 100Mb faz isso. Foi assim que o Switch B determinou que a porta

1/1 deve operar a 10Mb.

Não é possível detectar o modo de bidirecional correto da mesma forma que a velocidade correta pode ser detectada. Nesse caso, onde a porta 1/1 do switch B está configurada para a autonegociação, exceto a porta do switch A, a porta 1/1 do switch B foi forçada a selecionar o modo duplex padrão. Nas portas Catalyst Ethernet, o modo padrão é a negociação automática e, se isso falhar, half-duplex.

Esse exemplo mostra também que um enlace pode ser conectado com êxito quando houver uma incompatibilidade nos modos duplex. A porta 1/1 no Switch A está configurada para full-duplex, enquanto a porta 1/1 no Switch B definiu como padrão o half-duplex. Para evitar isso, sempre configure os dois parceiros de link.

O prefixo "a-" nos campos de status do Duplex e Speed nem sempre significa que o comportamento atual foi negociado. Às vezes, isso significa apenas que a porta não foi configurada para um modo de velocidade ou duplex. A saída anterior do Switch B mostra Duplex como "a-half" e Speed como "a-10", que indica que a porta opera a 10Mb no modo half-duplex. Neste exemplo, o parceiro de link nessa porta (porta 1/1 no Switch A) está configurado para "full" e "10Mb". Não foi possível para a porta 1/1 no Switch B ter negociado automaticamente seu comportamento atual. Isso prova que o prefixo "a-" indica apenas uma disposição para executar a autonegociação, mas não que a autonegociação realmente ocorreu.

Entenda a mensagem de erro de incompatibilidade de duplex.

Esta mensagem sobre uma incompatibilidade de modo duplex é exibida no switch A depois que a velocidade na porta 1/1 foi alterada para 10 MB. A incompatibilidade foi causada pela porta 1/1 do Switch B, que assume como padrão o half-duplex porque detectou que seu parceiro de link não podia mais executar a autonegociação.

```
%CDP-4-DUPLEXMISMATCH:Full/half-duplex mismatch detected o1
```

Éimportante observar que esta mensagem é criada pelo Protocolo de descoberta Cisco (CDP), e não pelo protocolo de autonegociação 802.3. O CDP pode relatar os problemas que ele descobre, mas normalmente não os corrigirá automaticamente. Uma incompatibilidade de duplex pode ou não resultar em uma mensagem de erro. Outra indicação de uma incompatibilidade duplex são o rápido aumento do FCS e erros de alinhamento no lado half-duplex e "runts" na porta full-duplex (como visto em uma **sh port {mod_num/port_num}**).

Entenda as mensagens de spanning tree.

Além da mensagem de erro de incompatibilidade de duplex, você também pode ver essas mensagens de spanning tree ao alterar a velocidade em um link. Uma discussão sobre Spanning Tree está além do escopo deste documento; consulte o capítulo sobre Spanning Tree para obter mais informações sobre Spanning Tree.

```
%PAGP-5-PORTFROMSTP:Port 1/1 left bridge port 1/1
%PAGP-5-PORTTOSTP:Port 1/1 joined bridge port 1/1
```

Para demonstrar o que acontece quando o modo duplex foi configurado, o modo na porta 1/1 no switch A é definido como half com o comando set port duplex 1/1 half.

```
Switch-A> (enable) set port duplex 1/1 half
Port(s) 1/1 set to half-duplex.
Switch-A> (enable)
```

O comando show port 1/1 mostra a alteração no modo Duplex nessa porta.

```
Switch-A> (enable) sh port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal half   10    10/100BaseTX
```

Neste momento, as portas 1/1 em ambos os interruptores operam-se em half duplex. A porta 1/1 no switch B ainda está configurada para autonegociação, como mostrado nesta saída do comando show port 1/1.

```
Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal a-half a-10  10/100BaseTX
```

Esta etapa mostra como configurar o modo duplex na porta 1/1 no switch B para half. Isso é compatível com a política recomendada para configurar os dois parceiros de link da mesma forma.

Para implementar a política de forma a configurar os dois parceiros de link para o mesmo comportamento, essa etapa agora define o modo duplex como half e a velocidade como 10 na porta 1/1 no switch B.

Esta é a saída quando você insere o comando **set port duplex 1/1 half** no Switch B:

```
Switch-B> (enable) set port duplex 1/1 half
Port 1/1 is in auto-sensing mode.
Switch-B> (enable)
```

O comando set port duplex 1/1 half falhou porque esse comando não é válido caso a autonegociação esteja ativada. Isto igualmente significa que este comando não desabilita a auto-negociação. A autonegociação só pode ser desativada com set port speed {mod_num/port_num {10 comando **| 100} }**.

Esta é a saída quando você insere o comando **set port speed 1/1 10** no Switch B:

```
Switch-B> (enable) set port speed 1/1 10
Port(s) 1/1 speed set to 10Mbps.
Switch-B> (enable)
```

Agora, o comando set port duplex 1/1 half no switch B funciona:

```
Switch-A> (enable) set port duplex 1/1 half
Port(s) 1/1 set to half-duplex.
Switch-A> (enable)
```

O comando show port 1/1 no Switch B mostra que as portas estão configuradas para semi-dúplex e 10Mb.

```
Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal half   10    10/100BaseTX
```

> **Observação**: o **conjunto de porta duplex {mod_num/port_num {half | full }}** depende da **velocidade de porta {mod_num/port_num {10** comando **| 100 }}**. Ou seja, você deve definir a velocidade antes de definir o modo bidirecional.

Configure as portas 1/1 em ambos os switches para negociar automaticamente com o comando **set port speed 1/1 aut**.

```
Switch-A> (enable) set port speed 1/1 auto
Port(s) 1/1 speed set to auto detect.
Switch-A> (enable)
```

> **Observação**: depois que um modo duplex de uma porta tiver sido configurado para algo diferente de automático, a única maneira de configurar a porta para detectar automaticamente seu modo duplex é emitir o comando **set port speed {mod_num/port_num} auto**. Não há comando automático {mod_num/port_num} para ajuste da porta bidirecional. Em outras palavras, se você executar o comando **set port speed {mod_num/port_num} auto**, ele redefinirá a detecção de velocidade da porta e a detecção do modo duplex como auto.

Examine o status das portas 1/1 em ambos os switches com o comando show port 1/1.

```
Switch-A> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal a-full a-100 10/100BaseTX
Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal a-full a-100 10/100BaseTX
```

Ambas as portas são ajustadas agora a seu comportamento padrão da auto-negociação. Ambas as portas negociaram full duplex e 100Mb.

Antes de ligar para a equipe de suporte técnico da Cisco Systems

Antes de ligar para o site de suporte técnico da Cisco Systems, certifique-se de ter lido este artigo e concluído as ações sugeridas para os problemas do seu sistema. Além disso, documente os resultados para que a Cisco possa ajudá-lo melhor a:

Capture a saída **de show** versionde todos os dispositivos afetados.

Capture a saída do comando show port mod_num/port_num de todas as portas afetadas.

Capture a saída do comando show port mod_num/port_num capabilities em todas as portas afetadas.

Configurar Conexões Switch a Switch EtherChannel nos Switches Catalyst 4000/5000/6000

O EtherChannel permite que vários links físicos Fast Ethernet ou Gigabit Ethernet sejam combinados em um canal lógico. Isso permite que o tráfego entre os links carregue o compartilhamento no canal, bem como redundância no caso de um ou mais links no canal falharem. O EtherChannel pode ser usado para interconectar switches LAN, roteadores, servidores e clientes através de cabeamento de par trançado não blindado (UTP) ou fibra monomodo e multimodo.

EtherChannel é um meio fácil para agregar largura de banda entre dispositivos de rede críticos. No Catalyst 5000, um canal pode ser criado com base em duas portas que o tornam um link de 200 Mbps (full-duplex de 400 Mbps) ou quatro portas que o tornam um link de 400 Mbps (full-duplex de 800 Mbps). Algumas placas e plataformas também suportam Gigabit EtherChannel e podem utilizar de duas a oito portas em um EtherChannel. O conceito é o mesmo, independente das velocidades e do número de enlace envolvidos. Normalmente, o protocolo STP considera esses links redundantes entre dois dispositivos como loops e define os links redundantes para o modo de bloqueio. Isso efetivamente torna esses links inativos (que fornecem apenas recursos de backup se o link principal falhar). Quando você usa o Cisco IOS 3.1.1 ou posterior, o spanning tree trata o canal como um link grande, de modo que todas as portas do canal possam estar ativas ao mesmo tempo.

Esta seção orienta você pelas etapas para configurar EtherChannel entre dois switches Catalyst 5000 e mostra os resultados dos comandos à medida que são executados. Os switches Catalyst 4000 e 6000 podem ter sido usados nos cenários apresentados neste documento para obter os mesmos resultados. Para o Catalyst 2900XL e 1900/2820, a sintaxe do comando é diferente, mas os conceitos de EtherChannel são os mesmos.

O EtherChannel pode ser configurado manualmente se você digitar os comandos apropriados ou pode ser configurado de forma automática se o switch negociar o canal com o outro lado usando o PAgP (Port Aggregation Protocol). É recomendável usar o modo desejado de PAgP para

configurar o EtherChannel sempre que possível, pois a configuração manual de EtherChannel pode criar complicações. Este documento fornece exemplos de como configurar o EtherChannel manualmente e exemplos de como configurar EtherChannel com PAgP. Também foram incluídas informações sobre como fazer troubleshooting do EtherChannel e como usar o truncamento com o EtherChannel. Neste documento, os termos EtherChannel, Fast EtherChannel, Gigabit EtherChannel ou canal se referem a EtherChannel.

Contents

Esta figura ilustra este ambiente de teste. A configuração dos switches foi apagada com o comando clear config all. Em seguida, o prompt foi alterado com o comando set system name. Um endereço IP e uma máscara foram atribuídos ao switch para fins de gerenciamento com **set int sc0 172.16.84.6 255.255.255.0** para o SwitchA e **set int sc0 172.16.84.17 255.255.255.0< /strong>para o SwitchB. Um gateway padrão foi atribuído a ambos os switches com set ip route default 172.16.84.1.**

As configurações do switch foram apagadas para que começassem a partir das condições padrão. Os switches receberam nomes para identificá-los a partir do prompt na linha de comando. Os endereços IP foram atribuídos para que você pudesse fazer ping entre os switches para testá-los. O gateway padrão não foi usado.

Muitos dos comandos exibem mais saída do que o necessário. A saída estranha é excluída deste documento.

Tarefas para a configuração manual de EtherChannel

Esta é uma sinopse de instruções para configurar manualmente o EtherChannel:

- Mostre a versão e os módulos do Cisco IOS usados neste documento.
- Certifique-se de que o EtherChannel seja compatível com as portas.
- Verifique se as portas estão conectadas e funcionando.

Verifique se as portas a serem agrupadas têm as mesmas configurações.

Identificar grupos de porta válidos.

Crie o canal.

Passo a passo

Estas são as etapas para configurar manualmente o EtherChannel.

O comando **show** version exibe a versão do software que o switch executa. O comando **show** module lista os módulos instalados no switch.

```
Switch-A show version
WS-C5505 Software, Version McpSW: 4.5(1) NmpSW: 4.5(1)
Copyright (c) 1995-1999 by Cisco Systems
?

Switch-A show module
Mod Module-Name         Ports Module-Type           Model    Serial-Num Status
--- ------------------- ----- --------------------- --------- --------- -------
1                       0     Supervisor III        WS-X5530  006841805 ok
2                       24    10/100BaseTX Ethernet WS-X5225R 012785227 ok
?
```

Verifique se o EtherChannel é suportado nas portas, **show port** capabilities aparece nas versões 4.x e superiores. Se você tiver um Cisco IOS anterior ao 4.x, ignore esta etapa. Nem todos os módulos Fast Ethernet suportam EtherChannel. Alguns dos módulos de EtherChannel originais têm "Fast EtherChannel" gravados no canto inferior esquerdo do módulo (quando você encontrá-lo no switch), o que indica que o recurso é compatível. Essa convenção foi abandonada em módulos posteriores. Os módulos deste teste não indicam "Fast EtherChannel", mas oferecem suporte ao recurso.

```
Switch-A show port capabilities
Model                   WS-X5225R
Port                    2/1
Type                    10/100BaseTX
Speed                   auto,10,100
Duplex                  half,full
Trunk encap type        802.1Q,ISL
Trunk mode              on,off,desirable,auto,nonegotiate
Channel                 2/1-2,2/1-4
Broadcast suppression   percentage(0-100)
Flow control            receive-(off,on),send-(off,on)
```

```
Security                yes
Membership              static,dynamic
Fast start              yes
Rewrite                 yes
Switch-B show port capabilities
Model                   WS-X5234
Port                    2/1
Type                    10/100BaseTX
Speed                   auto,10,100
Duplex                  half,full
Trunk encap type        802.1Q,ISL
Trunk mode              on,off,desirable,auto,nonegotiate
Channel                 2/1-2,2/1-4
Broadcast suppression   percentage(0-100)
Flow control            receive-(off,on),send-(off,on)
Security                yes
Membership              static,dynamic
Fast start              yes
Rewrite                 no
```

Uma porta que não suporta EtherChannel parece com esta:

```
Switch show port capabilities
Model                   WS-X5213A
Port                    2/1
Type                    10/100BaseTX
Speed                   10,100,auto
Duplex                  half,full
Trunk encap type        ISL
Trunk mode              on,off,desirable,auto,nonegotiate
Channel                 no
Broadcast suppression   pps(0-150000)
Flow control            no
Security                yes
Membership              static,dynamic
Fast start              yes
```

Verifique se as portas estão conectadas e funcionando. Antes de conectar os cabos, este é o status da porta.

```
Switch-A show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     notconnect 1          normal   auto  auto 10/100BaseTX
 2/2                     notconnect 1          normal   auto  auto 10/100BaseTX
 2/3                     notconnect 1          normal   auto  auto 10/100BaseTX
```

```
 2/4                    notconnect 1          normal   auto  auto 10/100BaseTX
```

Depois de conectar os cabos entre os dois switches, este é o status.

```
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/4

Switch-A show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     connected  1          normal a-full a-100 10/100BaseTX
 2/2                     connected  1          normal a-full a-100 10/100BaseTX
 2/3                     connected  1          normal a-full a-100 10/100BaseTX
 2/4                     connected  1          normal a-full a-100 10/100BaseTX
Switch-B show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     connected  1          normal a-full a-100 10/100BaseTX
 2/2                     connected  1          normal a-full a-100 10/100BaseTX
 2/3                     connected  1          normal a-full a-100 10/100BaseTX
 2/4                     connected  1          normal a-full a-100 10/100BaseTX
```

Como as configurações do switch foram limpas antes do início do teste, as portas estão nas condições padrão. Todas elas estão em vlan1 e sua velocidade e duplex estão configuradas para auto. Após a conexão dos cabos, elas negociam com uma velocidade de 100Mbps e full-duplex. O status é conectado, assim você pode fazer ping no outro switch.

```
Switch-A ping 172.16.84.17
172.16.84.17 is alive
```

Em sua rede, você pode definir as velocidades manualmente para 100 Mbps e full duplex em vez de depender da autonegociação, já que provavelmente deseja que suas portas sempre funcionem na velocidade mais rápida. Para uma discussão sobre autonegociação, consulte a seçãoTroubleshooting de Autonegociação Half/Half/Full Duplex da Ethernet 10/100Mb.

Verifique se as portas a serem agrupadas têm as mesmas configurações. Esse é um ponto importante que é abordado com mais detalhes na seção de solução de problemas. Se o comando para configurar EtherChannel não funcionar, geralmente, é porque as portas envolvidas no canal têm configurações diferentes. Isso inclui as portas no outro lado do link, bem como as portas locais. Nesse caso, como as configurações do switch foram limpas antes do início desse teste, as portas estão em suas condições padrão. Todos estão em vlan1; sua velocidade e duplex são definidos como auto e todos os parâmetros de spanning tree para cada porta são definidos da mesma forma. A saída mostra que, depois que os cabos são conectados, as portas negociam uma velocidade de 100 Mbps e full-duplex. Como o spanning tree é executado para cada VLAN, é mais fácil apenas configurar o canal

e responder às mensagens de erro do que tentar e verificar cada campo spanning tree para obter consistência para cada porta e VLAN no canal.

Identifique grupos válidos de portas. No Catalyst 5000, apenas algumas portas podem ficar juntas em um canal. Essas dependências restritivas não se aplicam a todas as plataformas. As portas em um canal no Catalyst 5000 devem ser contíguas. Observe pelo comando **show port** capabilities que, para a porta 2/1, estas são as combinações possíveis:

```
Switch-A show port capabilities
Model                   WS-X5225R
Port                    2/1
Channel                 2/1-2,2/1-4
```

Observe que essa porta pode ser uma parte de um grupo de dois (2/1-2) ou parte de um grupo de quatro (2/1-4). Há algo chamado de controlador de agrupamento Ethernet (EBC) no módulo que causa essas limitações de configuração. Examine outra porta.

```
Switch-A show port capabilities 2/3
Model                   WS-X5225R
Port                    2/3
Channel                 2/3-4,2/1-4
```

Essa porta pode ser agrupada em um grupo de duas portas (2/3-4) ou em um grupo de quatro (2/1-4).

Observação: dependendo do hardware, pode haver restrições adicionais. Em determinados módulos (WS-X5201 e WS-X5203), você não pode formar uma EtherChannel com as duas últimas portas em um "grupo de porta", a menos que as duas primeiras portas no grupo já formem um EtherChannel. Um "grupo de porta" é o que tem permissão para formar uma EtherChannel (2/1-4 é um grupo de portas neste exemplo). Por exemplo, se você criar EtherChannels separados com apenas duas portas em um canal, não será possível atribuir as portas 2/3-4 a um canal até que as primeiras portas 2/1-2 sejam configuradas para um canal, para os módulos que têm essa restrição! Da mesma forma, antes de configurar as portas 2/6-7, você deve configurar as portas 2/5-6. Essa restrição não ocorre nos módulos usados para este documento (WS-X5225R, WS-X5234).

Como você configura um grupo de quatro portas (2/1-4), ele está dentro do agrupamento aprovado. não é possível atribuir um grupo de quatro às portas 2/3-6. Esse é um grupo de portas contíguas, mas elas não começam no limite aprovado, como mostrado pelo comando **show port** capabilities (os grupos válidos seriam as portas 1-4, 5-8, 9-12, 13-16, 17-20, 21-24).

Crie o canal. Para criar o canal, use o comando **commandset port channel <mod/port** on para cada switch. é recomendável desativar as portas em um lado do canal ou no outro lado com o comando **set port** disableantes de ativar o EtherChannel manualmente. Isso evita possíveis problemas com o spanning tree no processo de configuração. O spanning tree pode desligar algumas portas (com um status de porta de "errdisable") se um lado estiver configurado como um canal, antes que o outro lado possa ser configurado como um canal. Devido a essa possibilidade, é muito mais fácil criar EtherChannels com PAgP, conforme

explicado posteriormente neste documento. Para evitar essa situação quando você configura o EtherChannel manualmente, você desabilita as portas no SwitchA, configura o canal no SwitchA, configura o canal no SwitchB e reabilita as portas no SwitchA.

Primeiro, verifique se a canalização *está desativada*.

```
Switch-A (enable) show port channel
No ports channelling
Switch-B (enable) show port channel
No ports channelling
```

Agora desative as portas no SwitchA até que os dois switches tenham sido configurados para EtherChannel, de modo que o spanning tree não gere erros e desligue as portas.

```
Switch-A (enable) set port disable 2/1-4
Ports 2/1-4 disabled.
[output from SwitchA upon disabling ports]
1999 Dec 15 00:06:40 %PAGP-5-PORTFROMSTP:Port 2/1 left bridg1
1999 Dec 15 00:06:40 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 15 00:06:40 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 15 00:06:40 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
```

Gire o toon do modo de canal para o Switch A.

```
Switch-A (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.
```

Verifique o status do canal. Observe que o modo de canal foi definido como *toon*, mas o status das portas é desabilitado (porque você desabilitou e não antes). O canal não está operacional neste ponto, mas se torna operacional quando as portas estão ativadas.

```
Switch-A (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  disabled   on        channel
 2/2  disabled   on        channel
 2/3  disabled   on        channel
 2/4  disabled   on        channel
----- ---------- --------- ----------- ------------------------- ----------
```

Because SwitchA ports were (temporarily) disabled, SwitchB ports no longer have a connection. Essa mensagem é exibida no console de SwitchB, quando as portas do SwitchA foram desativadas.

```
Switch-B (enable)
2000 Jan 13 22:30:03 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
2000 Jan 13 22:30:04 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 13 22:30:04 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 13 22:30:04 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
```

Ative o canal para o SwitchB.

```
Switch-B (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.
```

Verifique se o modo de canal está ativado para SwitchB.

```
Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  notconnect on        channel
 2/2  notconnect on        channel
 2/3  notconnect on        channel
 2/4  notconnect on        channel
----- ---------- --------- ----------- ------------------------- ----------
```

Observe que o modo de canal para o SwitchB está ligado, mas o status das portas *nãoconecta*. Isto acontece porque as portas do Switch A ainda estão desabilitadas.

Finalmente, o último passo é ativar as portas no Switch A.

```
Switch-A (enable) set port enable 2/1-4
Ports 2/1-4 enabled.
1999 Dec 15 00:08:40 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
1999 Dec 15 00:08:40 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
1999 Dec 15 00:08:40 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
1999 Dec 15 00:08:40 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4
```

Verificar a configuração

Para verificar se o canal está configurado corretamente, execute o comando **show port** channel.

```
Switch-A (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  on        channel     WS-C5505    066509957(Sw  2/1
 2/2  connected  on        channel     WS-C5505    066509957(Sw  2/2
```

```
 2/3  connected  on        channel     WS-C5505    066509957(Sw  2/3
 2/4  connected  on        channel     WS-C5505    066509957(Sw  2/4
----- ---------- --------- ----------- ------------------------ ----------

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                 Neighbor
                 mode      status      device                   port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  connected  on        channel     WS-C5505    066507453(Sw  2/1
 2/2  connected  on        channel     WS-C5505    066507453(Sw  2/2
 2/3  connected  on        channel     WS-C5505    066507453(Sw  2/3
 2/4  connected  on        channel     WS-C5505    066507453(Sw  2/4
----- ---------- --------- ----------- ------------------------ ----------
```

O spanning tree é mostrado para tratar as portas como uma porta lógica neste comando. Quando a porta é listada como*2/1-4*, o spanning tree trata as portas 2/1, 2/2, 2/3 e 2/4 *como uma única porta*.

```
Switch-A (enable) show spantree
VLAN 1
Spanning tree enabled
Spanning tree type          ieee

Designated Root             00-10-0d-b2-8c-00
Designated Root Priority    32768
Designated Root Cost        8
Designated Root Port        2/1-4
Root Max Age   20 sec    Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-90-92-b0-84-00
Bridge ID Priority          32768
Bridge Max Age 20 sec    Hello Time 2  sec   Forward Delay 15 sec

Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-Method
--------- ----  -------------  -----  --------  ----------  ------------
 2/1-4    1     forwarding         8        32   disabled       channel
```

Os EtherChannel podem ser implementados com diferentes maneiras de distribuição de tráfego nas portas em um canal. A especificação do EtherChannel não determina como o tráfego deve ser distribuído pelos links em um canal. O Catalyst 5000 usa o último bit ou os dois últimos bits (conforme a quantidade de links no canal) dos endereços MAC de origem e destino no quadro, para determinar qual porta no canal usar. Você vê quantidades semelhantes de tráfego em cada porta do canal, se esse tráfego for gerado por uma distribuição normal de endereços MAC em um lado do canal ou no outro. Para verificar se o tráfego passa por todas as portas no canal, você pode usar o comando **show** mac. Se suas portas estavam ativas antes de você configurar o EtherChannel, você pode redefinir os contadores de tráfego para zero pelo comando **clear** counterse, em seguida, os valores de tráfego representam como o EtherChannel distribuiu o tráfego.

Neste ambiente de teste, você não obteve uma distribuição real porque não há estações de trabalho, servidores ou roteadores que geram tráfego. Os únicos dispositivos que geram tráfego são os próprios switches. Você emitiu alguns pings do SwitchA para o SwitchB e pode dizer que o tráfego unicast usa a primeira porta no canal. As informações de Recebimento, neste caso (Rcv-Unicast), mostram como o Switch B distribuiu o tráfego através do canal para o Switch A. Um pouco mais abaixo na saída, as Informações de transmissão (Xmit-Unicast) mostram como o

Switch A distribuiu o tráfego através do canal para o Switch B. Você também vê que uma pequena quantidade de tráfego de multicast gerado pelo switch (Dynamic ISL, CDP) sai de todas as quatro portas. Os pacotes de broadcast são consultas ARP (para o gateway padrão - que não existe aqui). Se você tivesse estações de trabalho que enviassem pacotes através do switch para um destino no outro lado do canal, você esperaria ver o tráfego que passa por cada um dos quatro links no canal. Você pode monitorar a distribuição de pacotes em sua própria rede com o comando **show** maccommand.

```
Switch-A (enable) clear counters
This command will reset all MAC and port counters reported in CLI and SNMP.
Do you want to continue (y/n) [n]? y
MAC and Port counters cleared.
Switch-A (enable) show mac

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 2/1                        9                  320                  183
 2/2                        0                   51                    0
 2/3                        0                   47                    0
 2/4                        0                   47                    0
(...)

Port     Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
-------- -------------------- -------------------- --------------------
 2/1                        8                   47                  184
 2/2                        0                   47                    0
 2/3                        0                   47                    0
 2/4                        0                   47                    0
(...)

Port     Rcv-Octet            Xmit-Octet
-------- -------------------- --------------------
 2/1                    35176                17443
 2/2                     5304                 4851
 2/3                     5048                 4851
 2/4                     5048                 4851
(...)

Last-Time-Cleared
--------------------------
Wed Dec 15 1999, 01:05:33
```

Use o PAgP para configurar o EtherChannel (método preferido)

O protocolo de agregação de porta (PAgP) facilita a criação automática de links de EtherChannel com a troca de pacotes entre portas com capacidade de canal. O protocolo aprende os recursos dos grupos de porta dinamicamente e informa as portas adjacentes.

Após o PAgP identificar corretamente os enlaces compatíveis com canais emparelhados, ele agrupa as portas em um canal. O canal é, em seguida, adicionado ao spanning tree como uma única porta de ponte. Um determinado pacote de transmissão ou transmissão múltipla externa é transmitido apenas por uma porta no canal, não em todas as portas no canal. Além disso, os pacotes de transmissão e multicast de saída transmitidos em uma porta no canal têm o retorno bloqueado em qualquer outra porta do canal.

Há quatro modos de canal configuráveis pelo usuário: on, off, auto e desirable. Os pacotes PAgP são trocados apenas entre as portas no modo auto e desirable. As portas configuradas no modo

onoroffmode não trocam pacotes PAgP. As configurações recomendadas para os switches que você deseja formar e para o EtherChannel é ter ambos os switches definidos para o modo desejado. Isso fornece o comportamento mais robusto quando um lado ou o outro encontra situações de erro ou pode ser redefinido. O modo padrão do canal é **auto**.

Os modos auto e desirable permitem que as portas negociem com as portas conectadas para determinar se elas podem formar um canal com base em critérios como velocidade da porta, estado de entroncamento, VLAN nativa, etc.

As portas podem formar um EtherChannel quando estão em diferentes modos de canal, contanto que os modos sejam compatíveis:

Um modo indesejável de porta pode formar um EtherChannel com êxito com outra porta que seja indesirable ou automode.

Uma porta no modo automático pode formar um EtherChannel com outra porta no modo indesejável.

Uma porta inautomode não pode formar um EtherChannel com outra porta que também seja inautomode, já que nenhuma porta inicia a negociação.

Uma porta inonmode pode formar um canal apenas com uma porta inonmode porque as portas inonmode não trocam pacotes PAgP.

Um modo de entrada/saída de porta não forma um canal com nenhuma porta.

Quando você usa o EtherChannel, se uma mensagem "SPANTREE-2: Channel misconfig - x/x-x will be disabled" ou uma mensagem de syslog semelhante for exibida, isso indica uma incompatibilidade dos modos do EtherChannel nas portas conectadas. é recomendável corrigir a configuração e reabilitar as portas com o comando **set port** enable. As configurações de EtherChannel válidas incluem:

Tabela 22-5: Configurações válidas do EtherChannel

Modo de canal de porta	Modo(s) válido(s) de canal de porta de vizinho
desirable	desirable ou auto
auto (padrão)	desejável ou auto1
ligado	ligado
desligado	desligado

[1]Se as portas local e vizinha forem inautomode, um pacote EtherChannel não será formado.

Aqui está um resumo de todos os cenários possíveis do modo de canalização. Algumas dessas combinações podem fazer com que o spanning tree coloque as portas do lado da canalização em errdisablestate (ou seja, desative-as).

Tabela 22-6: Cenários do modo de canalização

Modo de canal do Switch A	Modo de canal do Switch B	Estado do canal:
Ligado	Ligado	Canal

Ligado	Off	Sem canal (errdisable)
Ligado	Auto	Sem canal (errdisable)
Ligado	Desejável	Sem canal (errdisable)
Off	Ligado	Sem canal (errdisable)
Off	Off	Sem canal
Off	Auto	Sem canal
Off	Desejável	Sem canal
Auto	Ligado	Sem canal (errdisable)
Auto	Off	Sem canal
Auto	Auto	Sem canal
Auto	Desejável	Canal
Desejável	Ligado	Sem canal (errdisable)
Desejável	Off	Sem canal
Desejável	Auto	Canal
Desejável	Desejável	Canal

Você desligou o canal do exemplo anterior com este comando no SwitchA e no SwitchB.

```
Switch-A (enable) set port channel 2/1-4 auto
Port(s) 2/1-4 channel mode set to auto.
```

O modo de canal padrão de uma porta que pode canalizar é automático. Para verificar isso, insira este comando:

```
Switch-A (enable) show port channel 2/1
Port  Status     Channel   Channel     Neighbor                 Neighbor
                 mode      status      device                   port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  connected  auto      not channel
```

O comando anterior também mostra que as portas no momento não são canalizadas. Essa é outra maneira de verificar o estado do canal.

```
Switch-A (enable) show port channel
No ports channelling
Switch-B (enable) show port channel
No ports channelling
```

Érealmente muito simples fazer o canal funcionar com PAgP. Nesse ponto, ambos os switches são definidos para o modo automático, o que significa que eles canalizam se uma porta conectada envia uma solicitação de PAgP ao canal. Se você definir o SwitchA como desirable (desejável), o SwitchA fará com que o SwitchA envie pacotes PAgP para o outro switch e solicitará que ele faça o canal.

```
Switch-A (enable) set port channel 2/1-4 desirable
Port(s) 2/1-4 channel mode set to desirable.
1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/1 left bridg1
1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 15 22:03:19 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 15 22:03:19 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 15 22:03:20 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 15 22:03:23 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
1999 Dec 15 22:03:23 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
1999 Dec 15 22:03:23 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
1999 Dec 15 22:03:24 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4
```

Para visualizar o canal, faça isso.

```
Switch-A (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  desirable channel     WS-C5505    066509957(Sw  2/1
 2/2  connected  desirable channel     WS-C5505    066509957(Sw  2/2
 2/3  connected  desirable channel     WS-C5505    066509957(Sw  2/3
 2/4  connected  desirable channel     WS-C5505    066509957(Sw  2/4
----- ---------- --------- ----------- ------------------------- ----------
```

Como o SwitchB estava no modo automático, ele respondeu aos pacotes de PAgP e criou um canal com o SwitchA.

```
Switch-B (enable)
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/1 left bridg1
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
2000 Jan 14 20:26:45 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 14 20:26:45 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 14 20:26:45 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
2000 Jan 14 20:26:47 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
2000 Jan 14 20:26:47 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 14 20:26:47 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 14 20:26:48 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  auto      channel     WS-C5505    066507453(Sw  2/1
 2/2  connected  auto      channel     WS-C5505    066507453(Sw  2/2
 2/3  connected  auto      channel     WS-C5505    066507453(Sw  2/3
 2/4  connected  auto      channel     WS-C5505    066507453(Sw  2/4
----- ---------- --------- ----------- ------------------------- ----------
```

Observação: é recomendável definir ambos os lados do canal para o desejado para que ambos os lados tentem iniciar o canal se um lado cair. Se você definir as portas EtherChannel no SwitchB para o modo desejado, mesmo que o canal esteja atualmente ativo e inautomode, não

haverá nenhum problema. Este é o comando.

```
Switch-B (enable) set port channel 2/1-4 desirable
Port(s) 2/1-4 channel mode set to desirable.

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  desirable channel     WS-C5505    066507453(Sw  2/1
 2/2  connected  desirable channel     WS-C5505    066507453(Sw  2/2
 2/3  connected  desirable channel     WS-C5505    066507453(Sw  2/3
 2/4  connected  desirable channel     WS-C5505    066507453(Sw  2/4
----- ---------- --------- ----------- ------------------------- ----------
```

Agora, se o SwitchA ficar inativo por algum motivo ou se um novo hardware substituí-lo, o SwitchB tentará restabelecer o canal. Se o novo equipamento não puder ser canalizado, o SwitchB tratará as portas 2/1-4 como portas não canalizadas normais. Esse é um dos benefícios do uso do mododesejável. Se o canal foi configurado com o comando PAgP no modo e um lado da conexão tem um erro de algum tipo ou uma redefinição, ele pode causar um estado de errdisable (desligado) no outro lado. Com o PAgP definido no modo desirable (desejado) em cada lado, o canal estabiliza e renegocia a conexão EtherChannel.

Entroncamento e EtherChannel

O EtherChannel é independente do entroncamento. Você pode ativar o entroncamento ou deixá-lo desativado. Você também pode ativar o entroncamento para todas as portas antes de criar o canal ou pode ativá-lo depois de criar o canal (como faz aqui). No que diz respeito ao EtherChannel, não importa; o entroncamento e o EtherChannel são recursos completamente separados. O que realmente importa é que todas as portas envolvidas estejam no mesmo modo: elas estão todas em entroncamento antes de você configurar o canal ou não estão em entroncamento antes de você configurar o canal. Todas as portas devem estar no mesmo estado de entroncamento antes de você criar o canal. Uma vez que um canal é formado, tudo o que for alterado em uma porta também é alterado para outras portas no canal. Os módulos usados neste ambiente de teste podem fazer entroncamento ISL ou 802.1 q. Por padrão, os módulos são definidos como entroncamento automático e modo de negociação, o que significa que eles se referem ao tronco, caso o outro lado peça que eles façam entrocamento, e negociem se devem usar o método ISL ou 802.1q para entroncamento. Se não for solicitado o tronco, eles funcionarão como portas normais de não entroncamento.

```
Switch-A (enable) show trunk 2
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      auto         negotiate      not-trunking  1
 2/2      auto         negotiate      not-trunking  1
 2/3      auto         negotiate      not-trunking  1
 2/4      auto         negotiate      not-trunking  1
```

Há várias maneiras diferentes de ativar o entroncamento. Para este exemplo, você define o SwitchA como desirable (desejável). O Switch A já está definido para negociação. A combinação desejável/negociar faz com que o switch peça que o SwitchB faça o entrocamento e negocie o tipo de entroncamento a fazer (ISL ou 802.1q). Como o padrões de SwitchB é para negociar automaticamente, o SwitchB responde à solicitação de SwitchA. Há esses resultados:

```
Switch-A (enable) set trunk 2/1 desirable
Port(s) 2/1-4 trunk mode set to desirable.
Switch-A (enable)
1999 Dec 18 20:46:25 %DTP-5-TRUNKPORTON:Port 2/1 has become isl trunk
1999 Dec 18 20:46:25 %DTP-5-TRUNKPORTON:Port 2/2 has become isl trunk
1999 Dec 18 20:46:25 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4
1999 Dec 18 20:46:25 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-4
1999 Dec 18 20:46:25 %DTP-5-TRUNKPORTON:Port 2/3 has become isl trunk
1999 Dec 18 20:46:26 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/1-4
1999 Dec 18 20:46:26 %DTP-5-TRUNKPORTON:Port 2/4 has become isl trunk
1999 Dec 18 20:46:26 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/1-4
1999 Dec 18 20:46:28 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
1999 Dec 18 20:46:29 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
1999 Dec 18 20:46:29 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
1999 Dec 18 20:46:29 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

Switch-A (enable) show trunk 2
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      desirable    n-isl          trunking      1
 2/2      desirable    n-isl          trunking      1
 2/3      desirable    n-isl          trunking      1
 2/4      desirable    n-isl          trunking      1
```

O modo de tronco foi definido conforme desejado. O resultado foi que o modo de entroncamento foi negociado com o switch vizinho e eles decidiram sobre ISL (**n-isl**). O status atual agora **está em execução**. Isso foi o que aconteceu no SwitchB devido ao comando emitido no SwitchA.

```
Switch-B (enable)
2000 Jan 17 19:09:52 %DTP-5-TRUNKPORTON:Port 2/1 has become isl trunk
2000 Jan 17 19:09:52 %DTP-5-TRUNKPORTON:Port 2/2 has become isl trunk
2000 Jan 17 19:09:52 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4
2000 Jan 17 19:09:52 %DTP-5-TRUNKPORTON:Port 2/3 has become isl trunk
2000 Jan 17 19:09:52 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-4
2000 Jan 17 19:09:53 %DTP-5-TRUNKPORTON:Port 2/4 has become isl trunk
2000 Jan 17 19:09:53 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/1-4
2000 Jan 17 19:09:53 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/1-4
2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

Switch-B (enable) show trunk 2
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      auto         n-isl          trunking      1
 2/2      auto         n-isl          trunking      1
 2/3      auto         n-isl          trunking      1
 2/4      auto         n-isl          trunking      1
```

Observe que todas as quatro portas (2/1-4) se tornaram troncos, mesmo que você tenha alterado apenas uma porta (2/1) especificamente para desejável. Este é um exemplo de como a alteração de uma porta no canal afeta todas as portas.

Solucionar problemas do EtherChannel

Os desafios do EtherChannel podem ser divididos em duas áreas principais: solucionar o

problema na fase de configuração e solucionar o problema na fase de execução. Os erros de configuração geralmente ocorrem devido a parâmetros incompatíveis nas portas envolvidas (velocidades diferentes, duplex diferente, valores de porta de spanning tree diferentes e assim por diante). Você também pode gerar erros na configuração se definir o canal em um lado toone esperar muito antes de configurar o canal no outro lado. Isso causa loops de spanning tree, o que gera um erro e desliga a porta.

Quando um erro for encontrado durante a configuração do EtherChannel, verifique o status das portas depois de corrigir a situação de erro do EtherChannel. Se o status da porta *éerrdisable*, significa que as portas foram desativadas pelo software e não voltam a funcionar até que você insira o comando **set port** enablecommand.

Observação: se o status da porta *se tornar errdisable*, você deve habilitar especificamente as portas com o comando *set port* enablepara que as portas se tornem ativas. Atualmente, você pode corrigir todos os problemas do EtherChannel, mas as portas não surgem ou formam um canal até que sejam habilitadas novamente! Versões futuras do sistema operacional podem verificar periodicamente se iferrdisableports deve ser habilitado.

Nesses testes, você desativa o entroncamento e o EtherChannel: Parâmetros Incompatíveis; Aguarde Muito Tempo Antes de Configurar o Outro Lado; Corrija o Estado Errdisable; e Mostre o Que Acontece Quando um Link É Interrompido e Restaurado.

Parâmetros incompatíveis

Aqui está um exemplo de parâmetros incompatíveis. Você define a porta 2/4 na VLAN 2 enquanto as outras portas ainda estão na VLAN 1. Para criar uma nova VLAN, você deve atribuir um domínio VTP ao switch e criar a VLAN.

```
Switch-A (enable) show port channel
No ports channelling

Switch-A (enable) show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     connected  1          normal a-full a-100 10/100BaseTX
 2/2                     connected  1          normal a-full a-100 10/100BaseTX
 2/3                     connected  1          normal a-full a-100 10/100BaseTX
 2/4                     connected  1          normal a-full a-100 10/100BaseTX

Switch-A (enable) set vlan 2
Cannot add/modify VLANs on a VTP server without a domain name.

Switch-A (enable) set vtp domain testDomain
VTP domain testDomain modified

Switch-A (enable) set vlan 2 name vlan2
Vlan 2 configuration successful

Switch-A (enable) set vlan 2 2/4
VLAN 2 modified.
VLAN 1 modified.
VLAN  Mod/Ports
---- ----------------------
2     2/4

Switch-A (enable)
1999 Dec 19 00:19:34 %PAGP-5-PORTFROMSTP:Port 2/4 left bridg4
```

```
Switch-A (enable) show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     connected  1          normal a-full a-100 10/100BaseTX
 2/2                     connected  1          normal a-full a-100 10/100BaseTX
 2/3                     connected  1          normal a-full a-100 10/100BaseTX
 2/4                     connected  2          normal a-full a-100 10/100BaseTX

Switch-A (enable) set port channel 2/1-4 desirable
Port(s) 2/1-4 channel mode set to desirable.

Switch-A (enable)
1999 Dec 19 00:20:19 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
1999 Dec 19 00:20:19 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 19 00:20:19 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 19 00:20:20 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 19 00:20:20 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 19 00:20:22 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 19 00:20:22 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 19 00:20:24 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-2
1999 Dec 19 00:20:25 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-2
1999 Dec 19 00:20:25 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3
1999 Dec 19 00:20:25 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/4

Switch-A (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  desirable channel     WS-C5505    066509957(Sw  2/1
 2/2  connected  desirable channel     WS-C5505    066509957(Sw  2/2
----- ---------- --------- ----------- ------------------------- ----------
```

Observe que o canal é formado apenas entre as portas 2/1-2. As portas 2/3-4 foram deixadas de fora porque a porta 2/4 estava em uma VLAN diferente. Não havia nenhuma mensagem de erro; o PAgP apenas fez o que podia para fazer o canal funcionar. Você precisa observar os resultados ao criar o canal para certificar-se de que ele faz o que você queria fazer.

Agora configure o canal manualmente para "on" com a porta 2/4 em uma VLAN diferente e veja o que acontece. Primeiro, você define o modo do canal de volta para auto, a fim de desmontar o canal atual, em seguida, você define o canal manualmente para "on".

```
Switch-A (enable) set port channel 2/1-4 auto
Port(s) 2/1-4 channel mode set to auto.
Switch-A (enable)
1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-2
1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-2
1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 19 00:26:18 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
1999 Dec 19 00:26:19 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2
1999 Dec 19 00:26:19 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3
1999 Dec 19 00:26:19 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/4

Switch-A (enable) show port channel
No ports channelling

Switch-A (enable) set port channel 2/1-4 on
Mismatch in vlan number.
Failed to set port(s) 2/1-4 channel mode to on.
```

```
Switch-A (enable) show port channel
No ports channelling
```

No SwitchB, você pode ligar o canal e observar que ele indica que o canal das portas está funcionando corretamente, mas você sabe que o SwitchA não está configurado corretamente.

```
Switch-B (enable) show port channel
No ports channelling

Switch-B (enable) show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     connected  1          normal a-full a-100 10/100BaseTX
 2/2                     connected  1          normal a-full a-100 10/100BaseTX
 2/3                     connected  1          normal a-full a-100 10/100BaseTX
 2/4                     connected  1          normal a-full a-100 10/100BaseTX

Switch-B (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.

Switch-B (enable)
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  on        channel     WS-C5505    066507453(Sw  2/1
 2/2  connected  on        channel     WS-C5505    066507453(Sw  2/2
 2/3  connected  on        channel     WS-C5505    066507453(Sw  2/3
 2/4  connected  on        channel     WS-C5505    066507453(Sw  2/4
----- ---------- --------- ----------- ------------------------- ----------
```

Isso torna claro que você deve verificar os dois lados do canal ao configurá-lo manualmente, para garantir que ambos os lados estejam ativos, não apenas um lado. Essa saída mostra que o SwitchB está definido para um canal, mas o SwitchA não canaliza porque tem uma porta que está na VLAN errada.

Aguardar muito tempo antes de configurar o outro lado

Nessa situação, o SwitchB tem o EtherChannel ativado, mas o SwitchA não tem porque ele tem um erro de configuração de VLAN (as portas 2/1-3 estão na vlan1, a porta 2/4 está na vlan2). O que acontece quando um lado de um EtherChannel é definido como ativado, enquanto o outro lado ainda está no modo automático. O SwitchB, após alguns minutos, desliga as portas devido a uma detecção de loop estendido. Isso ocorre porque as portas 2/1-4 do Switch Batuam como uma grande porta, enquanto as portas 2/1-4 do Switch A são porta totalmente independentes. Uma transmissão enviada do SwitchB para o SwitchA na porta 2/1 é enviado de volta para o SwitchB nas portas 2/2, 2/3 e 2/4 porque o SwitchA trata essas portas como independentes. É por isso que o SwitchB relata que há um loop de spanning tree. Observe que as portas no SwitchB agora estão desabilitadas e têm um status *oferrdisable*.

```
Switch-B (enable)
2000 Jan 17 22:55:48 %SPANTREE-2-CHNMISCFG: STP loop - channel 2/1-4 is disabled in vlan 1.
2000 Jan 17 22:55:49 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4
2000 Jan 17 22:56:01 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-4
2000 Jan 17 22:56:13 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/1-4
2000 Jan 17 22:56:36 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/1-4

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  errdisable on        channel
 2/2  errdisable on        channel
 2/3  errdisable on        channel
 2/4  errdisable on        channel
----- ---------- --------- ----------- ------------------------- ----------
Switch-B (enable) show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     errdisable 1          normal   auto  auto 10/100BaseTX
 2/2                     errdisable 1          normal   auto  auto 10/100BaseTX
 2/3                     errdisable 1          normal   auto  auto 10/100BaseTX
 2/4                     errdisable 1          normal   auto  auto 10/100BaseTX
```

Estado de errdisable correto

Às vezes, quando você tenta configurar o EtherChannel, mas as portas não estão configuradas da mesma forma, isso faz com que as portas em um lado do canal ou no outro sejam desativadas. As luzes de link são amarelas na porta. Você pode dizer isso pelo console se digitar show port. As portas estão listadas como *aserrdisable*. Para se recuperar disso, você deve corrigir os parâmetros não correspondentes nas portas envolvidas e, em seguida, reativar as portas. Observe que para reativar as portas, é uma etapa separada que deve ser feita para que elas se tornem funcionais novamente.

Neste exemplo, você sabe que o SwitchA tinha uma incompatibilidade de vlan. Você vai para o SwitchA e coloca a porta 2/4 de volta na vlan1. Em seguida, você ativa o canal para as portas 2/1-4. O SwitchA não aparece conectado até que você reative as portas do SwitchB. Depois, quando tiver corrigido o SwitchA e o colocar no modo de canalização, você voltará para o SwitchB e reabilitará as portas.

```
Switch-A (enable) set vlan 1 2/4
VLAN 1 modified.
VLAN 2 modified.
VLAN  Mod/Ports
---- ----------------------
1     2/1-24

Switch-A (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.
Switch-A (enable) sh port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  notconnect on        channel
 2/2  notconnect on        channel
 2/3  notconnect on        channel
 2/4  notconnect on        channel
----- ---------- --------- ----------- ------------------------- ----------
```

```
Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  errdisable on        channel
 2/2  errdisable on        channel
 2/3  errdisable on        channel
 2/4  errdisable on        channel
----- ---------- --------- ----------- ------------------------- ----------

Switch-B (enable) set port enable 2/1-4
Ports 2/1-4 enabled.
Switch-B (enable) 2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/1 joined bridg4
2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  on        channel
 2/2  connected  on        channel
 2/3  connected  on        channel
 2/4  connected  on        channel
----- ---------- --------- ----------- ------------------------- ----------
```

Mostrar o que acontece quando um link é interrompido e restaurado

Quando uma porta no canal fica inativa, todos os pacotes que são enviados normalmente nessa porta são deslocados para a próxima porta no canal. Você pode verificar isso com o comando **show** mac. Neste campo de teste, você tem o SwitchA enviando pacotes de ping ao SwitchB para ver qual link o tráfego usa. Primeiro você limpa os contadores, depois mostra mac, envia três pings e, em seguida, **mostra** macagain para ver em que canal as respostas do ping foram recebidas.

```
Switch-A (enable) clear counters
This command will reset all MAC and port counters reported in CLI and SNMP.
Do you want to continue (y/n) [n]? y
MAC and Port counters cleared.

Switch-A (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  on        channel     WS-C5505    066509957(Sw  2/1
 2/2  connected  on        channel     WS-C5505    066509957(Sw  2/2
 2/3  connected  on        channel     WS-C5505    066509957(Sw  2/3
 2/4  connected  on        channel     WS-C5505    066509957(Sw  2/4
----- ---------- --------- ----------- ------------------------- ----------

Switch-A (enable) show mac

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 2/1                       0                   18                    0
 2/2                       0                    2                    0
 2/3                       0                    2                    0
```

```
 2/4                       0                    2                    0
Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) show mac

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 2/1                       3                   24                    0
 2/2                       0                    2                    0
 2/3                       0                    2                    0
 2/4                       0                    2                    0
```

Neste ponto, você recebeu as respostas de ping na porta 3/1. Quando o console SwitchB envia uma resposta ao SwitchA, o EtherChannel usa a porta 2/1. Agora você desliga a porta 2/1 no SwitchB. No SwitchA, você emite outro ping e vê em qual canal a resposta volta. (O SwitchA envia na mesma porta à qual o SwitchB está conectado. Você apenas mostra os pacotes recebidos do SwitchB porque os pacotes de transmissão estão mais abaixo no show macdisplay).

```
1999 Dec 19 01:30:23 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4

Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) show mac

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 2/1                       3                   37                    0
 2/2                       1                   27                    0
 2/3                       0                    7                    0
 2/4                       0                    7                    0
```

Agora que a porta 2/1 está desativada, o EtherChannel usa automaticamente a próxima porta no canal, 2/2. Agora você reabilita a porta 2/1 e espera que ela se junte ao grupo de pontes. Em seguida, você emite mais dois pings.

```
1999 Dec 19 01:31:33 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4

Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) show mac

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 2/1                       5                   50                    0
 2/2                       1                   49                    0
 2/3                       0                   12                    0
 2/4                       0                   12                    0
```

Observe que esses pings são enviados da porta 2/1. Quando o link é revertido, a EtherChannel novamente o adiciona ao pacote e o usa. Tudo isso é feito de forma transparente para o usuário.

Comandos utilizados nesta seção

Estes são os comandos usados nesta seção.

Comandos a serem usados para definir a configuração

set port channel on - para ativar o recurso de EtherChannel.

set port channel auto - para redefinir as portas ao modo padrão de automático.

set port channel desirable- para enviar pacotes PAgP para as solicitações do outro lado para que um canal seja criado.

set port Enable - para ativar as portas após o comando set port Disable ou após um estado errdisable.

set port disable- para desativar uma porta enquanto outras definições de configuração são feitas.

set trunk desirable - para ativar o entroncamento e fazer com que essa porta envie uma solicitação ao outro switch para indicar que esse é um link de tronco. Se a porta estiver definida para negociar (a configuração padrão) para negociar o tipo de entroncamento a ser usado no link (ISL ou 802.1q).

Comandos para verificar a configuração

show version - para exibir qual versão do software o switch executa.

show module - para exibir quais módulos estão instalados no switch.

show port capabilities- para determinar se as portas que você deseja usar têm a capacidade de executar o EtherChannel.

show port - para determinar o status da porta (notconnect, connected) e as configurações de velocidade e frente e verso.

ping - para testar a conectividade com o outro switch.

show port channel – Para visualizar o status atual do pacote EtherChannel.

show port channel mod/port - para fornecer uma visão mais detalhada do status do canal de uma única porta.

show spantree - para verificar se a árvore de abrangência considerou o canal como um link.

show trunk – para ver o status de truncamento de portas.

Comandos a serem usados para solucionar problemas de configuração

show port channel – Para visualizar o status atual do pacote EtherChannel.

show port - para determinar o status da porta (notconnect, connected) e as configurações de velocidade e frente e verso.

clear counters - para redefinir os contadores do pacote do switch para zero. Os contadores são visíveis com o comando **show**.

show mac - para visualizar os pacotes recebidos e enviados pelo switch.

ping- para testar a conectividade com o outro switch e gerar o tráfego que aparece com o comando **show** maccommand.

Usar Portfast e Outros Comandos para Corrigir Problemas de Conectividade de Inicialização da Estação Final

Se você tiver estações de trabalho conectadas a switches que não conseguem fazer login no seu domínio de rede (NT ou Novell), ou não conseguem obter um endereço DHCP, então você pode tentar as sugestões listadas neste documento antes de explorar outros caminhos. As sugestões são relativamente fáceis de implementar e, muitas vezes, são a causa dos problemas de conectividade da estação de trabalho encontrados durante a fase de inicialização/inicialização da estação de trabalho.

Com mais e mais usuários que implantam switching no desktop e substituem seus hubs compartilhados por switches, você frequentemente vê problemas introduzidos em ambientes cliente/servidor devido a esse atraso inicial. O maior problema observado é que clientes Windows 95/98/NT, Novell, VINES, IBM NetworkStation/IBM Thin Clients e AppleTalk não conseguem se conectar a seus servidores. Se o software nesses dispositivos não for persistente no procedimento de inicialização, eles não tentarão mais se conectar ao servidor antes mesmo que o switch tenha permitido a passagem de tráfego.

Observação: esse atraso de conectividade inicial geralmente se manifesta como erros que aparecem quando você inicializa uma estação de trabalho pela primeira vez. Estes são vários exemplos de erros e mensagens de erro que você pode ver:

Um cliente de rede Microsoft exibe: No Domain Controllers Available" (Nenhum controlador de domínio disponível).

Relatórios de DHCP, "No DHCP Servers Available" (Nenhum servidor DHCP disponível).

Uma estação de trabalho de rede Novell IPX não apresenta a tela "Novell Login Screen"

durante a inicialização.

Um cliente de rede AppleTalk exibe, "Access to your AppleTalk network has been interrupted. In order to re-establish your connection, open and close the AppleTalk control panel." (O acesso à rede AppleTalk foi interrompido. Para restabelecer a conexão, abra e feche o painel de controle do AppleTalk) Também é possível que o aplicativo AppleTalk Client Chooser não exiba uma lista de zonas ou exiba uma lista de zonas incompleta.

O retardo inicial de conectividade também é observado freqüentemente em um ambiente comutado no qual um administrador de rede atualiza software ou drivers. Nesse caso, um fornecedor pode otimizar os drivers para que os procedimentos de inicialização da rede ocorram no começo do processo de inicialização do cliente (antes que o switch esteja pronto para processar os pacotes).

Com os vários recursos agora incluídos em alguns switches, pode levar alguns minutos para que um switch comece a fazer a manutenção de uma estação de trabalho conectada recentemente. Esse atraso pode afetar a estação de trabalho toda vez que ela é ligada ou reinicializada. Esses são os quatro principais recursos que causam esse atraso:

Spanning-Tree Protocol (STP)

Negociação EtherChannel

Negociação de truncamento

Negociação de velocidade/duplex do link entre o switch e a estação de trabalho

Os quatro recursos são listados na ordem do que causa o maior atraso (STP) até o que causa o menor atraso (negociação de velocidade/duplex). Uma estação de trabalho conectada a um switch geralmente não causa loops de spanning tree, geralmente não precisa de EtherChannel e de negociar um método de entroncamento. (Se você desativar a negociação de velocidade/detecção de link, ela também pode reduzir o atraso da porta, caso haja a necessidade de otimizar o tempo de inicialização o máximo possível.)

Esta seção mostra como implementar os comandos de otimização da velocidade de inicialização em três plataformas do switch Catalyst. Nas seções de cronometragem, você mostra como o atraso da porta do switch é reduzido e em quanto.

Contents

Os termos "estação de trabalho", "estação final", "servidor" são usados de modo intercambiável nesta seção. Você se refere a qualquer dispositivo conectado diretamente a um switch por uma única placa de rede. Ele também pode se referir a dispositivos com várias placas de rede, quando ela só é usada para redundância, em outras palavras a estação de trabalho ou o servidor não está configurado para atuar como ponte, ele tem apenas várias placas de rede para redundância.

Observação: há algumas placas NIC de servidor que suportam entroncamento e/ou EtherChannel. Há situações em que o servidor precisa estar em várias VLANs ao mesmo tempo (entroncamento) ou ele precisa de mais largura de banda no link que o conecta ao switch (EtherChannel). Nesses casos, não desligue o PAgP e não desligue o entroncamento. Além disso, esses dispositivos raramente são desligados ou reiniciados. As instruções incluídas neste documento não se aplicam a esses tipos de dispositivo.

Background

Esta seção abrange quatro características que alguns switches têm que causam atrasos iniciais quando um dispositivo está conectado a um switch. Geralmente, uma estação de trabalho não causa o problema de spanning tree (loops) ou não precisa do recurso (PAgP, DTP), portanto o atraso é desnecessário.

Spanning Tree

Se você tiver iniciado recentemente o movimento de um ambiente de Hub para um ambiente de switch, esses problemas de conectividade poderão ser exibidos porque um switch funciona de forma muito diferente do Hub. Um switch fornece conectividade na camada DataLink, não na camada física. O switch precisa usar um algoritmo de pontes para decidir se os pacotes recebidos em uma porta precisam ser transmitidos por outras portas. O algoritmo de bridging é suscetível a loops físicos na topologia da rede. Devido a essa susceptibilidade para fazer loops, os switches executam um protocolo chamado STP, que faz com que os loops sejam eliminados na topologia. Quando o STP é executado, ele faz com que todas as portas incluídas no processo de spanning tree se tornem ativas muito mais lentamente do que se fossem, pois detecta e bloqueia loops. Uma rede com ponte de loops físicos, sem o spanning tree, falha. Apesar do tempo envolvido, o STP é um recurso bom. O spanning tree executado nos switches Catalyst é uma especificação padrão do setor (IEEE 802.1 d).

Depois que uma porta no switch tem link e entra no grupo de ponte, ela o executa nessa porta. Uma porta que executa spanning tree pode ter 1 de 5 estados: Blocking (Bloqueio), Listening (Escuta), Learning (Aprendizado), Forwarding (Encaminhamento) e Disabled (Desabilitado). A árvore de abrangência determina se a porta deve iniciar o bloqueio e realizar imediatamente as fases de audição e identificação. Por padrão, ele passa aproximadamente 15 segundos ouvindo e

15 segundos aprendendo.

No estado de escuta, o switch tenta determinar onde ele se encaixa na topologia de spanning tree. Ele quer saber especialmente se essa porta faz parte de um loop físico. Se ele fizer parte de um loop, essa porta pode ser escolhida para entrar no modo de bloqueio. O bloqueio significa que ele não envia nem recebe dados do usuário para eliminar loops. Se a porta não fizer parte de um loop, ela continuará com o estado de aprendizagem, o que envolve o conhecimento de quais endereços MAC estão ativos dessa porta. Este processo de inicialização da árvore de abrangência leva aproximadamente 30 segundos.

Se você conectar uma estação de trabalho ou um servidor com uma única placa NIC a uma porta de switch, essa conexão não poderá criar um loop físico. Essas conexões são consideradas nós folhas. Não há motivo para fazer com que a estação de trabalho aguarde 30 segundos, enquanto o switch verifica se há loops, quando ela não pode causar um loop. Assim, a Cisco adicionou um recurso chamado "Portfast" ou "Fast-Start", o que significa que o spanning tree para essa porta pode supor que a porta não faz parte de um loop e pode imediatamente passar para o estado de encaminhamento e ignorar os estados de bloqueio, escuta ou aprendizagem. Isto pode economizar muito tempo. Esse comando não desativa a árvore de abrangência. Isto apenas faz com que a árvore de abrangência da porta selecionada ignore alguns passos (desnecessários nesta circunstância) no início.

Observação: o recurso Portfast nunca deve ser usado em portas de switch que se conectam a outros switches, hubs ou roteadores. Essas conexões podem causar loops físicos e é muito importante que o spanning tree passe pelo procedimento de inicialização completa nessas situações. Um loop de spanning tree pode interromper o funcionamento da sua rede. Se o PortFast estiver ativado para uma porta que faz parte de um loop físico, ele pode provocar uma janela de tempo, em que os pacotes poderiam ser encaminhados continuamente (e até mesmo multiplicados) de forma que a rede não consiga se recuperar. No software do sistema operacional mais recente do Catalyst (5.4[1]), há um recurso chamado Portfast BPDU-Guard, que detecta a recepção de BPDUs em portas com PortFast habilitado. Como isso nunca deve acontecer, a proteção de BPDU coloca a porta no estado "errDisable".

EtherChannel

Outro recurso que um switch pode ter é chamado EtherChannel (Fast EtherChannel ou Gigabit EtherChannel). Esse recurso permite que vários links entre os mesmos dois dispositivos funcionem como se fossem um link rápido, com carga de tráfego balanceada entre os links. Um switch pode formar esses pacotes automaticamente com um vizinho com um protocolo chamado PAgP (Port Aggregation Protocol). As portas do switch que podem executar o PAgP normalmente têm como padrão um modo passivo chamado "auto", o que significa que eles podem formar um pacote se o dispositivo vizinho do link solicitar. Se você executar o protocolo no modo automático, ele pode fazer com que uma porta seja atrasada por até 15 segundos antes de passar o controle para o algoritmo spanning tree (o PAgP é executado em uma porta antes da spanning tree.) Não há motivo para o PAgP ser executado em uma porta conectada a uma estação de trabalho. Se você definir o modo PAgP da porta do switch como "off" (desativado), isso eliminará esse atraso.

Entroncamento

Outro recurso do switch é a capacidade de uma porta formar um tronco. Um tronco é configurado entre dois dispositivos quando eles precisam levar o tráfego de várias redes de área local virtual (VLANs). Uma VLAN é algo que os switches criam para fazer com que um grupo de estações de trabalho pareça estar em seu próprio segmento ou "domínio de broadcast". As portas de tronco fazem com que essas VLANs se estendam por vários switches, de modo que uma única VLAN possa cobrir todo o campus. Eles fazem isso com a adição de marcas aos pacotes; isso indica a

qual VLAN o pacote pertence.

Há diferentes tipos de protocolos de truncamento. Se uma porta puder se tornar um tronco, ela também pode ter a capacidade de fazer o tronco automaticamente e, em alguns casos, até negociar o tipo de entroncamento a ser usado na porta. Esta capacidade de negociar o método de truncamento com o outro dispositivo é chamada de protocolo DTP; o precursor do DTP é um protocolo chamado ISL Dinâmico (DISL). Se esses protocolos forem executados, eles poderão atrasar uma porta no switch que se torna ativa.

Geralmente, uma porta conectada a uma estação de trabalho pertence a apenas uma VLAN e, portanto, não precisa criar um tronco. Se uma porta tem a capacidade de negociar a formação de um tronco, normalmente é padrão para o modo "auto". Se a porta for alterada para um modo de entroncamento "desligado", isso reduzirá ainda mais o atraso de uma porta de switch que se torna ativa.

Negociação de Velocidade e Duplex

Tudo o que você precisa fazer é ativar o Portfast e desativar o PAgP (se houver) para resolver o problema, mas se precisar eliminar todos os segundos possíveis, você também pode definir a velocidade da porta e o duplex manualmente no switch, se for uma porta de várias velocidades (10/100). A autonegociação é um recurso interessante, mas se você desativá-la, poderá economizar 2 segundos em um Catalyst 5000 (não ajuda muito no 2800 ou 2900XL).

Pode haver complicações, no entanto, se você desativar a autonegociação no switch, mas deixá-lo ativo na estação de trabalho. Como o switch não negocia com o cliente, o cliente pode escolher a mesma configuração duplex que o switch usa ou não. Consulte "Troubleshooting Ethernet 10/100Mb Half/Half/Full Duplex AutoNegotiation" para obter informações adicionais sobre os avisos da autonegociação.

Como reduzir o atraso de inicialização no Switch Catalyst 4000/5000/6000

Esses cinco comandos mostram como ativar o Portfast, desativar a negociação PAgP, desativar a negociação de entroncamento (DISL, DTP) e desativar a negociação de velocidade/duplex. O comando **set spantree portfast** é executado em um intervalo de portas de uma só vez (**set spantree portfast 2/1-12 enable**). **Normalmente, o** canal de **porta definido** deve ser desativado com um grupo válido de portas com capacidade para canal. Nesse caso, o módulo dois tem a capacidade de canalizar as portas 2/1-2 ou as portas 2/1-4, portanto, qualquer um desses grupos de portas seria válido para usar.

Observação: a versão 5.2 do Cat OS para Catalyst 4000/5000 tem um novo comando **chamado** set port host, que é uma macro que combina esses comandos em um comando fácil de usar (exceto que não altera as configurações de velocidade e duplex).

Configuração

```
Switch-A (enable) set spantree portfast 2/1 enable

Warning: Spantree port fast start should only be enabled on ports connected
to a single host. Connecting hubs, concentrators, switches, bridges, and so on to
a fast start port can cause temporary spanning tree loops.  Use with caution.

Spantree port 2/1 fast start enabled.
Switch-A (enable) set port channel 2/1-2 off
Port(s) 2/1-2 channel mode set to off.
```

```
Switch-A (enable) set trunk 2/1 off
Port(s) 2/1 trunk mode set to off.
```

As mudanças na configuração são salvas automaticamente na NVRAM.

Verificação

A versão do software do switch usada neste documento é 4.5 (1). Para obter a saída completa de show version e show module, consulte esta seção de teste de intervalo.

```
Switch-A (enable) show version
WS-C5505 Software,
Version McpSW: 4.5(1) NmpSW: 4.5(1)
```

Esse comando mostra como visualizar o estado atual de uma porta com relação à spanning tree. Atualmente, a porta está no estado de encaminhamento de spanning tree (envio e recebimento de pacotes) e a coluna de início rápido mostra que o PortFast está desativado no momento. Em outras palavras, a porta pode levar pelo menos 30 segundos para passar para o estado forwarding sempre que for inicializada.

```
Switch-A (enable) show port spantree 2/1

Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-Method
--------  ----  -------------  -----  --------  ----------  ------------
 2/1      1     forwarding        19        32
disabled
```

Agora você ativa o portfast nesta porta do switch. O switch avisa que esse comando deve ser usado apenas em portas conectadas a um único host (uma estação de trabalho, um servidor, etc.) e nunca deve ser usado em portas conectadas a outros hubs ou switches. A razão pela qual você habilita o portfast é, então a porta começa a encaminhar imediatamente. Você pode fazer isso porque uma estação de trabalho ou um servidor não causa um loop de rede. Isso pode desperdiçar tempo. Mas outro hub ou switch pode causar um loop, e você quer sempre passar pelos estágios normais de escuta e aprendizagem quando se conecta a esses tipos de dispositivos.

```
Switch-A (enable) set spantree portfast 2/1 enable

Warning: Spantree port fast start should only be enabled on ports connected
to a single host.  Connecting hubs, concentrators, switches, bridges, and so on to
a fast start port can cause temporary spanning tree loops.  Use with caution.

Spantree port 2/1 fast start enabled.
```

Para verificar se o PortFast está ativado para esta porta, emita este comando.

```
Switch-A (enable) show port spantree 2/1

Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-Method
--------  ----  -------------  -----  --------  ----------  ------------
 2/1      1     forwarding        19        32
enabled
```

Outra maneira de exibir as configurações de Portfast de uma ou mais portas é exibir as informações da árvore de abrangência uma VLAN específica. Posteriormente, na seção de temporização deste documento, você mostrará como fazer o switch reportar cada estágio do spanning tree pelo qual ele se move em tempo real. Essa saída também mostra o tempo de atraso de encaminhamento (15 segundos). Este é o tempo que a árvore de abrangência pode ficar no estado listening e quanto tempo pode ficar no estado learning de cada porta na VLAN.

```
Switch-A (enable) show spantree 1
VLAN 1
Spanning tree enabled
Spanning tree type          ieee

Designated Root             00-e0-4f-94-b5-00
Designated Root Priority    8189
Designated Root Cost        19
Designated Root Port        2/24
Root Max Age   20 sec    Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-90-92-b0-84-00
Bridge ID Priority          32768
Bridge Max Age 20 sec    Hello Time 2  sec   Forward Delay 15 sec

Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-Method
--------- ----  -------------  -----  --------  ----------  ------------

 2/1      1     forwarding        19        32   enabled
...
```

Para verificar se o PAgP está desativado, use o comando **show port** channel. Certifique-se de especificar o número do módulo (2 neste caso) para que o comando mostre o modo de canal, mesmo se não houver um canal formado. Se você **mostrar o canal da porta** sem canais formados, ele apenas diz que não há canais de portas. você quer ir mais longe e ver o modo de canal atual.

```
Switch-A (enable) show port channel
No ports channeling

Switch-A (enable) show port channel 2
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  notconnect auto      not channel
 2/2  notconnect auto      not channel
...
Switch-A (enable) set port channel 2/1-2 off
Port(s) 2/1-2 channel mode set to off.

Switch-A (enable) show port channel 2
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  off       not channel
 2/2  connected  off       not channel
...
```

Para verificar se a negociação de entroncamento está desativada, use o comando **set trunk** off. Você mostra o estado padrão . Em seguida, desative o entroncamento e mostre o resultado. Você especifica o número de módulo 2 para que possa ver o modo de canal atual para as portas neste módulo.

```
Switch-A (enable) show trunk 2
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      auto         negotiate      not-trunking  1
 2/2      auto         negotiate      not-trunking  1
...

Switch-A (enable) set trunk 2/1-2 off
Port(s) 2/1-2 trunk mode set to off.

Switch-A (enable) show trunk 2
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      off          negotiate      not-trunking  1
 2/2      off          negotiate      not-trunking  1
```

Não é necessário, exceto no mais raro dos casos, desativar a autonegociação de velocidade/duplex ou definir manualmente a velocidade e o duplex no switch. Você dá um exemplo de como fazer isso nos Testes de Medição de Tempo com e sem DTP, PAgP e Portfast em uma seção do Catalyst 5000 se achar que isso é necessário para a sua situação.

Testes de cronometragem com e sem DTP, PAgP e Portfast em um Catalyst 5000

Esse teste mostra o que acontece com o intervalo de inicialização da porta do switch, quando os vários comandos são aplicados. As configurações padrão da porta são utilizadas primeiramente para o teste de desempenho do sistema. Ela tem PortFast desabilitado, o modo PAgP (EtherChannel) é definido como auto (canaliza se for solicitado), e o modo de entroncamento (DTP) é definido como auto (forma o entroncamento se for solicitado). Em seguida, o teste continua a ativar o PortFast e a medir o tempo, desativar o PAgP e medir o tempo, em seguida, desativar o entroncamento e medir o tempo. Finalmente, você desliga a autonegociação e mede o tempo. Todos esses testes são feitos em um Catalyst 5000 com uma placa Fast Ethernet 10/100 compatível com DTP e PAgP.

Observação: quando o portfast está ativado, isso não é o mesmo que desativar o spanning tree (como observado no documento). Com o portfast ativado, o spanning tree ainda é executado na porta; ele simplesmente não bloqueia, ouve ou aprende e vai imediatamente para o estado forwarding. Desligar o spanning tree não é recomendado porque ele afeta a VLAN inteira e pode deixar a rede vulnerável a loops de topologia física, causando sérios problemas de rede.

Mostrar a versão e a configuração do Cisco IOS do switch (**show version, show module**).

```
Switch-A (enable) show version
WS-C5505 Software, Version McpSW: 4.5(1) NmpSW: 4.5(1)
Copyright (c) 1995-1999 by Cisco Systems
NMP S/W compiled on Mar 29 1999, 16:09:01
MCP S/W compiled on Mar 29 1999, 16:06:50

System Bootstrap Version: 3.1.2

Hardware Version: 1.0  Model: WS-C5505  Serial #: 066507453

Mod Port Model      Serial #  Versions
```

```
--- ---- ---------- --------- ---------------------------------------
1   0    WS-X5530   006841805 Hw : 1.3
                              Fw : 3.1.2

                              Fw1: 3.1(2)
                              Sw : 4.5(1)
2   24   WS-X5225R  012785227 Hw : 3.2
                              Fw : 4.3(1)
                              Sw : 4.5(1)

       DRAM                    FLASH                   NVRAM
Module Total   Used    Free    Total   Used    Free    Total Used  Free
------ ------- ------- ------- ------- ------- ------- ----- ----- -----
1       32640K  13648K  18992K   8192K   4118K   4074K  512K  119K  393K

Uptime is 28 days, 18 hours, 54 minutes

Switch-A (enable) show module
Mod Module-Name         Ports Module-Type           Model    Serial-Num Status
--- ------------------- ----- -------------------- --------- --------- -------
1                       0     Supervisor III        WS-X5530  006841805 ok
2                       24    10/100BaseTX Ethernet WS-X5225R 012785227 ok

Mod MAC-Address(es)                         Hw     Fw         Sw
--- --------------------------------------- ------ ---------- -----------------
1   00-90-92-b0-84-00 to 00-90-92-b0-87-ff 1.3    3.1.2      4.5(1)
2   00-50-0f-b2-e2-60 to 00-50-0f-b2-e2-77 3.2    4.3(1)     4.5(1)

Mod Sub-Type Sub-Model Sub-Serial Sub-Hw
--- -------- --------- ---------- ------
1   NFFC     WS-F5521  0008728786 1.0
```

Defina o log para spanning tree o mais detalhado possível (defina o nível de logging spantree 7). Este é o nível de registro padrão (2) para spanning tree, o que significa que apenas situações críticas são relatadas.

```
Switch-A (enable) show logging

Logging buffer size:          500
        timestamp option:     enabled
Logging history size:         1
Logging console:              enabled
Logging server:               disabled
        server facility:      LOCAL7
        server severity:      warnings(4)
```

```
Facility            Default Severity         Current Session Severity
------------        ----------------------   ------------------------
...
spantree            2                        2
...
0(emergencies)        1(alerts)             2(critical)
3(errors)             4(warnings)           5(notifications)
6(information)        7(debugging)
```

O nível do spanning tree é alterado para 7 (depuração), para que você possa ver os estados do spanning tree serem alterados na porta. Essa alteração de configuração dura apenas durante a sessão do terminal, retornando ao normal em seguida.

```
Switch-A (enable) set logging level spantree 7
System logging facility <spantree for this session set to severity 7(debugging)

Switch-A (enable) show logging
...

Facility            Default Severity         Current Session Severity
------------        ----------------------   ------------------------
...
spantree            2                        7
...
```

Inicie pela porta no fechamento do Catalyst.

```
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.
```

Agora é o horário e ative a porta. você deseja ver quanto tempo ela permanece em cada estado.

```
Switch-A (enable) show time
Fri Feb 25 2000, 12:20:17
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 12:20:39 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
2000 Feb 25 12:20:39 %SPANTREE-6-PORTBLK: port 2/1 state in vlan 1 changed to blocking.
2000 Feb 25 12:20:39 %SPANTREE-6-PORTLISTEN: port 2/1 state in vlane 1 changed to Listening
.
2000 Feb 25 12:20:53 %SPANTREE-6-PORTLEARN: port 2/1 state in vlan 1 changed to Learning.
2000 Feb 25 12:21:08 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 changed to forwarding.
```

Observe na saída que levou cerca de 22 segundos (20:17 a 20:39) para a porta começar o estágio de bloqueio de spanning tree. Esse foi o tempo necessário para negociar o link e fazer as tarefas de DTP e PAgP. Quando o bloqueio começar, você estará agora no território do spanning tree. Para bloquear a porta, ele foi imediatamente para escuta (20:39 a 20:39). Da escuta até a identificação, passaram-se aproximadamente 14 segundos (20:39 a 20:53).

Demorou 15 segundos do aprendizado ao encaminhamento (20:53 a 21:08). Assim, o tempo total para a porta ficar realmente funcional para tráfego foi de cerca de 51 segundos (20:17 a 21:08).

Observação: Tecnicamente, o estágio de escuta e aprendizagem é de 15 segundos, que é como o parâmetro de retardo de encaminhamento é definido para essa VLAN. O estágio de aprendizado provavelmente está mais próximo de 15 segundos do que 14 segundos se você tiver medidas mais precisas. Nenhuma das medidas aqui são perfeitamente precisas. Você apenas tentou dar uma ideia de quanto tempo as coisas levam.

Você sabe pela saída e pelo comando **show** spantreee que o spanning tree está ativo nessa porta. Vamos analisar outros aspectos que poderiam tornar a porta mais lenta à medida que ela alcança o estado de encaminhamento. O comando **show port** capabilities mostra que essa porta tem a capacidade de criar um tronco e criar um EtherChannel. O comando show trunk informa que essa porta está no modo automático e que está definida para negociar o tipo de entroncamento a ser usado (ISL ou 802.1q, negociado através do Dynamic Trunking Protocol (DTP)).

```
Switch-A (enable) show port capabilities 2/1
Model                     WS-X5225R
Port                      2/1
Type                      10/100BaseTX

Speed                     auto,10,100
Duplex                    half,full
Trunk encap type          802.1Q,ISL
Trunk mode                on,off,desirable,auto,nonegotiate
Channel                   2/1-2,2/1-4
Broadcast suppression     percentage(0-100)
Flow control              receive-(off,on),send-(off,on)
Security                  yes
Membership                static,dynamic
Fast start                yes
Rewrite                   yes
Switch-A (enable) show trunk 2/1
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      auto         negotiate      not-trunking  1
```

Primeiro, você pode habilitar o Portfast na porta. A negociação de entroncamento e EtherChannel (PAgP) (DTP) ainda estão no modo automático.

```
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.

Switch-A (enable) set spantree portfast 2/1 enable

Warning: Spantree port fast start should only be enabled on ports connected
to a single host.  Connecting hubs, concentrators, switches, bridges, and so on to
a fast start port can cause temporary spanning tree loops.  Use with caution.

Spantree port 2/1 fast start enabled.

Switch-A (enable) show time
Fri Feb 25 2000, 13:45:23
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
Switch-A (enable)
2000 Feb 25 13:45:43 %PAGP-5-PORTTOSTP:Port 2/1 joined bridgeport 2/1
2000 Feb 25 13:45:44 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 change to forwarding.
```

Agora você tem um tempo total de**21 segundos!**Leva 20 segundos para ele ingressar no grupo de pontes (45:23 a 45:43). Mas como o Portfast está habilitado, leva somente um segundo até que o STP comece a encaminhar (em vez de 30 segundos). Você economizou 29 segundos ao habilitar o Portfast. Veja se você pode reduzir ainda mais o atraso.

Agora, você desativa o modo PAgP. Você pode ver pelo comando show port channel que o modo PAgP está definido como *auto*, o que significa que ele canaliza se for solicitado por um vizinho que fala PAgP. A canalização deve estar desligada por, no mínimo, um grupo de duas portas. Não é possível fazer isso para apenas uma porta individual.

```
Switch-A (enable) show port channel 2/1
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  auto      not channel

Switch-A (enable) set port channel 2/1-2 off
Port(s) 2/1-2 channel mode set to off.
```

Feche a porta e repita o teste.

```
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.

Switch-A (enable) show time
```

```
Fri Feb 25 2000, 13:56:23
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 13:56:32 %PAGP-5-PORTTOSTP:Port 2/1 joined bridgeport 2/1
2000 Feb 25 13:56:32 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 changed to forwarding.
```

Observe que agora leva apenas**9** segundos para atingir o estado de encaminhamento (56:23 a 56:32) em vez de 21 segundos como no teste anterior. Desativar o PAgP de forma automática neste teste economizou cerca de 12 segundos.

Desative o entroncamento (em vez de colocá-lo em automático) e veja como isso afeta o tempo necessário para que a porta atinja o estado de encaminhamento. Você desliga e liga novamente a porta e grava o tempo.

```
Switch-A (enable) set trunk 2/1 off
Port(s) 2/1 trunk mode set to off.
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.
```

Inicie o teste com o truncamento definido como desligado (em vez de automático).

```
Switch-A (enable) show time
Fri Feb 25 2000, 14:00:19
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 14:00:22 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
2000 Feb 25 14:00:23 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 change for forwarding.
```

você economizou alguns segundos no início, já que levou apenas**4** segundos para atingir o estado de encaminhamento do spanning tree (00:19 a 00:22). Você economizou cerca de 5 segundos ao alterar o modo de entroncamento *fromautotooff*.

(Opcional) Se o tempo de inicialização da porta do switch foi o problema, ele deve ser resolvido agora. Se você tiver que economizar mais alguns segundos de tempo, você poderia definir a porta como a velocidade e o duplex manualmente e não usar a autonegociação.

Se você definir a velocidade e o duplex manualmente neste lado, será necessário definir a velocidade e o duplex no outro lado também. Isso ocorre porque a configuração da velocidade e do duplex da porta desativa a autonegociação na porta, e o dispositivo que se conecta não vê parâmetros de autonegociação. O dispositivo de conexão se conecta apenas em half-duplex e a incompatibilidade de duplex resultante provoca erros de porta e desempenho insatisfatórios. Lembre-se de que, se você definiu a velocidade e o duplex de um lado, deverá defini-los também no dispositivo de conexão para evitar esses problemas.

Para ver o status da porta após definir a velocidade e o duplex da **porta doshow**.

```
Switch-A (enable) set port speed 2/1 100
Port(s) 2/1 speed set to 100Mbps.
Switch-A (enable) set port duplex 2/1 full
Port(s) 2/1 set to full-duplex.
Switch-A (enable) show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     connected  1          normal   full   100 10/100BaseTX
...
```

Estes são os resultados de tempo:

```
Switch-A (enable) show time
Fri Feb 25 2000, 140528 Eastern
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 140529 Eastern -0500 %PAGP-5-PORTTOSTP:Port 2/1 joined bridgeport 2/1
2000 Feb 25 140530 Eastern -0500 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 changed to
forwarding.
```

O resultado final dá um tempo de**2 segundos**(0528 a 0530).

Você fez outro teste visualmente cronometrado iniciando um ping contínuo (ping -t) direcionado ao switch em um PC conectado ao switch. Em seguida, você desconectou o cabo do switch. Os pings começaram a falhar. Em seguida, você reconectou o cabo ao switch e verificou esses relógios para ver quanto tempo o switch levou para responder aos pings do PC. Levou cerca de 5 a 6 segundos com a autonegociação para velocidade e duplex ligado e cerca de 4 segundos com a autonegociação para velocidade e duplex desligado.

Há muitas variáveis nesse teste (inicialização do PC, software do PC, respostas da porta do console do switch a solicitações, etc.), mas você só queria ter uma ideia do tempo que levaria para obter uma resposta do ponto de vista dos PCs. Todos os testes eram do ponto de vista da mensagem de depuração interna dos switches.

Como reduzir o retardo na inicialização no Switch Catalyst 2900XL/3500XL

Os modelos 2900XL e 3500XL podem ser configurados em um navegador da Web ou por SNMP ou pela interface de linha de comando (CLI). você usa o CLI. Este é um exemplo onde você visualiza o estado do spanning tree de uma porta, ativa o portfast e verifica se ele está ativado. O 2900XL/3500XL suporta EtherChannel e entroncamento, mas não suporta criação dinâmica de EtherChannel (PAgP) ou negociação dinâmica de entroncamento (DTP) na versão que você testou (11.2(8.2)SA6), portanto, você não precisa desativá-los neste teste. Além disso, depois que você ativa o portfast, o tempo decorrido para que a porta seja ativada já é menos de 1 segundo, portanto, não há muito motivo para tentar alterar as configurações de negociação de velocidade/duplex para acelerar as coisas. você espera que um segundo seja rápido o suficiente!

Por padrão, o PortFast está desativado nas portas do switch. Estes são os comandos para ativar o PortFast:

Configuração

```
2900XL#conf t
2900XL(config)#interface fastEthernet 0/1
2900XL(config-if)#spanning-tree portfast
2900XL(config-if)#exit
2900XL(config)#exit
2900XL#copy run start
```

Essa plataforma é como o roteador Cisco IOS; você deve salvar a configuração (**copy run start**) se quiser salvá-la permanentemente.

Verificação

Para verificar se o PortFast está ativado, emita este comando.

```
2900XL#show spanning-tree interface fastEthernet 0/1
Interface Fa0/1 (port 13) in Spanning tree 1 is FORWARDING
   Port path cost 19, Port priority 128
   Designated root has priority 8192, address 0010.0db1.7800
   Designated bridge has priority 32768, address 0050.8039.ec40
   Designated port is 13, path cost 19
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 2105, received 1
   The port is in the portfast mode
```

Consulte a configuração de switches.

```
2900XL#show running-config
Building configuration...

Current configuration:
!
version 11.2
...
!
interface VLAN1
 ip address 172.16.84.5 255.255.255.0
 no ip route-cache
!
interface FastEthernet0/1
 spanning-tree portfast
!
interface FastEthernet0/2
!
...
```

Testes de cronometragem no Catalyst 2900XL

Esses são os testes de temporização no Catalyst 2900XL.

A versão de software 11.2 (8.2) SA6 foi usada no 2900XL para esses testes.

```
Switch#show version
Cisco Internetwork Operating System Software
Cisco IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 11.2(8.2)SA6, MAINTENANCE
INTERIM SOFTWARE
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 23-Jun-99 16:25 by boba
Image text-base: 0x00003000, data-base: 0x00259AEC

ROM: Bootstrap program is C2900XL boot loader

Switch uptime is 1 week, 4 days, 22 hours, 5 minutes
System restarted by power-on
System image file is "flash:c2900XL-c3h2s-mz-112.8.2-SA6.bin", booted via console

cisco WS-C2924-XL (PowerPC403GA) processor (revision 0x11) with 8192K/1024K bytes of
memory.
Processor board ID 0x0E, with hardware revision 0x01
Last reset from power-on

Processor is running Enterprise Edition Software
Cluster command switch capable
Cluster member switch capable
24 Ethernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:50:80:39:EC:40
Motherboard assembly number: 73-3382-04
Power supply part number: 34-0834-01
Motherboard serial number: FAA02499G7X
Model number: WS-C2924-XL-EN
System serial number: FAA0250U03P
Configuration register is 0xF
```

você quer que o switch nos diga o que acontece e quando acontece, então digite estes comandos:

```
2900XL(config)#service timestamps debug uptime
2900XL(config)#service timestamps log uptime
2900XL#debug spantree events
Spanning Tree event debugging is on
2900XL#show debug
General spanning tree:
  Spanning Tree event debugging is on
```

Em seguida, você desliga a porta em questão.

```
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#interface fastEthernet 0/1
2900XL(config-if)#shut
2900XL(config-if)#
00:31:28: ST: sent Topology Change Notice on FastEthernet0/6
00:31:28: ST: FastEthernet0/1 - blocking
00:31:28: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively
down
00:31:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down
2900XL(config-if)#exit
2900XL(config)#exit
2900XL#
```

Neste ponto, você cola esses comandos da área de transferência no switch. Estes comandos exibem a hora no 2900XL e ativam a porta novamente:

```
show clock
conf t
int f0/1
no shut
```

Por padrão, Portfast está desligada. Você pode confirmar isso de duas maneiras. A primeira maneira é que o comando **show spanning-tree** interface não menciona o Portfast. A segunda maneira é observar essa configuração que é executada e onde você não vê o comando **espanning-tree** portfastsob a interface.

```
2900XL#show spanning-tree interface fastEthernet 0/1
Interface Fa0/1 (port 13) in Spanning tree 1 is FORWARDING
   Port path cost 19, Port priority 128
   Designated root has priority 8192, address 0010.0db1.7800
   Designated bridge has priority 32768, address 0050.8039.ec40
   Designated port is 13, path cost 19
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 887, received 1
[Note: there is no message about being in portfast mode is in this spot...]

2900XL#show running-config
Building configuration...
...
!
interface FastEthernet0/1
```

```
[Note: there is no spanning-tree portfast command under this interface...]
!
```

Este é o primeiro teste de sincronismo com o Portfast desativado.

```
2900XL#show clock
*00:27:27.632 UTC Mon Mar 1 1993
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#int f0/1
2900XL(config-if)#no shut
2900XL(config-if)#
00:27:27: ST: FastEthernet0/1 - listening
00:27:27: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
00:27:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
00:27:42: ST: FastEthernet0/1 - learning
00:27:57: ST: sent Topology Change Notice on FastEthernet0/6
00:27:57: ST: FastEthernet0/1 - forwarding
```

O tempo total desde o desligamento até o início do encaminhamento da porta foi de**30 segundos**(27:27 a 27:57)

Para ativar o PortFast, faça o seguinte:

```
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#interface fastEthernet 0/1
2900XL(config-if)#spanning-tree portfast
2900XL(config-if)#exit
2900XL(config)#exit
2900XL#
```

Para verificar se o Portfast está habilitado, use o comando **show spanning-tree** interface. Observe que a saída do comando (extremidade próxima) indica que o Portfast está habilitado.

```
2900XL#show spanning-tree interface fastEthernet 0/1
Interface Fa0/1 (port 13) in Spanning tree 1 is FORWARDING
   Port path cost 19, Port priority 128
   Designated root has priority 8192, address 0010.0db1.7800
   Designated bridge has priority 32768, address 0050.8039.ec40
   Designated port is 13, path cost 19
   Timers: message age 0, forward delay 0, hold 0
```

```
   BPDU: sent 1001, received 1
```

The port is in the portfast mode

Também é possível ver se o Portfast está habilitado na saída de configuração.

```
2900XL#sh  ru
Building configuration...
...
interface FastEthernet0/1
 spanning-tree portfast

...
```

Agora faça o teste de tempo com PortFast ativado

```
2900XL#show clock
*00:23:45.139 UTC Mon Mar 1 1993
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#int f0/1
2900XL(config-if)#no shut
2900XL(config-if)#
00:23:45: ST: FastEthernet0/1 -jump to forwarding from blocking
00:23:45: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
00:23:45: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

Neste caso, o tempo total foi inferior a **1 segundo**. Se o retardo de inicialização da porta no switch era o problema, o portfast deve resolvê-lo.

Lembre-se de que o switch não suporta negociação de tronco no momento, portanto, não é necessário desligá-lo. Ele também não suporta PAgP para entroncamento, portanto, você também não precisa desativá-lo. O switch suporta autonegociação de velocidade e duplex, mas como o atraso é tão pequeno, isso não seria um motivo para desativá-lo.

você também fez o teste de ping de uma estação de trabalho para o switch. Foram necessários cerca de 5 a 6 segundos para que a resposta viesse do switch, independentemente da autonegociação de velocidade e duplex estar ativada ou desativada.

Como reduzir o retardo na inicialização no Switch Catalyst 1900/2800

Os 1900/2820 referem-se a Portfast por outro nome: Spantree Start-Forwarding. Para a versão do software, você executa (V8.01.05), os switches padrão são: Portfast está habilitado nas portas

Ethernet (10Mbps) e Portfast está desabilitado nas portas Fast Ethernet (uplink). Assim, quando **vocêmostrar** rpara ver a configuração, se uma porta Ethernet não disser nada sobre o Portfast, então o Portfast está habilitado. Se ela indicar "no spantree start-forwarding" na configuração, o PortFast será desativado. Em uma porta FastEthernet (100Mbps), o oposto é verdadeiro: Para uma porta FastEthernet, Portfast está somente ativado se a porta mostrar "spantree start-forwarding" na configuração.

Este é um exemplo de configuração Portfast em uma porta FastEthernet. Esses exemplos usam o software da edição Enterprise, versão 8. O 1900 salva automaticamente a configuração depois que as alterações são feitas. Lembre-se de que você não deseja que o PortFast esteja ativado em nenhuma porta que se conecte a outro switch ou hub, somente se a porta se conectar a uma estação final. A configuração é salva automaticamente na NVRAM.

Configuração

```
1900#show version
Cisco Catalyst 1900/2820 Enterprise Edition Software
Version V8.01.05
Copyright (c) Cisco Systems, Inc.  1993-1998
1900 uptime is 0day(s) 01hour(s) 10minute(s) 42second(s)
cisco Catalyst 1900 (486sxl) processor with 2048K/1024K bytes of memory
Hardware board revision is 5
Upgrade Status: No upgrade currently in progress.
Config File Status: No configuration upload/download is in progress
27 Fixed Ethernet/IEEE 802.3 interface(s)
Base Ethernet Address: 00-50-50-E1-A4-80
1900#conf t
Enter configuration commands, one per line.  End with CNTL/Z
1900(config)#interface FastEthernet 0/26
1900(config-if)#spantree start-forwarding
1900(config-if)#exit
1900(config)#exit
1900#
```

Verificação

Uma forma de verificar se o portfast está ativado é observar a configuração. Lembre-se, uma porta FastEthernet deve informar que está ativo. Uma porta Ethernet tem esse recurso ativado, a não ser que a configuração mostre que está desativado. Nesta configuração, a interface Ethernet 0/1 está desativada como PortFast (você pode ver o comando para desativá-la), interface Ethernet 0/2 tem PortFast ligado (você não vê nada - o que significa que ela está ativa) e a interface FastEthernet 0/26 (porta A no sistema de menu) tem PortFast ativado (você pode ver o comando para ligá-lo).

```
1900#show running-config
Building configuration...
...
!
interface Ethernet 0/1

  no spantree start-forwarding
!
interface Ethernet 0/2

!
...
```

```
!
interface FastEthernet 0/26
  spantree start-forwarding
```

A maneira mais fácil de exibir o status do portfast é por meio do sistema de menus. Se você escolher (**P**) para Configuração de porta no menu principal e, em seguida, escolher **aport**, a saída indica se o modo Port fast está habilitado. Esta saída é para a porta FastEthernet 0/26, que é a porta "A" nesse switch.

```
        Catalyst 1900 - Port A Configuration

        Built-in 100Base-FX
        802.1d STP State:  Blocking     Forward Transitions:  0

    ---------------------- Settings ------------------------------------
     [D] Description/name of port
     [S] Status of port                              Suspended-no-linkbeat
     [I] Port priority (spanning tree)               128 (80 hex)
     [C] Path cost (spanning tree)                   10
     [H] Port fast mode (spanning tree)              Enabled
     [E] Enhanced congestion control                 Disabled
     [F] Full duplex / Flow control                  Half-Duplex

    ---------------------- Related Menus -----------------------------------
     [A] Port addressing           [V] View port statistics
     [N] Next port                 [G] Goto port
     [P] Previous port             [X] Exit to Main Menu

Enter Selection:
```

Testes de cronometragem no Catalyst 1900

Os valores de tempo são mais difíceis de verificar em um 1900/2820 devido à falta de ferramentas de depuração, então você acabou de iniciar um ping de um PC conectado ao switch direcionado ao próprio switch. Você desconectou e reconectou o cabo e registrou quanto tempo levou para o switch responder ao ping com o Portfast ativado e com o Portfast desativado. Para uma porta Ethernet com Portfast ativado (o estado padrão), o PC recebeu uma resposta em**5-6 segundos**. Com Portfast desativado, o PC recebeu uma resposta em 34 a 35 segundos.

Um benefício adicional ao Portfast

Há outro benefício relacionado ao spanning tree para o uso de PortFast na rede. Toda vez que um link se torna ativo e é movido para o estado de encaminhamento no spanning tree, o switch envia um pacote especial de spanning tree chamado de TCN (notificação de alteração de topologia). A notificação de TCN é passada até a raiz da spanning tree, onde ela é propagada para todos os switches na VLAN. Isso faz com que todos os switches eliminem a tabela de endereços MAC com o parâmetro de atraso de encaminhamento. O parâmetro de retardo de encaminhamento geralmente é definido como 15 segundos. Toda vez que uma estação de trabalho entra no grupo de ponte, os endereços MAC em todos os switches são classificados por 15 segundos, em vez dos 300 segundos normais.

Quando uma estação de trabalho se torna ativa, ela não altera realmente a topologia em grau significativo, no que diz respeito a todos os switches da VLAN, portanto é desnecessário que eles precisem passar pelo período de TCN de envelhecimento rápido. Se você ativar o PortFast, o switch não envia pacotes de TCN quando uma porta se torna ativa.

Comandos a serem usados para verificar se a configuração funciona

Esta é uma lista de comandos a serem usados quando você verificar se a configuração funciona.

4000/5000/6000

show port spantree 2/1 – veja se "Fast-Start" (Portfast) está ativado ou desativado

show spantree 1- veja todas as portas na VLAN 1 e se elas têm o "Início rápido" habilitado

show port channel –verifica se você tem qualquer canal ativo

show port channel 2- veja o modo de canal (auto, off e assim por diante) para cada porta no módulo 2

show trunk 2- consulte o modo de tronco (auto, off e assim por diante) para cada porta no módulo 2

show port - visualiza o status (conectado, não conectado, assim por diante), velocidade, duplex para todas as portas no switch

2900XL/3500XL

show spanning-tree interface FastEthernet 0/1 – para ver se Portfast está habilitado nessa porta (o Portfast não será mencionado se não estiver habilitado)

show running-config - se uma porta mostrar o comando spanning-tree portfast, o Portfast será habilitado.

1900/2800

show running-config - para ver as configurações atuais (alguns comandos são invisíveis quando representam as configurações padrão do switch)

Use o sistema de menus para a tela de status da porta

Comandos a serem usados para solucionar problemas de configuração

Esta é uma lista de comandos a serem usados para solucionar problemas de configuração.

4000/5000/6000

show port spantree 2/1 – veja se "Fast-Start" (Portfast) está ativado ou desativado

show spantree 1- veja todas as portas na VLAN 1 e se elas têm o "Início rápido" habilitado

show port channel –verifica se você tem qualquer canal ativo

show port channel 2- veja o modo de canal (auto, off e assim por diante) para cada porta no módulo 2

show trunk 2- consulte o modo de tronco (auto, off e assim por diante) para cada porta no módulo 2

show port- ver o status (connected, notconnect e do on), velocidade, duplex para todas as portas no switch

show Logging - visualiza quais tipos de mensagens geram saída de registro

set logging level spantree 7 - define o switch para registrar a porta da árvore de expansão, informa o tempo real no console

set port disable 2/1 - desliga a porta no software (como "shutdown" no roteador).

set port enable 2/1 - ativa a porta no software (como "no shutdown" no roteador)

show time - mostra o tempo atual em segundos (usado no início de um teste de temporização)

show port capabilities Veja quais recursos estão implementados na porta

set trunk 2/1 off - desativa o modo de truncamento (para acelerar o tempo de inicialização da porta)

set port channel 2/1-2 off - desativa o modo EtherChannel (PAgP) (para acelerar o tempo de inicialização da porta)

set port speed 2/1 100- configure a porta para 100Mbps e desative a autonegociação

set port duplex 2/1 full define a porta dúplex como completa

2900XL/3500XL

service timestamps debug uptime - mostra o tempo gasto com as mensagens de depuração

service timestamps log uptime – mostra o tempo com as mensagens de registro

debug spantree events - mostra quando a porta passa pelos estágios de spanning tree

exibir relógio - para ver o horário atual (para os testes de cronometragem)

show spanning-tree interface FastEthernet 0/1 – para ver se Portfast está habilitado nessa porta (o Portfast não será mencionado se não estiver habilitado)

shut - desliga uma porta de software

no shut Para ativar uma porta no software

1900/2800

show running-config - para ver as configurações atuais (alguns comandos são invisíveis quando representam as configurações padrão do switch)

Configurar e solucionar problemas de IP Multilayer Switching (MLS)

Objetivos

Este documento descreve como solucionar problemas de Multilayer Switching (MLS) para IP. Esse recurso se tornou um método altamente desejado para acelerar o desempenho de roteamento com o uso de circuitos integrados específicos de aplicativos dedicados (ASICs). O roteamento tradicional é feito por meio de uma CPU e um software central; o MLS descarrega uma parte significativa do roteamento (regravação de pacotes) no hardware e também é chamado de switching. MLS e switching de terceira camada são termos equivalentes. O recurso NetFlow do Cisco IOS é distinto e não abordado neste documento. O MLS também inclui suporte para IPX (IPX MLS) e multicast (MPLS), mas este documento concentra-se exclusivamente em como solucionar problemas básicos de MLS IP.

Introduction

A necessidade por maior desempenho aumenta à medida que demandas maiores são exigidas das redes. Mais e mais PCs estão conectados às LANs, às WANs e à Internet, e seus usuários requerem acesso rápido a bancos de dados, arquivos/páginas da Web, aplicativos em rede, outros PCs e transmissão de vídeo. Para manter as conexões rápidas e confiáveis, as redes devem conseguir se ajustar rapidamente às alterações e falhas e encontrar o melhor caminho, tudo isso enquanto permanecem o mais invisível possível para os usuários finais. Os usuários finais que experimentam um fluxo rápido de informações entre seu PC e o servidor com uma lentidão mínima da rede ficam muito satisfeitos. A determinação do melhor caminho é a função principal dos protocolos de roteamento, e isso pode ser um processo intensivo de CPU; um aumento significativo de desempenho é obtido com o descarregamento de uma parte dessa função para o hardware de switching. Esse é o ponto do recurso de MLS.

Há três componentes principais do MLS: dois deles são o MLS-RP e o MLS-SE. O MLS-RP é o roteador ativado para MLS, que executa a função tradicional de roteamento entre sub-

redes/VLANs. O MLS-SE é um switch ativado para MLS, que normalmente requer um roteador para rotear entre sub-redes/VLANs, mas com hardware e software especiais, pode manipular a regravação do pacote. Quando um pacote atravessa uma interface roteada, as partes do pacote que não contêm dados são alteradas (regravadas) à medida que ele é transportado salto a salto para o seu destino. Pode haver confusão aqui, pois parece que um dispositivo da camada dois assume uma tarefa da camada três; na verdade, o switch está apenas reescrevendo as informações da camada três e está alternando entre sub-redes/VLANs—o roteador ainda é responsável pelos cálculos de rota baseados em padrões e pela determinação do melhor caminho. Grande parte dessa confusão pode ser evitada se você mentalmente manter as funções de roteamento e switching separadas, especialmente quando, como geralmente é o caso, estão contidas no mesmo chassi (como com um MLS-RP interno). Pense no MLS como uma maneira muito mais avançada de armazenar o roteador em cache, com o cache separado do roteador em um switch. O MLS-RP e o MLS-SE, juntamente com os mínimos respectivos de seus hardware e software, são necessários ao MLS.

O MLS-RP pode ser interno (instalado em um chassi do switch) ou externo (conectado por meio de um cabo a uma porta de tronco no switch). Exemplos de MLS-RPs internos são o módulo de switch de rota (RSM) e a placa de recurso de switch de rota (RSFC), que são instalados em um slot ou supervisor de um membro da família Catalyst 5xxx, respectivamente; o mesmo se aplica à placa de recurso de switch multicamada (MSFC) para a família Catalyst 6xxx. Exemplos de MLS-RPs externos incluem qualquer membro dos Cisco 7500, 7200, 4700, 4500 ou 3600 Series Routers. Em geral, para suportar o recurso MLS IP, todos os MLS-RPs exigem uma versão mínima do Cisco IOS nas trilhas 11.3WA ou 12.0WA; consulte a documentação da versão para obter detalhes. Além disso,**o MLS deve ser** habilitado para que um roteador seja um MLS-RP.

O MLS-SE é um switch com hardware especial. Para um membro da família Catalyst 5xxx, o MLS exige que o supervisor tenha uma placa de recurso NetFlow (NFFC - NetFlow Feature Card) instalada; o Supervisor IIG e o IIIG têm uma, por padrão. Além disso, um mínimo limitado do software Catalyst OS 4.1.1 também é necessário. Observe que a sequência 4.x passou por "Implantação geral (GD)" ou por critérios rigorosos de usuário final e metas de experiência de campo em busca de estabilidade. Verifique o site da Cisco para obter as versões mais recentes. O IP MLS é suportado e habilitado automaticamente para o hardware e o software do Catalyst 6xxx com o MSFC/PFC (por padrão, outros roteadores têm o MLS desabilitado). Observe que o IPX MLS e o MLS para multicast podem ter diferentes requisitos de hardware e software (Cisco IOS e Catalyst OS). Mais plataformas Cisco suportam/podem suportar o recurso MLS. Além disso,**o MLS deve ser** habilitado para que um switch seja um MLS-SE.

O terceiro componente principal do MLS é o MLSP (Multilayer Switching Protocol). Isso ocorre porque quando você compreende os conceitos básicos de MLSP, obtém o coração do MLS, e isso é essencial para solucionar com eficiência os problemas do MLS. O MLSP é utilizado pelo MLS-RP e pelo MLS-SE para se comunicarem entre si; tarefas que ativam o MLS e instalam, atualizam ou excluem fluxos (informações de cache) e o gerenciamento e a exportação das estatísticas de fluxo (a Exportação de Dados do NetFlow é abordada em outra documentação). O MLSP também permite que o MLS-SE aprenda os endereços de Controle de acesso de mídia (MAC, camada dois) das interfaces de roteador ativadas por MLS, verifique a máscara de fluxo do MLS-RP (explicado posteriormente neste documento) e confirme se o MLS-RP está funcionando. O MLS-RP envia pacotes multicast de saudação a cada 15 segundos com MLSP; se três desses intervalos forem perdidos, o MLS-SE reconhecerá que o MLS-RP falhou ou que a conectividade com ele foi perdida.

O diagrama ilustra três itens essenciais que devem ser concluídos (com MLSP) para que um atalho seja criado: as etapas de candidato, ativador e cache. O MLS-SE verifica se há uma entrada de MLS em cache; se a entrada do cache de MLS e as informações do pacote corresponderem (um acerto), o cabeçalho do pacote será regravado localmente no switch (um

atalho ou desvio do roteador) em vez de ser enviado para o roteador como normalmente acontece. Os pacotes que não correspondem e são enviados para o MLS-RP são pacotes candidatos; isto é, há uma possibilidade de comutá-los localmente. Depois de passar o pacote candidato através da máscara de fluxo de MLS (explicado em uma seção posterior) e reescrever as informações contidas no cabeçalho do pacote (a parte de dados não é tocada), o roteador envia-a para o próximo salto pelo caminho de destino. O pacote é denominado pacote habilitador. Se o pacote retornar para o mesmo MLS-SE do qual partiu, um atalho MLS será criado e colocado no cache MLS; a regravação desse pacote e de todos os pacotes semelhantes que o rastreiam (chamado fluxo) agora é feita localmente pelo hardware do switch, em vez de pelo software do roteador.**O mesmo MLS-SE deve ver os pacotes candidatos e ativadores de um fluxo específico para que um atalho MLS seja criado** (é por isso que a topologia de rede é importante para o MLS). Lembre-se de que o ponto de MLS é permitir o caminho de comunicação entre dois dispositivos em VLANs diferentes, conectados do mesmo switch, ignorar o roteador e melhorar o desempenho da rede.

Com o uso da máscara de fluxo (essencialmente uma lista de acesso), o administrador pode ajustar o grau de similaridade desses pacotes e ajustar o escopo dos fluxos: endereço de destino; endereços de destino e de origem; ou informações de destino, origem e camada quatro. Observe que o primeiro pacote de um fluxo sempre passa pelo roteador; a partir daí, ele é comutado localmente. Cada fluxo é unidirecional; a comunicação entre PCs, por exemplo, exige a configuração e o uso de dois atalhos. O principal objetivo do MLSP é configurar, criar e manter esses atalhos.

Esses três componentes (o MLS-RP, o MLS-SE e o MLSP) liberam recursos vitais do roteador quando permitem que outros componentes da rede assumam algumas de suas funções. Dependendo da topologia e da configuração, o MLS fornece um método simples e altamente eficaz que aumenta o desempenho da rede na LAN.

Solução de problemas de tecnologia IP MLS

Um fluxograma a ser usado para solucionar problemas básicos de IP MLS é incluído e discutido. É derivado dos tipos mais comuns de casos MLS-IP abertos no site de suporte técnico da Cisco e enfrentados pelos usuários e engenheiros de suporte técnico até o momento em que este documento foi criado. O MLS é um recurso robusto, e você não deve ter problemas com ele; se houver um problema, isso o ajudará a resolver os tipos de problemas de MLS IP que você provavelmente enfrentará. Algumas suposições essenciais são feitas:

Você está familiarizado com as etapas de configuração básica necessárias para ativar o IP MLS no roteador e nos switches e concluiu estas etapas: consulte os recursos listados no final deste documento para obter material excelente.

O roteamento IP está ativado no MLS-RP (está ativado por padrão): se o **comando no ip** routingaparecer na configuração global de **ashow run**, ele foi desativado e o IP MLS não funciona.

Existe conectividade IP entre o MLS-RP e o MLS-SE:faça ping nos endereços IP do roteador a partir do switch e procure pontos de exclamação (chamados de "bangs") para exibir em retorno.

As interfaces MLS-RP estão em um estado 'up/up' no roteador: **typeshow ip interface** informe ao roteador para confirmar isso.

Aviso: sempre que você fizer alterações de configuração em um roteador destinado a ser permanente, lembre-se de salvar essas alterações com **acopy running-config starting-config** (versões abreviadas desse comando **includecopy run startandwr mem).** Todas as modificações de configuração serão perdidas se o roteador for recarregado ou redefinido. O RSM, RSFC e MSFC são roteadores, não switches. Em contraste, as alterações feitas no prompt do switch de um membro da família Catalyst 5xxx ou 6xxx são salvas automaticamente.

Esta seção soluciona problemas de tecnologia IP MLS.

Os requisitos mínimos de hardware e software foram atendidos?

Faça a atualização do MLS-RP e SE para atender aos requisitos mínimos de software e de hardware. Não é necessário hardware adicional para o MLS-RP. Embora o MLS possa ser configurado em interfaces não entroncamento, a conexão com o MLS-SE geralmente é através de interfaces de VLAN (como com um RSM) ou de suporte a entroncamento (pode ser configurado para transportar várias informações de VLAN configurando ISL ou 802.1q). Além disso, lembre-se de que, desde o momento da publicação, somente membros das famílias de roteador 7500, 7200, 4700, 4500 e 3600 são compatíveis com MLS externamente. Atualmente, apenas esses roteadores externos e os roteadores que se encaixam nas famílias de switches Catalyst 5xxx ou 6xxx (como o RSM e o RSFC para a família Catalyst 5xxx e o MSFC para a família Catalyst 6xxx) podem ser MLS-RPs. O MSFC requer também o PFC (Placa de Recurso de Política), ambos instalados no Catalyst 6xx Supervisor. O IP MLS agora é um recurso padrão no software do roteador Cisco IOS 12.0 e posterior. O software Cisco IOS inferior ao Cisco IOS 12.0 geralmente requer um treinamento especial; para tal suporte IP MLS, instale as imagens mais recentes no Cisco IOS 11.3 que tenham as letras 'WA' em seus nomes de arquivos.

Para o MLS-SE, uma Placa de Recurso NetFlow (NFFC - NetFlow Feature Card) é necessária para um membro da família Catalyst 5xxx; essa placa é instalada no módulo Supervisor do switch Catalyst e está incluída como hardware padrão nos Supervisores mais recentes da série Catalyst 5xxx (isto é, desde 1999). O NFFC não é suportado no Supervisor I ou II e é uma opção em versões anteriores do Supervisor III. Além disso, um mínimo de 4.1.1 CatOS é necessário para IP MLS. Em contrapartida, para a família Catalyst 6xxx, o hardware necessário vem como equipamento padrão e há suporte para o MLS de IP desde a primeira versão do software CatOs, a 5.1.1 (na verdade, MLS é um elemento padrão e essencial para o alto desempenho). Com novas plataformas e novos softwares lançados que suportam IP MLS, é importante verificar a documentação e as notas de versão e, em geral, instalar a versão mais recente no treinamento mais baixo que atenda aos seus requisitos de recursos. Sempre verifique as notas de versão e consulte seu escritório de vendas local da Cisco para novos desenvolvimentos de suporte e recursos de MLS.

Comandos fundidos para verificar a versão instalada do hardware e do software **areshow** no roteador **e no módulo show** no switch

Observação: a família de switches Catalyst 6xxx NÃO suporta um MLS-RP externo no momento. O MLS-RP deve ser um MSFC.

Os dispositivos de origem e destino em VLANs diferentes estão saindo do mesmo MLS-SE, compartilhando um único MLS-RP?

Esse é um requisito de topologia básico de MLS que o roteador têm um caminho para cada uma das VLANs. Lembre-se de que o ponto do MLS é criar um atalho entre duas VLANs, de modo que o roteamento entre os dois dispositivos finais possa ser executado pelo switch, e

isso libera o roteador para outras tarefas. Na verdade, o switch não faz o roteamento; ele regrava os quadros para que pareça aos dispositivos finais que eles conversam através do roteador. Se os dois dispositivos estiverem na mesma VLAN, o MLS-SE alterna o quadro localmente sem o uso de MLS, à medida que os switches fazem isso de forma transparente, e nenhum atalho de MLS é criado. Pode haver vários switches e roteadores na rede, e até mesmo vários switches ao longo do caminho de fluxo, mas o caminho entre os dois dispositivos finais para os quais um atalho de MLS deve incluir um único MLS-RP nessa VLAN para esse caminho. Em outras palavras, o fluxo da fonte para o destino deve cruzar um limite de VLAN no mesmo MLS-RP, e o candidato e o par de pacote de habilitador devem ser vistos pelo mesmo MLS-SE para o atalho de MLS a ser criado. Se esses critérios não forem atendidos, o pacote será roteado normalmente sem o uso de MLS. Consulte os documentos sugeridos no final deste documento para obter diagramas e discussões em relação a topologias de rede com e sem suporte.

O MLS-RP contém a instrução **anmls rp** ipna configuração global e na configuração de interface?

Se não houver um presente, **addmls rp** ipstatement adequadamente no MLS-RP. Exceto com roteadores com os quais um IP MLS é ativado automaticamente (como o Catalyst 6xxx MSFC), esta é uma etapa obrigatória da configuração. Para a maioria dos MLS-RPs (roteadores configurados para IP MLS), essa instrução deverá aparecer na configuração global e na configuração da interface.

Observação: ao configurar o MLS-RP, lembre-se de colocar o comando **themls rp management-**interface em uma de suas interfaces IP MLS. Essa etapa obrigatória faz com que o MLS-RP saia da interface que deve enviar mensagens de MLSP para se comunicar com o MLS-SE. Mais uma vez, é necessário colocar este comando apenas em uma interface.

Existem recursos configurados no MLS-RP que desativam automaticamente o MLS nessa interface?

Há várias opções de configuração no roteador que não são compatíveis com o MLS. Isto inclui relatório de IP, criptografia, compressão, segurança de IP, Tradução de endereços de rede (NAT) e Taxa de acesso confirmada (CAR). Para obter mais informações, consulte links em relação à configuração de MLS IP incluída no final deste documento. Os pacotes que atravessam uma interface de roteador configurada com qualquer um desses recursos devem ser roteados normalmente; nenhum atalho MLS é criado. Para que o MLS funcione, desative esses recursos na interface MLS-RP.

Outra função importante que afeta o MLS é as listas de acesso, de entrada e saída. Uma discussão adicional dessa opção está incluída em " máscaras de fluxo".

O MLS-SE reconhece o endereço de MLS-RP?

Para que o MLS funcione, o switch deve reconhecer o roteador como MLS-RP. Os MLS-RPs internos (mais uma vez, o RSM ou RSFC em um membro da família Catalyst 5xxx e o MSFC em um membro da família Catalyst 6xxx) são reconhecidos automaticamente pelo MLS-SE em que estão instalados. Para MLS-RPs externos, é necessário informar explicitamente ao switch o endereço do roteador. Esse endereço não é realmente um endereço IP, embora em MLS-RPs externos ele seja escolhido na lista de endereços IP configurados nas interfaces do roteador; é simplesmente um ID de roteador. Na verdade, para MLS-RPs internos, o

MLS-ID normalmente nem é um endereço IP configurado no roteador; como os MLS-RPs internos são incluídos automaticamente, geralmente é um endereço de loopback (127.0.0.x). Para que o MLS funcione, inclua no MLS-SE o MLS-ID encontrado no MLS-RP.

Usa show mls rpno roteador para localizar o MLS-ID. Em seguida, configure esse ID no switch com o comando **set mls include <MLS-ID>**. Essa é uma etapa de configuração necessária quando você usa MLS-RPs externos.

Observação: se você alterar o endereço IP das interfaces MLS-RP e recarregar o roteador, o processo MLS no roteador poderá escolher um novo MLS-ID. Esse novo MLS-ID pode ser diferente do MLS-ID que foi incluído manualmente no MLS-SE, o que pode fazer com que o MLS pare; isso não é uma falha de software, mas um efeito do switch que tenta se comunicar com um MLS-ID que não é mais válido. Certifique-se de incluir esse novo MLS-ID no switch para que o MLS funcione novamente. Também pode ser necessário desativar/ativar o IP MLS.

Observação: quando o MLS-SE não está diretamente conectado ao MLS-RP, como nesta topologia, o endereço que deve ser incluído no MLS-SE pode aparecer como o endereço de loopback mencionado: um switch conectado entre o MLS-SE e o MLS-RP. Você deve incluir o MLS-ID mesmo que o MLS-RP seja interno. Para o segundo switch, o MLS-RP aparece como um roteador externo, pois o MLS-RP e o MLS-SE não estão contidos no mesmo chassi.

As interfaces MLS-RP e MLS-SE estão no mesmo domínio habilitado para VTP?

O MLS exige que os componentes do MLS, juntamente com as estações finais, estejam no mesmo domínio do VTP (Virtual Trunking Protocol). O VTP é um protocolo de camada dois usado para gerenciar VLANs em vários switches Catalyst de um switch central. Ele permite que um administrador crie ou exclua uma VLAN em todos os switches de um domínio e não tenha que fazer isso em todos os switches desse domínio. O Protocolo de Comutação Multicamada (MLSP - Multilayer Switching Protocol), que o MLS-SE e o MLS-RP usam para se comunicarem entre si, não atravessa um limite de domínio VTP. Se o administrador de rede tiver o VTP habilitado nos switches (o VTP é habilitado nos membros da família Catalyst 5xxx e 6xxx por padrão), use o comando **show vtp** domain no switch para saber em que domínio VTP o MLS-SE foi colocado. Exceto para o Catalyst 6xxx MSFC, no qual o MLS é essencialmente o recurso *aplug-and-*play, você precisa adicionar o domínio VTP a cada uma das interfaces MLS do roteador. Isso permite que MLSP multicasts se movam entre o MLS-RP e o MLS-SE e que o MLS funcione.

No modo de configuração de interface do MLS-RP, insira esses comandos:

no mls rp ipDesative o MLS na interface MLS-RP afetada antes de modificar o domínio do VTP.

mls rp vtp-domain < VTP domain name> O nome do domínio do VTP em cada interface ativada por MLS deve corresponder ao switch.

mls rp vlan-id <VLAN #> É necessário apenas para as interfaces MLS-RP externas de entroncamento não ISL.

mls rp management-interfaceFaça isso para apenas uma interface no MLS-RP. Essa etapa necessária informa ao MLS-RP de qual interface ele deve enviar mensagens MLSP.

mls rp ipAtive o MLS novamente na interface do MLS-RP.

Para alterar o nome de domínio de VTP do MLS-SE, use este comando no prompt de ativação de CatOs do switch:

set vtp domain name <nome do domínio VTP>

Para que o MLS funcione, certifique-se de que o VTP esteja ativado no switch:

set vtp enable

As máscaras de fluxo concordam com MLS-RP e MLS-SE?

Uma máscara de fluxo é um filtro configurado por um administrador de rede que é usado pelo MLS para determinar se um atalho precisa ser criado. Assim como uma lista de acesso, quanto mais detalhado forem os critérios configurados, maior o nível de detalhamento a ser procurado no pacote pelo processo de MLS para verificar se o pacote atende a esses critérios. Para ajustar o escopo dos atalhos criados por MLS, a máscara de fluxo pode se tornar mais ou menos específica; a máscara de fluxo é essencialmente um dispositivo de sintonia. Há três tipos de modos IP MLS: destination-IP, destination-source-IP e full-flow-IP. O modo destination-IP, o padrão, é usado quando nenhuma lista de acesso é aplicada à interface ativada por MLS do roteador. O modo Source-destination-IP é usado quando uma lista de acesso padrão é aplicada. Full-flow-IP está, em vigor, em uma lista de acesso estendida. O modo MLS em MLS-RP é determinado implicitamente pelo tipo de lista de acesso aplicada à interface. Em contraste, o modo MLS no MLS-SE está configurado explicitamente. Se o modo apropriado for escolhido, o usuário pode configurar o MLS de modo que somente o endereço de destino corresponda para que um atalho de MLS seja criado, ou origem e destino, ou até mesmo informações de camada quatro, como números de porta TCP/UDP.

O modo MLS é configurável tanto no MLS-RP quanto no MLS-SE e, em geral, eles devem corresponder. SE os modos MLS source-destination-IP ou full-flow-IP forem considerados necessários, é melhor configurá-los no roteador e aplicar a lista de acesso apropriada. O MLS sempre escolhe a máscara mais específica. Ele dá à máscara de fluxo configurada na precedência de MLS-RP sobre a máscara encontrada no MLS-SE. TOME CUIDADO se alterar o modo MLS do switch do destination-ip padrão: certifique-se de que ele corresponda ao modo MLS no roteador para que o MLS funcione. Para os modos source-destination-ip e full-flow-ip, lembre-se de aplicar a lista de acesso à interface de roteador apropriada; sem nenhuma lista de acesso aplicada, mesmo se configurado, o modo MLS é simplesmente destination-ip, o padrão.

Aviso: sempre que a máscara de fluxo é alterada, seja no MLS-RP ou no MLS-SE, todos os fluxos MLS em cache são limpos e o processo MLS é reiniciado. Uma limpeza também pode ocorrer quando você aplica o comando **clear ip route-**cache no roteador. Se você aplicar o **comando de** configuração global do roteador **no ip routing**, que desativa o roteamento IP e transforma essencialmente o roteador em uma ponte transparente, ele causa uma limpeza e desativa o MLS (lembre-se de que o roteamento é um pré-requisito do MLS). Cada um deles pode afetar temporariamente, mas seriamente, o desempenho do roteador em uma rede de produção. O roteador enfrenta um pico em sua carga, até que os novos atalhos sejam criados porque agora ele deve lidar com todos os fluxos que foram processados anteriormente pelo switch.

Observação: especialmente com um membro da família Catalyst 5000 como o MLS-SE, você deve evitar o uso muito amplo de máscaras de fluxo configuradas com informações da camada quatro. Se o roteador for forçado a examinar profundamente todos os pacotes na

interface, muitos dos benefícios pretendidos do MLS serão ignorados. Isso é muito menos problemático quando você usa um membro da família Catalyst 6xxx como o MLS-SE, já que as próprias portas do switch podem reconhecer informações da camada quatro.

Observação: até recentemente, o MLS não oferecia suporte a máscaras de fluxo configuradas na entrada em uma interface MLS-RP, somente na saída. Se você **usar o comando mls rp ip input-**acl além dos comandos de configuração MLS-RP normais em uma interface de roteador, uma máscara de fluxo de entrada será suportada.

Há mais de duas mensagens de erro de *MLST* demais continuamente vistas no switch?

Conforme visto na observação, para alterar uma máscara de fluxo, limpar o cache de rota ou desativar o roteamento IP globalmente causa uma limpeza do cache. Outras circunstâncias também podem causar depurações completas ou muitas entradas únicas e fazer com que o MLS reclame *deExcesso de movimentações*. Há diversas formas desta mensagem, mas cada uma contém estas três palavras. Além do que já foi mencionado, a causa mais comum desse erro é quando o switch aprende vários endereços MAC (Media Access Control) Ethernet idênticos dentro da mesma VLAN; os padrões Ethernet não permitem endereços MAC idênticos dentro da mesma VLAN. Se visto com pouca frequência, ou apenas algumas vezes seguidas, não há motivo para preocupação; o MLS é um recurso robusto, e a mensagem pode ser simplesmente causada por eventos normais de rede, como uma conexão de PC movida entre portas, por exemplo. Se visto continuamente por vários minutos, provavelmente é um sintoma de um problema mais sério.

Quando essa situação surge, a causa principal é normalmente devido à presença de dois dispositivos com o mesmo endereço MAC realmente conectado a uma VLAN, ou um loop físico dentro da VLAN (ou várias VLANs, se houver pontes através desses domínios de transmissão). Solucione problemas com o spanning-tree (abordado em outros documentos) e a dica para localizar o loop e eliminá-lo. Além disso, qualquer alteração rápida na topologia pode causar instabilidade temporária da rede (e MLS) (interfaces do roteador não sincronizadas, uma placa de rede (NIC) defeituosa e assim por diante).

Dica: use os comandos **show mls notification e show looktableno switch para indicar a direção do endereço MAC duplicado ou loop físico.** A primeira fornece um valor TA. O comando **show looktable <TA value>**retorna um possível endereço MAC que pode ser rastreado até a raiz do problema.

Informações Relacionadas

Contents

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.