

# Pesquisando defeitos ambientes de LAN switching

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Convenções](#)

[Introdução à switching de LAN](#)

[Concentradores e Switches](#)

[Ligações e Switches](#)

[VLANs](#)

[Algoritmo de Transparent Bridging](#)

[Spanning Tree Protocol](#)

[Entroncamento](#)

[EtherChannel](#)

[Switching Multicamadas \(MLS\)](#)

[Como aprender sobre esses recursos](#)

[Sugestões gerais para o Troubleshooting de Switches.](#)

[Troubleshooting Problemas de Conectividade de Portas](#)

[Problemas de hardware](#)

[Problemas de configuração](#)

[Problemas de tráfego](#)

[Falha do Hardware do Switch](#)

[Troubleshooting de Auto-Negociação Semi-Duplex/Bidirecional de Ethernet 10/100Mb](#)

[Objetivos](#)

[Introdução](#)

[Troubleshooting de Auto-Negociação de Ethernet entre Dispositivos de Infra-estrutura de Rede](#)

[Procedimentos e/ou cenários](#)

[Exemplo de Configuração e Troubleshooting de Auto-Negociação de Ethernet 10/100Mb](#)

[Passo a passo](#)

[Antes que você chamar a equipe de Suporte técnico do Cisco Systems](#)

[Configurando conexões EtherChannel Switch a Switch nos Switches Catalyst 4000/5000/6000](#)

[Tarefas para a configuração manual do EtherChannel](#)

[Passo a passo](#)

[Verificar a configuração](#)

[Use o PAgP para configurar o EtherChannel \(o método preferido\)](#)

[Entroncamento e EtherChannel](#)

[Troubleshooting do EtherChannel](#)

[Comandos utilizados nesta seção](#)

[Usando Portfast e outros comandos para corrigir problemas de conectividade de inicialização de estação final.](#)

[Índice](#)

[Background](#)

[Como reduzir o atraso de inicialização no Switch Catalyst 4000/5000/6000](#)

[Testes de cronometragem com e sem DTP, PAgP e Portfast em um Catalyst 5000](#)

[Como reduzir o retardo na inicialização no Switch Catalyst 2900XL/3500XL](#)

[Testes de cronometragem no Catalyst 2900XL](#)

[Como reduzir o retardo na inicialização no Switch Catalyst 1900/2800](#)

[Testes de cronometragem no Catalyst 1900](#)

[Um benefício adicional ao Portfast](#)

[Os comandos usar-se para verificar a configuração trabalham](#)

[Comandos usar-se para pesquisar defeitos a configuração](#)

[Configurar e pesquise defeitos o Multi-Layer Switching \(MLS\) IP](#)

[Objetivos](#)

[Introdução](#)

[Troubleshooting com o IP MLS Technology](#)

[Comandos ou capturas de tela](#)

[Antes que você chamar a equipe de Suporte técnico do Cisco Systems](#)

[Informações Relacionadas](#)

## **Introdução**

As seções neste capítulo descreve os recursos comuns de switching de LAN e as soluções para alguns dos problemas mais comuns de switching de LAN. Estes artigos são cobertos:

- Introdução à switching de LAN
- Sugestões de Troubleshooting de problemas gerais de Switches
- Troubleshooting Problemas de Conectividade de Portas
- Troubleshooting de autonegociação half/full duplex da Ethernet 10/100Mb
- Entroncamento ISL em Catalyst 5000 e 6000 Family Switches
- Configurando e pesquisando defeitos o interruptor do EtherChannel para comutar
- Usando Portfast e outros comandos para corrigir problemas de conectividade de inicialização de estação final.
- Configurando e Troubleshooting de Switching Multicamada

## **Pré-requisitos**

### **Requisitos**

Não existem requisitos específicos para este documento.

### **Convenções**

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

## Introdução à switching de LAN

Se você é novo à Comutação LAN, estas seções tomam-no com alguns dos conceitos principais relativos ao Switches. Um dos pré-requisitos para o Troubleshooting de qualquer dispositivo é conhecer as regras de operação desse dispositivo. O Switches tornou-se muito mais complexo ao longo dos últimos anos porque ganhou na popularidade e na sofisticação. Estes parágrafos descrevem alguns dos conceitos chaves para saber sobre o Switches.

### Concentradores e Switches

Devido à grande demanda colocada em redes de área local, nós vimos uma SHIFT de uma rede da largura de banda compartilhada, com Hubs e cabo coaxial, a uma rede da largura de banda dedicada, com Switches. Um hub permite que vários dispositivos sejam conectados ao mesmo segmento de rede. Os dispositivos nesse segmento compartilham da largura de banda um com o outro. Se é um hub 10Mb, e há os dispositivos 6 conectados às portas 6 diferentes no hub, todos os seis dispositivos compartilham do 10Mb da largura de banda um com o outro. Um hub 100Mb compartilha de 100Mb da largura de banda entre os dispositivos conectados. Em termos do modelo OSI, um hub é considerado um dispositivo da camada-um (camada física). Ele ouve um sinal elétrico no fio e o passa para as outras portas.

Um interruptor pode fisicamente substituir um hub em sua rede. Um interruptor permite que os dispositivos múltiplos estejam conectados à mesma rede, apenas como um hub faz, mas este é o lugar onde a similaridade termina. Um interruptor permite que cada dispositivo conectado tenha a largura de banda dedicada em vez da largura de banda compartilhada. A largura de banda entre o interruptor e o dispositivo é reservada para uma comunicação a e desse dispositivo apenas. Seis dispositivos conectaram a seis portas diferentes em um 10Mb Switch que cada um tem 10Mb da largura de banda a trabalhar com, em vez da largura de banda compartilhada com os outros dispositivos. Um interruptor pode extremamente aumentar a largura de banda disponível em sua rede, que pode conduzir ao desempenho de rede aprimorado.

### Ligações e Switches

Um switch básico é considerado um dispositivo da camada-dois. Quando utilizamos a palavra camada, estamos nos referindo ao modelo OSI de 7 camadas. Um interruptor apenas não passa sinais bondes avante, como um hub faz; em lugar de, monta os sinais em um quadro (camada dois), e decide então o que fazer com o quadro. Um interruptor determina o que fazer com um quadro pedindo um algoritmo de um outro dispositivo de rede de comunicação comum: um Transparent Bridge. Logicamente, um interruptor atua apenas como um Transparent Bridge, mas pode segurar quadros muito mais rapidamente do que um Transparent Bridge poderia (devido ao hardware especial e à arquitetura). Uma vez que um interruptor decide onde o quadro deve ser enviado, passa ao quadro para fora a porta apropriada (ou portas). Você pode pensar de um interruptor como um dispositivo que cria conexões instantâneas entre várias portas, em um quadro pela base do quadro.

### VLANs

Desde que o interruptor decide em um quadro pela base do quadro que move dados de intercâmbio, é uma extensão natural para pôr a lógica dentro do interruptor para permitir que escolha portas para disposições especiais. Este agrupamento de portas é chamado de Rede de área local virtual (VLAN). O interruptor certifica-se de que o tráfego de um grupo de portas nunca obtém enviado a outros grupos de portas (que estariam distribuindo). Estes grupos de porta

(VLAN) podem cada um ser considerados um segmento de LAN individual.

Os VLAN são descritos igualmente como domínios de transmissão. Isto é devido ao algoritmo de Transparent Bridging, que diz que os pacotes de transmissão (pacotes destinados para *todo o endereço de dispositivos*) estejam mandados todas as portas que estão no mesmo grupo (isto é, no mesmo VLAN). Todas as portas que estão no mesmo VLAN estão igualmente no mesmo domínio de transmissão.

## Algoritmo de Transparent Bridging

O algoritmo de Transparent Bridging e medida - a árvore é coberta com maiores detalhes em outra parte (capítulo 20: Pesquisando defeitos ambientes de Transparent Bridging). Quando um interruptor recebe um quadro, deve decidir o que fazer com esse quadro. Poderia ignorar o quadro; poderia passar ao quadro para fora outra uma porta, ou poderia passar ao quadro para fora muitas outras portas.

A fim conhecer o que fazer com o quadro, o interruptor aprende o lugar de todos os dispositivos no segmento. Esta informação de localização é colocada em uma tabela do Content Addressable Memory (CAM - nomeado para o tipo de memória usado para armazenar estas tabelas). A tabela CAM mostra, para cada dispositivo, o MAC address do dispositivo, para fora que porta que o MAC address pode ser encontrado, e com que porta VLAN esta é associado. O interruptor faz continuamente este processo de aprendizagem enquanto os quadros são recebidos no interruptor. A tabela CAM do interruptor é atualizada continuamente.

Esta informação na tabela CAM é usada para decidir como um frame recebido é segurado. A fim decidir onde enviar um quadro, os olhares do interruptor no endereço MAC de destino em um frame recebido e olham acima esse endereço MAC de destino na tabela CAM. As mostras da tabela CAM que movem o quadro devem ser mandadas para que esse quadro alcance o MAC address do destino especificado. Estão aqui as regras básicas que um interruptor se usa para realizar a responsabilidade do encaminhamento de frame:

- Se o endereço MAC de destino é encontrado na tabela CAM, o interruptor envia ao quadro para fora a porta que é associada com esse endereço MAC de destino na tabela CAM. Isso se chama encaminhamento.
- Se a porta associada para enviar o quadro para fora é a mesma porta que o quadro entrou originalmente sobre, não há nenhuma necessidade de enviar para trás o quadro para fora que a mesma porta, e o quadro é ignorada. Isso é chamado de filtragem.
- Se o endereço MAC de destino não está na tabela CAM (o endereço é *desconhecido*), o interruptor envia ao quadro para fora todas portas restantes que estão no mesmo VLAN que o frame recebido. Isso é chamado de inundação. Não inunda o quadro para fora a mesma porta em que o quadro foi recebido.
- Se o endereço MAC de destino do frame recebido é o endereço de broadcast (FFFF.FFFF.FFFF), o quadro está mandado todas as portas que estão no mesmo VLAN que o frame recebido. Isto é chamado igualmente inundação. O quadro não é mandado a mesma porta em que o quadro foi recebido.

## Spanning Tree Protocol

Como pudemos verificar, o algoritmo de Transparent Bridging inunda quadros desconhecidos e de transmissão a partir 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 este algoritmo são conectados junto em um laço físico, os quadros inundados (como transmissões) estão passando do interruptor para comutar, em torno e em torno do laço, para sempre. O dependente em cima das conexões físicas envolvidas, os quadros podem realmente multiplicar exponencialmente devido ao algoritmo de inundação, que pode causar problemas de rede graves.

Há um benefício a um laço físico em sua rede: pode fornecer a Redundância. Se um link falhar, ainda haverá outra maneira de o tráfego poder atingir seu destino. A fim de permitir os benefícios derivados da Redundância, sem quebrar a rede devido à inundação, um protocolo chamado *medida - a árvore* foi criada. A abrangência de *árvore* foi padronizada na especificação IEEE 802.1d.

A finalidade do Spanning Tree Protocol (STP) é identificar e obstruir temporariamente os laços em um segmento de rede ou em um VLAN. O Switches executa o STP, que envolve eleger um *bridge-raiz* ou um interruptor. O outro Switches mede sua distância do *switch-raiz*. Se há mais de uma maneira de obter ao *switch-raiz*, há um laço. O Switches segue o algoritmo para determinar que portas devem ser obstruídas a fim de quebrar o laço. O STP é dinâmico; se um link no segmento falha, as portas que estavam obstruindo originalmente podem possivelmente ser mudadas ao modo de encaminhamento.

## Entroncamento

O entroncamento é um mecanismo que seja o mais usado frequentemente para permitir que os VLANs múltiplos funcionem independentemente através dos switches múltiplos. Os roteadores e os servidores podem usar o entroncamento, também, que permite que viva simultaneamente em VLANs múltiplos. Se sua rede tem somente um VLAN nela, você pode nunca precisar do entroncamento; mas se sua rede tem mais de um VLAN, você quer provavelmente aproveitar-se dos benefícios do entroncamento.

Uma porta em um interruptor pertence normalmente a somente um VLAN; todo o tráfego recebido ou enviado sobre esta porta é suposto para pertencer ao VLAN configurado. Uma porta de tronco, por outro lado, é uma porta que pode ser configurada para enviar e receber tráfego para muitas VLANs. Realiza esta quando anexa a informação de VLAN a cada quadro, um processo chamado *etiquetar o quadro*. Também, o entroncamento deve ser ativo em ambos os lados do link; o outro lado deve esperar os quadros que incluem a informação de VLAN para que uma comunicação apropriada ocorra.

Há uns métodos diferentes do dependente do entroncamento em cima do *media* que é usado. Os métodos de truncamento de Fast Ethernet ou de Gigabit Ethernet são ISL (Link InterSwitch) ou 802.1q. O truncamento via ATM usa LANE. Entroncamento sobre os usos 802.10 FDDI.

## EtherChannel

O EtherChannel é uma técnica que seja usada quando você tem conexões múltiplas ao mesmo dispositivo. Um pouco do que cada função do link independentemente, grupos de EtherChannel as portas junto a trabalhar como uma unidade. Distribui o tráfego através de todos os links e fornece a Redundância se uns ou vários links falham. As configurações do EtherChannel devem ser iguais em ambos os lados dos enlaces envolvidos no canal. Normalmente, *medindo - a árvore* obstruiria todas estas conexões paralelas entre dispositivos porque são laços, mas o EtherChannel é executado *debaixo da medida - a árvore*, de modo que *medindo - a árvore* pensa que todas as portas dentro de um EtherChannel dado são somente uma porta única.

## Switching Multicamadas (MLS)

O switching multicamada (MLS) é a capacidade de um interruptor para enviar os quadros baseados na informação na camada três e às vezes no encabeçamento da camada-quatro. Isto geralmente aplica-se aos pacotes IP mas agora igualmente pode-se ocorrer para pacotes IPX. O interruptor aprende como segurar estes pacotes quando se comunica com os ou mais roteadores. Com uma explicação simplificada, os relógios do interruptor como os processos de roteador um pacote, e então o interruptor processam pacotes futuros neste mesmo fluxo. Tradicionalmente, o Switches foi muito mais rápido em quadros de interruptor do que o Roteadores, assim que mandá-lo offload o tráfego do roteador pode conduzir às melhorias significativas da velocidade. Se algo muda na rede, o roteador pode dizer o interruptor para apagar seu esconderijo da camada três e para construí-lo a partir do zero outra vez enquanto 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

Estes são apenas alguns dos recursos básicos que o Switches apoia. Mais são adicionadas cada dia. São importante compreender como seu Switches funciona, que o caracteriza uso, e como aquelas características deve trabalhar. Um dos melhores lugares para aprender esta informação sobre switch Cisco está na site da Cisco na Web. Vá e sob ao *serviço & ao apoio da seção*, escolhem *documentos técnico*. De aqui, escolha o *Home Page da documentação*. Os grupos da documentação para todo o Produtos da Cisco podem ser encontrados aqui. *Os switch LAN da Multi-camada* ligam ligações você à documentação para todos os Cisco LAN Switch. A fim aprender sobre as características de um interruptor, leia o *manual de configuração do software* para a versão particular de software que você usa. Os manuais de configuração do software dão-lhe a informações de fundo sobre o que a característica faz e que comandos se usar para o configurar em seu interruptor. Todas essas informações estão disponibilizadas gratuitamente na Web. Você precisa nem sequer esclarecer esta documentação; está disponível a qualquer um. Alguns destes manuais de configuração podem ser lidos dentro uma tarde e são valor que bom o tempo gastou.

Outro a site da Cisco na Web é povoado parte de pelo site do apoio e da documentação de Cisco. É enchido com a informação projetada ajudá-lo a executar, manter, e pesquisar defeitos sua rede. Vá ao site do [apoio e da documentação](#) obter informação da sustentação detalhada pelo Produtos ou por Tecnologias específicas.

## Sugestões gerais para o Troubleshooting de Switches.

Há muitas maneiras de pesquisar defeitos um interruptor. Enquanto as características do Switches crescem, as coisas possíveis que podem quebrar igualmente aumentam. Se você desenvolve uma aproximação ou um plano de teste para pesquisar defeitos, você é mais em melhor situação a longo prazo do que se você apenas tenta uma aproximação da batida-e-falta. Estão aqui algumas sugestões gerais para fazer sua pesquisa de defeitos de mais eficaz:

- Tome o momento de tornar-se familiar com a operação normal de switch. A site da Cisco na Web tem um valor enorme da informação técnica que descreve como seu Switches funciona, como mencionado na seção anterior. Os manuais de configuração são particularmente muito úteis. Muitos casos são abertos que são resolvidos com informação dos guias de configuração de produto.



- Para mais situações complexas, tenha um físico preciso e um mapa lógico de sua rede. Um mapa físico mostra como os dispositivos e os cabos são conectados. Um mapa lógico mostra que segmentos (VLAN) exista em sua rede e que Roteadores proporciona serviços de roteamento a estes segmentos. Uma medida - o mapa da árvore é altamente útil pesquisar defeitos problemas complexos. Devido à capacidade de um interruptor para criar segmentos diferentes com a aplicação dos VLAN, as conexões física apenas não dizem a história inteira; um tem que saber o Switches é configurado para determinar que segmentos (VLAN) exista e para saber são conectados logicamente.
- Tenha um plano. Alguns problemas e soluções são óbvios; alguns não são. Os sintomas que você vê em sua rede podem ser o resultado dos problemas em uma outra área ou camada. Antes que você salte às conclusões, tente verificar em uma maneira estruturada o que trabalham e o que não faz. Desde que as redes podem ser complexas, é útil isolar domínios do problema possível. Uma maneira de fazer isto é usar o modelo da sete-camada OSI. Por exemplo: verifique as conexões física envolvidas (camada 1); verifique problemas de conectividade dentro do VLAN (camada 2), e verifique problemas de conectividade através de VLAN diferentes (camada 3), etc. Se há uma configuração correta no interruptor, muitos dos problemas que você encontra estão relacionados às questões de camada física (portas física e expedição de cabogramas). Hoje, o Switches é envolvido na camada três e nas quatro edições, que a inteligência incorporada comutar os pacotes baseados na informação derivada do Roteadores, ou tem realmente o Roteadores que vive dentro do interruptor (camada três ou interruptor da camada-quatro).
- Não supõe trabalhos de um componente sem verificá-la primeiramente. Isso pode economizar um longo período de tempo. Por exemplo, se um PC não pode entrar a um server através de sua rede, há muitas coisas que podem ser erradas. Não salte as coisas básicas e supõe que algo trabalha; alguém pode ter mudado algo e não o ter dito. Toma somente um minuto para verificar algumas das coisas básicas (por exemplo, aquele as portas envolvidas é conectado ao local correto e é ativo), que poderiam o salvar muitas horas desperdiçadas.

## Troubleshooting Problemas de Conectividade de Portas

Se a porta não trabalha, nada trabalha! As portas são a base da sua rede de switching. Algumas portas têm o significado especial devido a seu lugar na rede e na quantidade de tráfego que levam. Estas portas incluem conexões a outros Switches, Roteadores, e server. Os problemas nessas portas podem ser mais complicados de resolver, pois elas sempre utilizam recursos especiais, como truncamento e EtherChannel. O resto das portas é significativo, também, porque conectam os usuários reais da rede.

Muitas coisas podem fazer com que uma porta seja NON-funcional: problemas de hardware, problemas de configuração, e edições do tráfego. Estas categorias são um pouco de mais profundas explorado.

### Problemas de hardware

#### **Geral**

A funcionalidade de porta exige duas portas em funcionamento conectadas por um cabo em funcionamento (do tipo correto). O padrão da maioria de switch Cisco é ter uma porta no *notconnectstate*, assim que significa que não está conectado atualmente a qualquer coisa mas

quer conectar. Se você conecta um bom cabo a duas portas de switch no *estado não conectado*, a luz de enlace torna-se verde para ambas as portas, e o status de porta diz *conectado*, que significa que a porta está acima tanto quanto a camada uma. Estes parágrafos indicam os artigos para que verifiquem se a camada uma não está acima.

Verifique o status das duas portas envolvidas. Assegure-se de que nenhuma porta envolvida no enlace esteja fechada. O administrador possivelmente pode ter fechado uma ou ambas as portas. O software dentro do interruptor pode ter fechado a porta para baixo devido às condições de erro de configuração (nós expandiremos neste mais tarde). Se um lado é parada programada e o outro não é, o estado no lado ativado é *não-conectado* (porque não detecta um vizinho no outro lado do fio). O estado no lado de fechamento diz algo como o *desabilitação* ou o *errdisable* (dependente do que fechou realmente a porta para baixo). O link não vem acima a menos que ambas as portas forem permitidas.

Quando você engancha acima de um bom cabo (outra vez, se é do tipo correto) entre duas portas habilitadas mostram uma luz de enlace verde dentro de alguns segundos. Também, as mostras do estado de porta *conectadas no* comando line interface(cli). Neste momento, se você não tem o link, seu problema é limitado a três coisas: a porta em um lado, a porta no outro lado, ou o cabo no meio. Em alguns casos, há os outros dispositivos envolvidos: os conversores de mídia (fibra a revestir, etc.), ou em enlaces de gigabit você pode ter os conectores de interface do gigabit (GBIC). Ainda, esta é razoavelmente uma área limitada a procurar.

Os conversores de mídia podem adicionar o ruído a uma conexão ou enfraquecer o sinal se não funcionam corretamente. Igualmente adicionam os conectores extra que podem causar problemas e são um outro componente a debugar.

Verifique se existem conexões soltas. Às vezes um cabo parece ser assentado no jaque, mas não é realmente; desconecte o cabo e reintroduza-o. Você deve igualmente procurar a sujeira ou os pinos quebrados ou de faltas. Faça isso para as duas portas envolvidas na conexão.

O cabo pode ser obstruído dentro à porta errada, que acontece geralmente. Certifique-se que o ambas as extremidades do cabo está obstruído dentro às portas onde você as quer realmente.

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

Uma luz de link não garante que o cabo esteja funcionando adequadamente. Pode ter encontrado o esforço físico que faz com que seja funcional a nível marginal. Geralmente você observa este pela porta que tem lotes dos erros de pacote.

A fim determinar se o cabo é o problema, troque-o com um bom cabo conhecido. Apenas não o troque com nenhum outro cabo; certifique-se de que você o troca com um cabo que você conhece seja bom e seja do tipo correto.

Se este é um funcionamento do cabo muito longo (subterrâneo, através de um grande terreno, por exemplo), é agradável ter um testador de cabo sofisticado. Se você não tem um testador de cabo, você pode considerar estes:

- Tente portas diferentes ver se vêm acima com este cabo longo.
- Conecte a porta na pergunta a uma outra porta no mesmo interruptor apenas para ver se os links da porta acima localmente.
- Relocate temporariamente o Switches perto de se, assim que você pode tentar um bom cabo



conhecido.

## **Cobre**

Certifique-se de que você tem o cabo correto para o tipo de conexão que você faz. O cabo da categoria 3 pode ser usado para as conexões UTP 10MB, mas a categoria 5 deve ser usada para 10/100 das conexões.

A reto-através do cabo RJ-45 é usado para que estações finais, Roteadores, ou os server conectem a um interruptor ou a um hub. Um cabo de cruzamento de Ethernet é usado para o interruptor para comutar ou o hub às conexões de switch. Este é o pino-para fora para um cabo de cruzamento de Ethernet. As distâncias máximas para os fios de cobre Ethernet ou Fast Ethernet são de 100 metros. Um bom princípio básico geral é aquele quando você cruza uma camada de OSI, como entre um interruptor e um roteador, usa um cabo straight-through; quando você conecta dois dispositivos na mesma camada de OSI, como entre dois Roteadores ou dois Switches, use uma cruz sobre o cabo. Somente para a finalidade desta regra, trate uma estação de trabalho como se fosse um roteador.

Estes dois gráficos mostram as pino-saídas exigidas para um cabo crossover de switch a switch.

## **Fibra**

Para a fibra, certifique-se de que você tem o cabo correto para as distâncias envolvidas e o tipo de portas de fibra que é usado (modo simples, multi-modo). Certifique-se que as portas que são conectadas junto são o modo simples ou ambas as portas de multimodo. A fibra de modo único alcança geralmente os quilômetros 10, e a fibra multimodo pode geralmente alcançar 2 quilômetros, mas há o exemplo especial de multimodo 100BaseFX usado no modo semi-duplex, que pode somente ir 400 metros.

Para conexões de fibra ótica, certifique-se que a ligação transmitir de uma porta está conectada à ligação da recepção da outra porta, e vice-versa; transmita para transmitir, receba para receber, não trabalhe.

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

Um SX GBIC precisa de conectar com um SX GBIC; um SX GBIC não liga com um LX GBIC. Também, algumas conexões de gigabit exigem os cabos de condição dependentes dos comprimentos envolvidos. Refira as notas de instalação GBIC.

Se seu enlace de gigabit não vem acima, a verificação para certificar-se dos ajustes do controle de fluxo e da negociação de porta é consistente em ambos os lados do link. Pode haver umas incompatibilidades na aplicação destas características se o Switches que está conectado é dos vendedores diferentes. Em caso de dúvida, gire estas características fora em ambo o Switches.

## **Problemas de configuração**

Uma outra causa de edições da conectividade de porta é configuração de software incorreto do interruptor. Se uma porta tem uma luz alaranjada sólida, essa significa que esse software dentro do interruptor fechou a porta, pela interface do utilizador ou por processos internos.

Certifique-se de que o administrador não fechou as portas envolvidas (como mencionado). O administrador pode manualmente ter fechado a porta em um lado do link ou no outro. Este link não vem acima até que você re-permita a porta; verifique o status de porta.

Alguns Switches, tal como o Catalyst 4000/5000/6000, pode fechar a porta se os processos de software dentro do interruptor detectam um erro. Quando você olha o status de porta, lê o *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*. Estes são algumas das causas para este estado *errdisable*:

- **Configuração de EtherChannel incorreta:** Se um lado está configurado para o EtherChannel e o outro não é, pode causar a medida - processo da árvore para fechar a porta no lado configurado para o EtherChannel. Se você tenta configurar o EtherChannel mas as portas envolvidas não têm os mesmos ajustes (velocidade, duplex, modo de entroncamento, etc.) como suas portas vizinha através do link, poderia causar o estado *errdisable*. É o melhor ajustar cada lado para o *modo desejável* do EtherChannel se você quer usar o EtherChannel. As seções falam mais tarde detalhado sobre como configurar o EtherChannel.
- **Incompatibilidade duplex (bidirecional):** Se a porta de switch recebe um lote dos colisões atrasada, esta indica geralmente um problema de incompatibilidade bidirecional. Há umas outras causas para colisões atrasada: um NIC ruim, os segmentos de cabo que são demasiado longos, mas a maioria de motivo comum é hoje uma incompatibilidade duplex (bidirecional). O lado bidirecional pensa que pode enviar sempre que quer a. O lado semi-duplex espera somente pacotes por vezes - não em "toda a" hora.
- **Guarda-porto BPDU:** Algumas versões de software de switch mais novas podem monitorar se o portfast é permitido em uma porta. Uma porta que use o portfast deve ser conectada a uma estação final, não aos dispositivos que gerenciem os pacotes de Spanning Tree chamados BPDU. Se o interruptor observa um BPDU que venha em uma porta que tenha o portfast permitido, põe a porta no modo *errdisable*.
- **UDLD:** Detecção de enlace unidirecional é um protocolo usado em algumas versões novas de software que descobre se a comunicação em um enlace é realizada em apenas um sentido único. Um cabo de fibra quebrado ou outros problemas de porta/cabeamento podem ocasionar essa comunicação apenas em sentido único. Estes links parcialmente funcionais podem causar problemas quando o Switches envolvido não sabe que o link é parcialmente quebrado. Podem ocorrer circuitos de árvore de abrangência com esse problema. O UDLD pode ser configurado para pôr uma porta no estado *errdisable* quando detecta um enlace unidirecional.
- **Incompatibilidade da VLAN nativa** Antes de a porta ter um truncamento ativado, ela pertence a um único VLAN. Se o truncamento estiver ativado, a porta poderá suportar tráfego para vários VLANs. A porta ainda recordou que o VLAN ele estava dentro antes que o entroncamento esteve girado sobre, que é chamado o VLAN nativo. A VLAN nativa é central para o truncamento 802.1q Se o VLAN nativo em cada extremidade do link não combina, uma porta entra no estado *errdisable*.
- **Outro:** Todo o processo dentro do interruptor que reconhece 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 interruptor pertence a um VLAN. Se esse VLAN é suprimido, a porta torna-se inativa. Alguns Switches mostra uma luz alaranjada constante em cada porta onde este aconteceu. Se você

entra trabalhar um dia e ver centenas de luzes alaranjadas, não se apavore; poder-se-ia ser que todas as portas pertenceram ao mesmo VLAN e alguém suprimiu acidentalmente do VLAN que as portas pertenceram a. Quando você adiciona o VLAN de novo na tabela de vlan, as portas tornam-se ativas outra vez. Uma porta recorda seu vlan designada.

Se você tiver um link e as portas parecerem conectadas, mas não for possível estabelecer comunicações com outro dispositivo, isso pode ser particularmente complicado. Em geral, indica um problema acima da cama física: tentativa da camada 2 ou da camada 3. estas coisas.

- Verifique o modo de entroncamento em cada lado do enlace. Certifique-se que os ambos os lados reagem do mesmo modo. Se você gerencie o modo de entroncamento para "ON" (ao contrário do "automóvel" ou do "desirable") para uma porta, e a outra porta tem o modo de entroncamento ajustado a "OFF", não podem comunicar-se. O entroncamento muda o formato do pacote; as portas precisam de estar no acordo a respeito de que formato usam no link ou não se compreendem.
- Verifique se todos os dispositivos estão na mesma VLAN. Se não estão no mesmo VLAN, um roteador deve ser configurado para permitir que os dispositivos comuniquem-se.
- Certifique-se de que o endereçamento de camada três esteja corretamente configurado.

## Problemas de tráfego

Nesta seção, nós descrevemos algumas das coisas que você pode aprender quando você olha essa informação de tráfego de uma porta. A maioria de Switches tem alguma maneira de seguir os pacotes que vão dentro e fora de uma porta. Os comandos que gerenciem este tipo de saída no Switches do Catalyst 4000/5000/6000 são **show port** e **mostram o Mac**. A saída destes comandos no Switches de 4000/5000/6000 é descrita nas referências do comando switch.

Alguns destes campos de tráfego da porta mostram quanto dados são transmitidos e recebidos na porta. Outros campos mostram quantos frames de erro são encontrados na porta. Se você tem uma grande quantidade de erros de alinhamento, de erros de FCS, ou de colisões atrasada, este pode indicar uma incompatibilidade duplex (bidirecional) no fio. As outras causas para estes tipos de erros podem ser placas de interface de rede ruim ou problemas de cabo. Se você tem um grande número frames diferidos, é um sinal que seu segmento tem demasiado tráfego; o interruptor não pode enviar bastante tráfego no fio para esvaziar seus buffers. Considere a remoção de alguns dispositivos a um outro segmento.

## Falha do Hardware do Switch

Se você tentou tudo que você pode pensar de e a porta não trabalha, lá pôde ser hardware defeituoso.

As portas são danificadas às vezes pelo Eletro-Static Discharge (ESD). Você pode ou não pode ver nenhuma indicação deste.

Olhe os resultados do auto-teste de energia (CARGO) do interruptor para ver se havia alguma falha indicada para parte do interruptor.

Se você vê o comportamento que pode somente ser considerado "estranho," este poderia indicar problemas de hardware, mas poderia igualmente indicar problemas de software. Normalmente, é mais fácil recarregar o software do que obter um novo hardware. Tente trabalhar primeiramente com o software de switch.

O sistema operacional pode ter um bug. Se você carrega um sistema operacional mais novo, poderia fixar este. Você pode pesquisar Bug conhecido se você lê os Release Note para a versão de código que você usa ou usa o [conjunto de ferramentas do Bug da Cisco](#).

O sistema operacional poderia de algum modo ter-se tornado corrompido. Se você recarrega a mesma versão do sistema operacional, você poderia fixar o problema.

Se a luz de status no interruptor pisca alaranjada, esta significa geralmente que há algum tipo do problema de hardware com a porta ou o módulo ou o interruptor. A mesma coisa é verdadeira se a porta ou o status de módulo indicam *defeituoso*.

Antes que você troque o hardware do interruptor, você pode tentar algumas coisas:

- Assente o módulo no interruptor. Se você fizer isso com o equipamento ligado, verifique se o módulo pode trocado ou removido em operação. Em caso de dúvida, desligue o interruptor antes que você assente o módulo ou refira o guia de instalação de hardware. Se a porta é construída dentro ao interruptor, ignore esta etapa.
- Recarregue o interruptor. Às vezes isto faz com que o problema desapareça; esta é uma ação alternativa, não um reparo.
- Verifique o software de switch. Se esta é uma instalação nova, recorde que alguns componentes podem somente trabalhar com determinadas liberações do software. Verifique os Release Note ou a instalação de hardware e o manual de configuração para ver se há o componente que você instala.
- Se você está razoavelmente certo que você tem um problema de hardware, substitua o componente defeituoso.

## [Troubleshooting de Auto-Negociação Semi-Duplex/Bidirecional de Ethernet 10/100Mb](#)

### [Objetivos](#)

Esta seção apresenta a informação do Troubleshooting geral e uma discussão de técnicas para pesquisar defeitos a autonegociação dos Ethernet.

- Esta seção mostra como determinar o comportamento atual de um enlace. Vai sobre mostrar como os usuários podem controlar o comportamento, assim como explica situações quando a autonegociação falha.
- Muitos Cisco Catalyst Switches e muitos Cisco Routers suporte negociação automática. Esta seção centra-se sobre a autonegociação entre Catalyst 5000 Switch. Os conceitos explicados aqui podem igualmente ser aplicados aos outros tipos de dispositivos.

### [Introdução](#)

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 têm uma porta Ethernet conectada permanentemente à rede do escritório. Porque não é possível se assegurar de que cada usuário tenha um 10Mb, um Ethernet 100Mb, ou um cartão 10/100Mb em seu portátil, as portas de switch que seguram estas conexões devem poder negociar seu modo da velocidade e duplexação. A alternativa pode fornecer um 10Mb e uma porta 100Mb em cada escritório ou cubá-los em conformidade e etiquetar.

A autonegociação não deve ser usada para as portas que apoiam dispositivos da infraestrutura de rede, tais como o Switches e o Roteadores ou outros sistemas finais NON-transientes tais como server e impressoras. Embora a autonegociação para a velocidade e duplexação seja normalmente o comportamento padrão nas portas de switch que são capazes dele, as portas conectadas aos dispositivos fixos devem sempre ser configuradas para o comportamento correto um pouco do que reservadas negociá-lo. Isto elimina todas as edições potenciais da negociação e assegura-se de que você saiba sempre exatamente as portas devem se operar. Por exemplo, um enlace de switch a switch dos Ethernet 10/100BaseTX que seja configurado para o Full-duplex 100Mb opera-se somente nessas velocidade e modo. Não há nenhuma possibilidade para que as portas degradem o link a uma velocidade mais lenta dentro de uma restauração da porta ou de uma restauração do interruptor. Caso as portas não puderem se operar como configurado, não devem passar nenhum tráfego. Por outro lado, um enlace de switch a switch que seja permitido negociar seu comportamento pode operar-se na metade 10Mb - duplex. Um link NON-funcional é geralmente mais fácil de descobrir do que um link, que seja operacional, mas não se opera na velocidade ou no modo previsto.

Uma da maioria de causas comum dos problemas de desempenho nas ligações de Ethernet 10/100Mb é quando uma porta no link se opera na metade - duplex, quando a outra porta se operar em completamente - duplex. Isto acontece ocasionalmente quando uma ou ambas a porta em um link é restaurada e o processo de auto-negociação não conduz a ambos os parceiros de enlace que têm a mesma configuração. Isso também ocorre quando usuários reconfiguram um lado de um enlace e esquecem de configurar o outro. Muitas chamadas de suporte relacionadas com desempenho estão evitadas se você cria uma política que exija portas para que todos os dispositivos NON-transientes estejam configurados para seu comportamento exigido e reforça a política com medidas de controle de alterações adequadas.

## [Troubleshooting de Auto-Negociação de Ethernet entre Dispositivos de Infra-estrutura de Rede](#)

### [Procedimentos e/ou cenários](#)

Cat 5k da encenação 1. com Fast Ethernet

**Tabela 22-2: Problemas de conectividade de autonegociação**

Possível problema	Solução
O comportamento atual do	1. Use o comando <code>show port mod_num/port_num</code> para determinar o comportamento atual do link. Se ambos os parceiros de enlace (relações em uma ou outra

automóvel do link foi negociado?	extremidade do link) indicam tenha um prefixo "a" em seu duplex e os campos de estado da velocidade, autonegociação eram provavelmente bem sucedidos.
Auto negociação não apoiada.	2. Emita o comando do <b>mod_num/port_num das capacidades do show port</b> verificar que seus módulos apoiam a auto negociação.
A auto negociação não trabalha em Catalyst Switches.	3. Use o <b>comando auto do mod_num/port_num da velocidade do set port em um</b> catalizador configurar a auto negociação. 4. Tente portas ou os módulos diferentes. 5. Tente restaurar as portas. 6. Tente cabos de correção diferentes. 7. Desligue os dispositivos e para trás sobre outra vez.
A auto negociação não trabalha em roteadores Cisco.	8. Emita o comando ios correto permitir a auto negociação (se disponível) 9. relações diferentes da tentativa. 10. Tente restaurar as relações. 11. Tente cabos de correção diferentes. 12. Desligue os dispositivos e para trás sobre outra vez.

## [Exemplo de Configuração e Troubleshooting de Auto-Negociação de Ethernet 10/100Mb](#)

Esta seção do documento anda você com do exame do comportamento de uma porta Ethernet 10/100Mb que apoie a autonegociação. Igualmente mostra como fazer mudanças a seu comportamento padrão e como restaurá-lo ao comportamento padrão.

### Tarefas que são executadas

1. Analisar as capacidades das portas.
2. Configurar a auto negociação para a porta 1/1 em ambo o Switches.
3. Determine se a velocidade e o modo duplex estão definidos para negociação automática.
4. Mude a velocidade na porta 1/1 no Switch à 10Mb.
5. Entendendo o significado do prefixo "a-" nos campos de status de duplex e velocidade.
6. Visualize o status duplex da porta 1/1 no Switch B.
7. Compreenda o erro de incompatibilidade bidirecional.
8. Compreenda as mensagens de erro de spanning tree.
9. Mude o modo duplex para half na porta 1/1 no interruptor A.
10. Ajuste o modo duplex e a velocidade da porta 1/1 no switch B.
11. Restaure o modo duplex padrão e a velocidade às **portas 1/1 em** ambos os interruptores.
12. Veja as mudanças do status de porta em ambos os interruptores.

### [Passo a passo](#)

Execute estas etapas:

1. O comando `show port capabilities 1/1` exibe as capacidades de uma porta Ethernet 10/100BaseTX 1/1 em um Switch A. Incorpore este comando para ambas as portas que você pesquisa defeitos. Ambas as portas devem apoiar as capacidades da velocidade e duplexação mostradas se são supostas para usar a auto negociação. Switch-A> (enable) show

```
port capabilities 1/1
Model WS-X5530
Port 1/1
Type 10/100BaseTX
Speed auto,10,100
Duplex half,full
```

2. A auto negociação está configurada para ambos modo da velocidade e duplexação na porta 1/1 de ambo o Switches se você inscreve o **comando set port speed 1/1 auto** (o automóvel é o padrão para as portas que apoiam a autonegociação). Switch-A> (enable) set port speed

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

**Nota:** 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.

3. O comando `show port 1/1` indica o estado das portas 1/1 em comuta 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. Consequentemente pode negociar automaticamente seus modo duplex e velocidade se o dispositivo que está conectada a (seu parceiro de enlace) igualmente pode negociar automaticamente seus modo duplex e 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.

4. A fim demonstrar o que acontece quando um parceiro de enlace está negociando automaticamente e o outro parceiro de enlace não é, a velocidade na porta 1/1 no Switch A é ajustada a 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)
```

**Nota:** Se você código duro a velocidade em uma porta, ele desabilita toda a funcionalidade de auto-negociação na porta para a velocidade e duplexação. Quando uma porta foi configurada para uma velocidade, seu modo duplex está configurado automaticamente para o modo que tinha negociado previamente; neste caso, completamente - duplex. Quando você entra o **comando set port speed 1/1 10** fez com que o modo duplex na porta 1/1 estivesse configurado como se o comando `set port duplex 1/1 full` tinha sido inscrito igualmente. Isto é explicado em seguida.



5. Compreenda o significado do prefixo "a" no duplex e apresse campos de estado. A ausência do "a" prefixo no campos do estado da saída do **comando show port 1/1** no Switch A mostra que o modo duplex está configurado agora para "completamente," e a velocidade é configurada agora 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
```

6. O comando **show port 1/1** no switch B indica que a porta se opera agora na metade - 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 bonde que está chegando para considerar se é 10Mb ou 100Mb faz esta. Isto é como o switch B determinou que a porta 1/1 deve se operar em 10Mb. Não é possível detectar o modo de bidirecional correto da mesma forma que a velocidade correta pode ser detectada. Neste caso, onde a porta de 1/1 do switch B é configurada para a autonegociação e a porta do Switch A não é, a porta de 1/1 do switch B foi forçada para selecionar o modo frente e verso 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 é configurada para full duplex, enquanto a porta 1/1 no Switch B padronizou para half duplex. A fim evitar isto, configurar sempre ambos os parceiros de enlace. 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", o que indica que a porta está operando a 10Mb em modo semi-duplex. Neste exemplo, o parceiro de enlace nesta porta (a porta 1/1 no interruptor A) é configurada para "completamente" e "10Mb." não era possível para a porta 1/1 no switch B ter negociado automaticamente seu comportamento atual. Isto mostra que o prefixo "a" indica somente uma vontade de executar a autonegociação - não essa autonegociação ocorreu realmente.

7. Compreenda a mensagem de erro de incompatibilidade bidirecional. Esta mensagem sobre uma má combinação do modo duplex é indicada no Switch A depois que a velocidade na porta 1/1 foi mudada a 10Mb. A má combinação foi causada pela porta de 1/1 do switch B, que optam a metade - o duplex porque detectou seu parceiro de enlace poderia já não executar a autonegociação. `%CDP-4-DUPLEXMISMATCH:Full/half duplex mismatch detected on` É importante observar que esta mensagem é criada pelo Protocolo de descoberta Cisco (CDP), e não pelo protocolo de autonegociação 802.3. O CDP pode relatar problemas que descobre, mas tipicamente não os fixa automaticamente. Uma incompatibilidade duplex (bidirecional) pode ou não pode conduzir a um Mensagem de Erro. Outra indicação de uma incompatibilidade bidirecional é o rápido aumento de FCS e de erros de alinhamento no lado semi-duplex e runts na porta bidirecional (como visto em uma porta `sh {mod_num/port_num}`).

8. Compreenda a medida - mensagens da árvore. Além do que a mensagem de erro de incompatibilidade bidirecional, você pode igualmente ver estes medir - mensagens da árvore quando você muda a velocidade em um link. Um exame da medida - a árvore é além do alcance deste documento; consulte o capítulo em medir - árvore para obter mais

informações sobre da medida - a árvore.%PAGP-5-PORTFROMSTP:Port 1/1 left bridge port 1/1  
%PAGP-5-PORTTOSTP:Port 1/1 joined bridge port 1/1

9. A fim demonstrar o que acontece quando o modo duplex foi configurado, o modo na porta 1/1 no Switch A é ajustado à metade 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 ambo o Switches estão operando-se na metade - duplex. A porta 1/1 no switch B é configurada ainda ao automível negocia, segundo as indicações desta 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 à metade. Isto é consistente com a política recomendada configurar da mesma forma ambos os parceiros de enlace.

10. A fim executar a política às maneiras configurar ambos os parceiros de enlace para o mesmo comportamento, esta etapa ajusta agora o modo duplex à metade e à velocidade ao 10 na porta 1/1 no switch B.Está é a saída da emissão do comando **set port duplex 1/1**

```
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 este comando é inválido se a autonegociação é permitida. Isto igualmente significa que este comando não desabilita a auto-negociação. A autonegociação pode somente ser desabilitada com o set port speed {mod\_num/port\_num {10 | comando 100}}.Here is the output of entering the set port speed 1/1 10 command on 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** em trabalhos do switch B: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
```

**Nota:** O **set port duplex {mod\_num/port\_num {half | full}}** comando é dependente do **set port speed {mod\_num/port\_num {10 | 100}}** comando. Ou seja, você deve definir a velocidade antes de definir o modo bidirecional.

11. Configurar as portas 1/1 em ambo o Switches ao automível negociam com o comando **set port speed 1/1 auto**.Switch-A> (enable) set port speed 1/1 auto

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

**Nota:** Um modo duplex de uma porta foi configurado uma vez a algo a não ser o automível, a única maneira de configurar a porta ao auto sentido que 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. Ou seja se você emite o comando

**set port speed {mod\_num/port\_num} auto**, restaura a velocidade de porta que detecta e detecção de modo bidirecional ao automóvel.

12. Examine o estado das portas 1/1 em ambo o 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

As duas portas agora estão configuradas em seu comportamento padrão de negociação automática. Ambas as portas negociaram bidirecional e 100Mb.

## [Antes que você chamar a equipe de Suporte técnico do Cisco Systems](#)

Antes que você chame o Web site do Suporte técnico do Cisco Systems, certifique-se de você ter lido com este capítulo e ter terminado as ações sugeridas para seu problema de sistema.

Adicionalmente, faça estes e documente os resultados de modo que nós possamos melhor lhe ajudar:

- Capture a saída da **versão da mostra de** todos os dispositivos afetados.
- Capture a saída do **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.

## [Configurando conexões EtherChannel Switch a Switch nos Switches Catalyst 4000/5000/6000](#)

O EtherChannel permite que vários links físicos Fast Ethernet ou Gigabit Ethernet sejam combinados em um canal lógico. Isto permite que o tráfego entre os links estado loadshared no canal, assim como a Redundância caso uns ou vários links no canal falharem. O EtherChannel pode ser usado para interconectar switch LAN, Roteadores, server, e clientes através da fiação do par não-blindado (UTP) ou o modo simples e a fibra multimodo.

EtherChannel é um meio fácil para agregar largura de banda entre dispositivos de rede críticos. No catalizador 5000, um canal pode ser criado de duas portas que lhe fazem um link 200Mbps (400Mbps FULL-frente e verso) ou de quatro portas que lhe fazem um link 400Mbps (800Mbps FULL-frente e verso). 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 Spanning Tree Protocol (STP) considera estes enlaces redundantes entre dois dispositivos ser laços e faz com que os enlaces redundantes reajam do modo de bloqueio, que faz eficazmente estes links inativos (que forneça somente recursos de backup se o enlace principal falha). Quando você usar IO 3.1.1 ou maior, medindo - a árvore trata o canal como um link grande, assim que todas as portas no canal podem ser ativas ao mesmo tempo.

Esta seção toma-o com as etapas para configurar um EtherChannel entre dois Catalyst 5000 Switch e para mostrar-lhe os resultados dos comandos enquanto são executados. Os Catalyst 4000 e 6000 Switches poderiam ter sido usados nas encenações apresentadas neste documento para obter os mesmos resultados. Para o Catalyst 2900XL e o 1900/2820, a sintaxe de comando

é diferente, mas os conceitos de EtherChannel são os mesmos.

O EtherChannel pode ser configurado manualmente se você datilografa dentro os comandos apropriados, ou pode ser configurado automaticamente se o interruptor negocia o canal com o outro lado com o Port Aggregation Protocol (PAgP). Recomenda-se usar o modo desirable PAgP para configurar o EtherChannel sempre que possível desde que a configuração manual do EtherChannel pode criar algumas complicações. Este documento dá exemplos de como configurar manualmente o EtherChannel e os exemplos de como configurar o EtherChannel com PAgP. Também foram incluídas informações sobre como fazer troubleshooting do EtherChannel e como usar o truncamento com o EtherChannel. Neste documento, todo o EtherChannel dos termos, Fast EtherChannel, Gigabit EtherChannel ou canaliza refere o EtherChannel.

## Índice

1. [Tarefas para a configuração manual do EtherChannel](#)
2. [Verifique a configuração de EtherChannel](#)
3. [Uso PAgP configurar automaticamente o EtherChannel \(método preferido\)](#)
4. [Entroncamento e EtherChannel](#)
5. [Troubleshooting do EtherChannel](#)
6. [Comandos usados neste documento](#)

Esta figura ilustra nosso ambiente de teste. A configuração do Switches foi cancelada com o comando **clear config all**. Então, a alerta foi mudada com **nome de sistema do grupo**. Um endereço IP de Um ou Mais Servidores Cisco ICM NT e uma máscara foram atribuídos ao interruptor para propósitos do gerenciamento com **int sc0 172.16.84.6 255.255.255.0 do grupo** para o **int sc0 172.16.84.17 255.255.255.0 de SwitchA** e de **grupo** para SwitchB. Um gateway padrão foi atribuído a ambo o Switches com **set ip route default 172.16.84.1**.

As configurações de switch foram canceladas de modo que nós pudéssemos partir das condições padrão. O Switches era nomes concedidos de modo que nós pudéssemos o identificar da alerta na linha de comando. Os endereços IP de Um ou Mais Servidores Cisco ICM NT foram atribuídos de modo que nós pudéssemos sibilar entre o Switches para testar. O gateway padrão não foi usado.

Muito dos comandos exigem mais saídas do que o necessário para nossa discussão. A saída estranha é suprimida neste documento.

## [Tarefas para a configuração manual do EtherChannel](#)

Este é um sumário dos sentidos para configurar manualmente o EtherChannel.

1. [Mostre a Versão do IOS e os módulos que nós nos usamos neste documento.](#)
2. [Certifique-se de que o EtherChannel seja compatível com as portas.](#)
3. [Verifique se as portas estão conectadas e funcionando.](#)
4. [Verifique se as portas a serem agrupadas têm as mesmas configurações.](#)
5. [Identifique grupos válidos de portas.](#)
6. [Crie o canal.](#)

## [Passo a passo](#)

Estas são as etapas para configurar manualmente o EtherChannel.

1. O comando **show version** indica a versão de software que o interruptor executa. As lista de comando **show module** que os módulos são instalados no interruptor.

```
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

2. Verifique se EtherChannel é suportado nas portas. O **show port capabilities** aparece nas versões 4.x e superiores. Se você tiver um IOS anterior ao 4.x, deve ignorar esta etapa. Nem todos os módulos Fast Ethernet suportam EtherChannel. Alguns dos módulos originais de EtherChannel têm o "Fast EtherChannel" escrito no canto esquerdo inferior do módulo (enquanto você o enfrenta no interruptor) que lhe diz que a característica está apoiada. Esta convenção foi abandonada em uns módulos mais atrasados. 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 apoie olhares do EtherChannel como este.

```
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

```

3. Verifique se as portas estão conectadas e funcionando. Antes que você conecte os cabos, este é o status de 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 que você conecta os cabos entre os dois Switches, este é o estado.

```

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

```

Desde que as configurações de switch foram canceladas antes que este teste começado, as portas estiver em suas condições padrão. Todas elas estão em vlan1 e sua velocidade e duplex estão configuradas para auto. Após a conexão dos cabos, negociam a uma velocidade de 100Mbps e completamente - duplex. O estado é conectado, assim que nós podemos sibilhar o outro interruptor.

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

Em sua rede, você pôde querer a ajustar manualmente as velocidades a 100Mbps e completamente - duplex em vez da confiança na autonegociação desde que você quer provavelmente suas portas ser executado sempre na velocidade a mais alta. Para uma discussão de auto-negociação, veja a [metade/auto-negociação half/full duplex dos Ethernet 10/100Mb do Troubleshooting da](#) seção.

4. Verifique se as portas a serem agrupadas têm as mesmas configurações. Este é um ponto importante que seja coberto com maiores detalhes na seção de Troubleshooting. Se o comando setup o EtherChannel não trabalha, é geralmente porque as portas envolvidas no canal têm as configurações que diferem de se. Isto inclui as portas no outro lado do link, assim como as portas local. Em nosso caso, desde que as configurações de switch foram canceladas antes que este teste começado, as portas estiver em suas condições padrão. São todos em vlan1; sua velocidade e duplexação é ajustada ao automóvel, e a toda a medida - os parâmetros da árvore para cada porta são ajustados o mesmos. Nós vimos da saída que depois que os cabos são conectados, as portas negocia a uma velocidade de 100Mbps e completamente - duplex. Desde que medindo - a árvore é executado para cada VLAN, é mais fácil configurar o canal e responder apenas aos Mensagens de Erro do que para tentar e verificar cada medida - a árvore coloque para a consistência para cada porta e o VLAN no canal.

5. Identifique grupos válidos de portas. No catalizador 5000, somente as determinadas portas podem ser unidas em um canal. Essas dependências restritivas não se aplicam a todas as plataformas. As portas em um canal em um catalizador 5000 devem ser contíguas.

Observação do **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 um controlador de Ethernet de empacotamento no módulo que causa estas limitações de configuração. Vejamos outra porta.

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

Esta porta pode ser agrupada em um grupo de duas portas (2/3-4) ou em um grupo de quatro (2/1-4). **Nota:** O dependente em cima do hardware, lá pode ser restrições adicionais. Nos módulos determinados (WS-X5201 e WS-X5203), você não pode formar um EtherChannel com as últimas duas portas em um “grupo de porta” a menos que as primeiras duas portas no grupo já formarem um EtherChannel. Um “grupo de porta” é um grupo de portas seja permitido que formar um EtherChannel (2/1-4 são um grupo de porta neste exemplo). Por exemplo, se você cria EtherChannels separados com as somente duas portas em um canal, você não pode atribuir a portas 2/3-4 a um canal até que você tenha primeiras portas configuradas 2/1-2 a um canal, para os módulos que têm esta limitação! Iguamente, antes que você configure portas 2/6-7, você deve configurar portas 2/5-6. Esta limitação não ocorre nos módulos usados para este documento (WS-X5225R, WS-X5234). Desde que nós configuramos um grupo de quatro portas (2/1-4), este está dentro do agrupamento aprovado. Nós não podemos atribuir a um grupo de quatro às portas 2/3-6. Este é um grupo de porta contínua, mas não começam no limite aprovado, como mostrado pelo **comando show port capabilities** (os grupos válidos seriam portas 1-4, 5-8, 9-12, 13-16, 17-20, 21-24).

6. Crie o canal. A fim criar o canal, use o comando **set port channel <mod/port sobre** para cada interruptor. Nós recomendamos que você gerencie as portas fora em um lado do canal ou no outro lado com o **comando set port disable** antes que você gire o EtherChannel sobre manualmente. Isto evita problemas possíveis com medida - árvore dentro do processo de configuração. Medida - a árvore pode fechar algumas portas (com um status de porta do “errdisable”) se um lado está configurado enquanto um canal antes que o outro lado possa ser configurado como um canal. Devido a esta possibilidade, é muito mais fácil criar EtherChannels com o PAgP, que é explicado mais tarde neste documento. A fim evitar esta situação quando você configura o EtherChannel manualmente, nós desabilitamos as portas em SwitchA, configuramos o canal em SwitchA, configuramos o canal em SwitchB, e re-permitimos então as portas em 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
```

Desabilite agora as portas em SwitchA até que ambo o Switches esteja configurado para o EtherChannel de modo que medindo - a árvore não gerencie erros e fecha 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 modo de canal para *sobre* para SwitchA. 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 esteve ajustado a *sobre*, mas o estado das portas é desabilitado (porque nós desabilitamos então mais cedo). O canal não é operacional neste momento, mas torna-se operacional quando as portas são permitidas. Switch-A (enable) `show port channel`

Port	Status	Channel mode	Channel status	Neighbor device	Neighbor 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. Esta mensagem é indicada no console de SwitchB quando as portas de SwitchA foram desabilitadas. 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

```

Gire sobre o canal para o switch B. Switch-B (enable) `set port channel 2/1-4 on` Port(s) 2/1-4 channel mode set to on. Verifique que o modo de canal está ligada para SwitchB. Switch-B (enable) `show port channel`

Port	Status	Channel mode	Channel status	Neighbor device	Neighbor 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 SwitchB está ligada, mas o estado das portas é *não-conectado*. 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

A fim verificar que o canal setup corretamente, faça o comando `show port channel`.

```

Switch-A (enable) show port channel

```

Port	Status	Channel mode	Channel status	Neighbor device	Neighbor 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
-----
```

Medida - a árvore é mostrada para tratar as portas como uma porta lógica neste comando. Quando a porta for alistada como 2/1-4, medindo - a árvore está tratando as portas 2/1, 2/2, 2/3 e 2/4 como *uma 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
```

O EtherChannel pode ser executado com maneiras diferentes de distribuição de tráfego através das portas em um canal. A especificação EtherChannel não determina como o tráfego deve ser distribuído pelos enlaces em um canal. O catalizador 5000 usa o último bit ou os últimos dois bit (dependente de quantos links estão no canal) dos endereços MAC de origem e de destino no quadro para determinar que porta no canal a se usar. Você vê quantidades de tráfego similares em cada um das portas no canal se esse tráfego é gerado por uma distribuição normal de endereços MAC em um lado do canal ou no outro. A fim verificar que o tráfego vai sobre todas as portas no canal, você pode usar o **comando show mac**. Se suas portas eram ativas antes que você configurou o EtherChannel, você pôde restaurar os contadores de tráfego a zero pelo **comando clear counters**, e então os valores de tráfego representam como o EtherChannel distribuiu o tráfego.

Em nosso ambiente de teste, nós não obtivemos uma distribuição do mundo real porque não há nenhuma estação de trabalho, server, ou Roteadores que gerencie o tráfego. Os únicos dispositivos que gerenciem o tráfego são o Switches ele mesmo. Nós emitimos alguns sibilos de SwitchA a SwitchB, e você pode dizer que o tráfego de 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 de mais baixo na saída, a informação transmitir (Xmit-unicast) mostra como SwitchA distribuiu o tráfego através do canal a SwitchB. Nós igualmente vemos que uma quantidade pequena de tráfego multicast interruptor-gerado (ISL dinâmico, CDP) sai todas as quatro portas. Os pacotes de transmissão são perguntas ARP (para o gateway padrão - que não existe em nosso laboratório aqui). Se nós tivemos as estações de trabalho que enviam pacotes através do interruptor a um destino no outro lado do canal, nós esperaríamos ver o tráfego que vai sobre cada um dos quatro links no canal. Você pode monitorar a distribuição de pacote de informação em sua própria rede com o **comando show mac**.

```
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 \(o método preferido\)](#)

O Port Aggregation Protocol (PAgP) facilita a criação automática dos enlaces de EtherChannel

com a troca dos pacotes entre portas de canal apto. O protocolo aprende as capacidades de grupos de porta dinamicamente e informa as portas próximas.

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, os pacotes de multicast e broadcast externos transmitidos em uma porta em um canal são obstruídos de seu retorno em toda a outra porta do canal.

Há quatro modos de canal que podem ser configurados pelo usuário: em, fora, automático, e desejável. Os pacotes PAgP são trocados apenas entre portas no modo automático e desejável. As portas configuradas no modo ligado ou desligado não trocam pacotes PAgP. As configurações recomendadas para o Switches que você quer formar e o EtherChannel são ter ambos o Switches ajustado ao **modo desirable**. Isso fornece o comportamento mais robusto em que um lado ou o outro deve encontrar situações de erro ou ser reinicializado. O modo padrão do canal é automático.

Ambos os **modos de auto e desejável** permitem que as portas negociem com as portas conectadas para determinar e assim por diante se podem formar um canal baseado em critérios tais como a velocidade de porta, estado de entroncamento, VLAN nativo.

As portas podem formar um EtherChannel quando reagem de modos de canal diferentes enquanto os modos são compatíveis:

- Uma porta no modo desejável pode formar um EtherChannel bem-sucedido com outra porta que esteja no modo desejável ou auto.
- Uma porta em modo automático pode formar um EtherChannel com outra porta no modo desejado.
- Uma porta no **modo automático** não pode formar um EtherChannel com uma outra porta que reaja igualmente do **modo automático** desde que nenhuma porta inicia a negociação.
- Uma porta dentro no modo pode formar um canal somente com uma porta dentro no modo porque as portas dentro no modo não trocam pacotes PAgP.
- Uma porta no **modo desligado** não forma um canal com nenhuma porta.

Quando você usar o EtherChannel, se um "SPANTREE-2: A mensagem "Channel misconfig - x/x-x will be disabled" (Erro de configuração de canal - x/x-x será desabilitado) ou uma mensagem de syslog semelhante é exibida, indicando uma incompatibilidade dos modos EtherChannel nas portas conectadas. Nós recomendamos que você corrija a configuração e re-permite as portas com o **comando set port enable**. As configurações de EtherChannel válidas incluem estes:

**Tabela 22-5: Configurações EtherChannel Válidas**

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

<sup>11f</sup> o local e portas vizinha reagem do **modo automático**, um conjunto EtherChannel não formam.

Está aqui um sumário de todos os cenários de modo canalização possíveis. Algumas destas combinações podem causar a medida - árvore para pôr as portas sobre o lado de canalização no *estado errdisable* (isto é, fechado lhes para baixo).

Tabela 22-6: Cenários de modo canalização

Modo de canal do Switch A	Modo de canal do Switch B	Estado do canal:
Ligado	Ligado	Canal
Ligado	Desligado	Sem canal (errdisable)
Ligado	Automático	Sem canal (errdisable)
Ligado	Desirable	Sem canal (errdisable)
Desligado	Ligado	Sem canal (errdisable)
Desligado	Desligado	Sem canal
Desligado	Automático	Sem canal
Desligado	Desirable	Sem canal
Automático	Ligado	Sem canal (errdisable)
Automático	Desligado	Sem canal
Automático	Automático	Sem canal
Automático	Desirable	Canal
Desirable	Ligado	Sem canal (errdisable)
Desirable	Desligado	Sem canal
Desirable	Automático	Canal
Desirable	Desirable	Canal

Nós desligamos o canal do exemplo anterior com este comando em SwitchA e em 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. A fim verificar isto incorpore 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 precedente igualmente mostra que atualmente as portas não canalizam. Uma outra maneira de verificar o estado de canal é esta.

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

É realmente muito simples fazer o canal trabalhar com PAgP. Ambo o Switches é ajustado neste momento ao modo automático que significa que canaliza se uma porta conectada envia um pedido PAgP canalizar. Se você setSwitchA a desejável, SwitchA, ele faz com que SwitchA envie pacotes PAgP ao outro interruptor e o pede para canalizar.

```
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
```

A fim ver o canal, faça isto.

```
Switch-A (enable) show port channel Port Status Channel Channel Neighbor Neighbor mode status
device port -----
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 -----
```

Desde que SwitchB reagia do modo automático, respondeu aos pacotes 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 -----
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 -----
```

**Nota:** Recomenda-se ajustar ambos os lados do canal a **desejável** de modo que os ambos os lados tentem iniciar o canal se um lado sai. Se você ajusta as portas EtherChannel em SwitchB ao **modo desejável**, mesmo que o canal reaja atualmente ativo e do **modo automático**, não levanta 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 -----
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 SwitchA sai por qualquer motivo, ou se o hardware novo substitui SwitchA, SwitchB tenta restabelecer o canal. Se o equipamento novo não pode canalizar, SwitchB trata suas portas 2/1-4 como portas decanalização normais. Este é um dos benefícios do uso do **modo desejável**. Se o canal esteve configurado com o PAgP no modo e um lado da conexão tem um erro de algum tipo ou uma restauração, pode causar um estado errdisable (parada programada) no outro lado. Com o PAgP ajustado no modo desejável 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 pode igualmente girar o entroncamento sobre para todas as portas antes que você crie o canal, ou você pode girá-lo sobre depois que você cria o canal (como nós fazemos aqui). Tanto quanto o EtherChannel, não importa; o entroncamento e o EtherChannel são separar recursos-se completamente. O que importa é que todas as portas envolvidas estejam no mesmo modo: ou são todo o entroncamento antes que você configure o canal ou forem todos não entroncamento antes que você configure o canal. Todas as portas devem estar no mesmo estado de entroncamento antes que você crie 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 aparelho de teste podem fazer o entroncamento ISL ou 802.1q. À revelia, os módulos são ajustados ao auto entroncamento e negociados o modo, assim que significa que tronco se o outro lado os pede ao tronco, e negociam se usar o método para entroncamento ISL ou 802.1q. Se não perguntado ao tronco, trabalham como portas normais do NON-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, nós ajustamos SwitchA a desejável. O Switch A já está definido para negociação. A combinação desejável/negocia causas SwitchA para pedir SwitchB ao tronco e para negociar o tipo de entroncamento para fazer (ISL ou 802.1q). Desde que SwitchB opta a autonegociação, SwitchB responde ao pedido de SwitchA. Estes resultados ocorrem:

```
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 era que o modo de entroncamento esteve negociado com o switch vizinho, e decidiram em ISL (n-ISL). O status atual está truncando agora. Este é o que aconteceu em SwitchB devido ao comando emitido em 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 transformaram troncos, mesmo que nós somente mudemos especificamente uma porta (2/1) a desejável. Este é um exemplo de como a mudança de uma porta no canal afeta todas as portas.

## Troubleshooting do EtherChannel

É possível dividir os desafios de EtherChannel em duas áreas principais: Troubleshooting dentro da fase de configuração, e Troubleshooting dentro da fase de execução. Erros de configuração normalmente ocorrem devido a parâmetros incompatíveis nas portas envolvidas (velocidades diferentes, dúplex diferente, valores diferentes de porta de árvore de abrangência, etc.). Você pode igualmente gerar erros dentro da configuração se você ajusta o canal em um lado a **sobre** e em espera demasiado muito antes que você configurar o canal no outro lado. Isto causa loop de Spanning Tree, que gerencie um erro, e fecha a porta.

Quando um erro é encontrado quando você configurar o EtherChannel, seja certo verificar o estado das portas depois que você corrige a situação de erro do EtherChannel. Se o status de porta é *errdisable*, esse significa que as portas estiveram fechadas pelo software e não se aproximam outra vez até que você inscreva o **comando set port enable**.

**Nota:** Se o status de porta se transforma *errdisable*, você deve especificamente permitir as portas com o **comando set port enable** para que as portas tornem-se ativo. Atualmente, você pode corrigir todas as edições do EtherChannel mas as portas não vêm acima nem formam um canal até que estejam permitidas outra vez! As versões futuras do sistema operacional podem periodicamente verificar se as *portas errdisable* devem ser permitidas.

Para estes testes nós desligamos o entroncamento e o EtherChannel: Parâmetros incompatíveis; Espera demasiado muito antes que você configurar o outro lado; Estado *errdisable* correto; e mostra o que acontecer quando rupturas de enlace e é restaurado.

## Parâmetros incompatíveis

Veja aqui um exemplo de parâmetros incompatíveis. Nós o set port 2/4 no VLAN2 quando as outras portas estiverem ainda em VLAN 1. a fim criar um VLAN novo, nós devemos atribuir um VTP domain para o interruptor e criar o 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 formou somente entre portas 2/1-2. As portas 2/3-4 foram deixadas para fora porque a porta 2/4 estava em um VLAN diferente. Não havia nenhuma Mensagem de Erro; O PAgP fez o que podia para fazer o canal funcionar. Você precisa de olhar os resultados quando você cria o canal para se certificar que fez o que você o quis fazer.

Ajuste agora o canal manualmente a sobre com porta 2/4 em um vlan diferente e veja o que acontece. Primeiramente nós ajustamos o modo de canal de volta ao automático a fim rasgar para baixo o canal atual, a seguir nós ajustamos o canal manualmente a sobre.

```

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

```

Em SwitchB nós podemos girar o canal sobre e observar que diz a multa do canal das portas, mas nós sabemos que 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 -----
-----

```

Isto faz claro que você deve ambos os lados de verificação do canal quando você configura manualmente o canal para se certificar que os ambos os lados estão acima, de não apenas um lado. Esta saída mostra que SwitchB está ajustado para um canal, mas SwitchA não canaliza porque tem uma porta que está no VLAN errado.

**Espera demasiado muito antes que você configurar o outro lado**

Em nossa situação, SwitchB tem o EtherChannel girado sobre, mas SwitchA não faz porque tem um erro de configuração vlan (as portas 2/1-3 estão em vlan1, a porta 2/4 estão em vlan2). É aqui o que acontece quando um lado de um EtherChannel está ajustado a sobre quando o outro lado reagir ainda do modo automático. SwitchB, após alguns minutos, fechou suas portas devido a

uma detecção de medida do laço. 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 de SwitchB a SwitchA na porta 2/1 é enviada para trás a SwitchB nas portas 2/2, 2/3 e 2/4 porque SwitchA trata estas portas como portas independente. Esse é o motivo pelo qual o SwitchB acredita que há um circuito de árvore de abrangência. Observe que as portas em SwitchB estão desabilitadas agora e tenha um estado do *errdisable*.

```
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 -----
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
```

### Corrija o estado errdisable

Às vezes quando você tenta configurar o EtherChannel mas as portas não estão configuradas o mesmos, causa as portas em um lado do canal ou no outro a ser fechados. As luzes de enlace são amarelas na porta. Você pode dizer este pelo console se você datilografa o **show port**. As portas são alistadas como o *errdisable*. A fim recuperar disto, você deve fixar os parâmetros combinados mal nas portas envolvidas, a seguir re-permite as portas. Apenas note isso re-para permitir as portas é uma etapa separada que deva ser executada para que as portas se tornem funcional outra vez.

Em nosso exemplo nós sabemos que SwitchA teve uma má combinação vlan. Nós vamos a SwitchA e pomos a parte traseira da porta 2/4 dentro a vlan1. Então nós gerenciemos o canal para portas 2/1-4 sobre. SwitchA não mostra conectado até que nós re-permitamos portas de SwitchB. Então quando nós fixamos SwitchA e o pusemos no modo de canalização, nós vamos para trás a SwitchB e re-permitimos 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
-----
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 -----
-----
```

### Mostra o que acontecer quando rupturas de enlace e é restaurado

Quando uma porta no canal vai para baixo, todos os pacotes que forem enviados normalmente nessa porta estão deslocados sobre à porta seguinte no canal. Você pode verificar que este

acontece com o comando **show mac**. Em nosso aparelho de teste, nós mandamos SwitchA enviar pacotes de ping a SwitchB a fim de ver que link o tráfego usa. Primeiramente nós cancelamos os contadores, a seguir mostramos o Mac, enviamos três sibilos, e **mostramos** então o Mac outra vez para ver em que canal as respostas de 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
-----
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 momento, nós recebemos as respostas de ping na porta 3/1. Quando o console de SwitchB envia uma resposta a SwitchA, o EtherChannel usa a porta 2/1. Agora nós fechamos a porta 2/1 em SwitchB. De SwitchA nós emitimos um outro sibilo e vemos que canal a resposta volta. (SwitchA envia sobre a mesma porta a que SwitchB é conectado. Mostramos apenas os pacotes recebidos do SwitchB porque os pacotes de transmissão estão mais adiante na exibição de show mac).

```
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 é desabilitada, o EtherChannel usa automaticamente a porta seguinte no canal, 2/2. Agora nós re-permitimos a porta 2/1 e esperamos-la para juntar-se ao grupo de bridge. Emitiremos então 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
```

Note que estes sibilos estão enviados da porta 2/1. Quando o link vem apoio, o EtherChannel outra vez adicionar-lo ao pacote e usa-o. Tudo isso é feito de forma transparente para o usuário.

## Comandos utilizados nesta seção

Estes são os comandos que foram usados nesta seção.

### Comandos usar-se para ajustar a configuração

- **set port channel on** - para girar sobre os recursos EtherChannel.
- **set port channel auto** - para restaurar as portas a seu modo de auto padrão.
- **set port channel desirable** - para enviar pacotes PAGP ao outro lado que pede que um canal esteja criado.
- **o set port permite** - de permitir as portas depois que desabilitação do set port ou após um estado errdisable.

- `set port disable` para desabilitar uma porta enquanto outras configuração estão sendo definidas.
- **set trunk desirable** - para girar sobre o entroncamento e para fazer com que esta porta envie um pedido ao outro interruptor indicar que este é um enlace de tronco. Se a porta está ajustada para negociar (a configuração padrão) para negociar o tipo de entroncamento para se usar no link (ISL ou 802.1q).

### Comandos usar-se para verificar a configuração

- **versão da mostra** - para indicar que versão de software o interruptor executa.
- **módulo show** - para indicar que módulos são instalados no interruptor.
- **as capacidades do show port** - de determinar se as portas que nós queremos se usar têm a capacidade para fazer o EtherChannel.
- `show port` - para determinar o status da porta (notconnect, connected) e as configurações de velocidade e frente e verso.
- **sibilo** - para testar a Conectividade ao outro interruptor.
- `show port channel` - Para visualizar o status atual do pacote EtherChannel.
- **show port channel mod/port** - para dar mais vista detalhada do status do canal de uma porta única.
- `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 usar-se para pesquisar defeitos a 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.
- **cancela contadores** - para restaurar os contadores de pacote de switch a zero. Os contadores ficam visíveis com o comando `show mac`.
- **Mac da mostra** - para ver os pacotes recebidos e enviados pelo interruptor.
- **sibilo** - para testar a Conectividade ao outro interruptor e para gerar o tráfego que aparece com o comando `show mac`.

## Usando Portfast e outros comandos para corrigir problemas de conectividade de inicialização de estação final.

Se você tem as estações de trabalho conectadas ao Switches que são incapazes de entrar a seu domínio de rede (NT ou Novell), ou são incapazes de obter um endereço de DHCP, a seguir você pôde querer tentar as sugestões alistadas neste documento antes que você explore outras avenidas. As sugestões são relativamente fáceis de executar e são muito frequentemente a causa dos problemas de conectividade da estação de trabalho encontrados durante a iniciação/fase de inicialização da estação de trabalho.

Com cada vez mais os clientes que o interruptor de distribuição ao desktop e substitui seu Hubs compartilhado com o Switches, nós considera frequentemente os problemas introduzidos no cliente/ambientes de servidor devido a este retardo inicial. O maior problema observado é que clientes Windows 95/98/NT, Novell, VINES, IBM NetworkStation/IBM Thin Clients e AppleTalk não são capazes de se conectar aos seus servidores. Se o software nestes dispositivos não é persistente dentro do procedimento de inicialização dão acima a tentativa conectar a seu server antes que o interruptor permita mesmo que o tráfego passe completamente.

**Nota:** Esse atraso na conectividade inicial geralmente se manifesta como erros que aparecem quando você faz a primeira inicialização de uma estação de trabalho. Estes são diversos exemplos dos Mensagens de Erro e dos erros que você pode ver:

- Um cliente de rede Microsoft exibe: "No Domain Controllers Available" (Nenhum controlador de domínio disponível).
- Relatórios DHCP, "nenhuns servidores DHCP disponíveis."
- Uma estação de trabalho de rede Novell IPX não apresenta a tela "Novell Login Screen" durante a inicialização.
- Os indicadores de um cliente do trabalho em rede Appletalk, "acesso a sua rede de Appletalk foram interrompidos. A fim restabelecer sua conexão, aberta e fechar o painel de controle do appletalk." É igualmente possível que o aplicativo de opção do cliente de appletalk ou não indica uma lista da zona, ou indica uma lista da zona incompleta.

O retardo inicial de conectividade também é observado freqüentemente em um ambiente comutado no qual um administrador de rede atualiza software ou drivers. Neste caso, um vendedor pode aperfeiçoar os direcionadores de modo que os procedimentos de inicialização da rede aconteçam mais cedo no processo de inicialização do cliente (antes que o interruptor esteja pronto para processar os pacotes).

Com as várias características que são incluídas agora em alguns Switches, pode tomar perto de um minuto para que um interruptor comece a prestar serviços de manutenção a uma estação de trabalho recentemente conectada. Este atraso pode afetar a estação de trabalho cada vez que é girado sobre ou recarregado. Estes são os quatro recursos principais que causam este atraso:

- Medida - protocolo de árvore (STP)
- Negociação EtherChannel
- Negociação de truncamento
- Negociação de velocidade/duplex do link entre o switch e a estação de trabalho

As quatro características estão listadas por ordem de que causa a maioria de atraso (que mede - protocolo de árvore) a que causa menos atraso (negociação de velocidade/bidirecional). Uma estação de trabalho conectada a um interruptor geralmente não causa loop de Spanning Tree, geralmente não precisa o EtherChannel, e geralmente não o precisa de negociar um método de entroncamento. (Se você desabilita a velocidade/negociação de detecção do link, pode igualmente reduzir o retardo de porta se você precisa de aperfeiçoar tanto quanto possível seu período de inicialização.)

Esta seção mostra como executar comandos startup da velocidade-otimização em três plataformas de Catalyst switch. Nas seções de cronometragem, nós mostramos por como o atraso da porta de switch é reduzido, e por quanto.

## [Índice](#)

1. [Background](#)
2. [Como reduzir o atraso de inicialização no Switch Catalyst 4000/5000/6000](#)
3. [Testes de temporização no Catalyst 5000](#)
4. [Como reduzir o retardo na inicialização no Switch Catalyst 2900XL/3500XL](#)
5. [Testes de cronometragem no Catalyst 2900XL](#)
6. [Como reduzir o retardo na inicialização no Switch Catalyst 1900/2800](#)
7. [Teste de cronometragem no Catalyst 2820](#)
8. [Um benefício adicional ao Portfast](#)

Os termos "estação de trabalho", "estação final", "servidor" são usados de modo intercambiável nesta seção. O que nós referimos é todo o dispositivo conectado diretamente a um interruptor por um único cartão NIC. Pode igualmente referir dispositivos com placas NIC múltiplas onde o cartão NIC é usado somente para a Redundância, em outras palavras a estação de trabalho ou o server não é configurado para atuar como uma ponte, ele apenas tem placas NIC múltiplas para a Redundância.

**Nota:** Há algumas placas NIC de servidor que suportam entroncamento e/ou EtherChannel. Há as situações onde o server precisa de viver ao mesmo tempo (no entroncamento) diversos VLAN ou o server precisa mais largura de banda no link que a conecta ao interruptor (EtherChannel). Nesses casos você não desliga o PAgP e você não desliga 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 cobre quatro características que alguns Switches tem que retardos iniciais da causa quando um dispositivo é conectado a um interruptor. Geralmente uma estação de trabalho não causa a medida - problema da árvore (laços), nem não precisa a característica (PAgP, DTP), assim que o atraso é desnecessário.

## Spanning Tree

Se você tem começado recentemente se transportar de um ambiente do hub a um ambiente do interruptor estes problemas de conectividade podem aparecer porque um interruptor funciona muito diferentemente do que um hub. Um interruptor fornece a Conectividade na camada de ligação de dados, não na camada física. O interruptor tem que usar um algoritmo de Bridging para decidir se os pacotes recebidos em uma porta precisam de ser transmitidos para fora outras portas. O algoritmo de bridging é suscetível a loops físicos na topologia da rede. Devido a esta susceptibilidade aos laços, o Switches executa um protocolo chamado o Spanning Tree Protocol (STP) esse os laços das causas a ser eliminados na topologia. O corredor do STP causa todas as portas que são incluídas na medida - processo da árvore a transformar-se muito mais lento ativo do que de outra maneira, como detecta e obstrui laços. Uma rede interligada que tenha laços físicos, sem medir - árvore, quebra. Apesar do tempo envolvido, o STP é uma boa coisa. A medida - a árvore que é executado em Catalyst Switches é uma especificação do padrão para indústria (IEEE 802.1D).

Depois que uma porta no interruptor tem o link e se junta ao grupo de bridge que executa a medida - árvore nessa porta. Uma medida sendo executado da porta - a árvore pode ter 1 dos estados 5: Obstrução, escutando, aprendendo, enviando, e desabilitado. A árvore de abrangência determina se a porta deve iniciar o bloqueio e realizar imediatamente as fases de audição e identificação. À revelia passa aproximadamente 15 segundos que escutam e 15 segundos que aprendem.

Quando no estado de escuta e aprendizagem, o interruptor tentar determinar onde cabe na topologia de Spanning Tree. Quer especialmente saber se esta porta é parte de um laço físico. Se é parte de um laço, esta porta pode ser escolhida entrar no modo de bloqueio. Obstruir significa que não envia nem recebe dados do usuário para a eliminação de laços. Se a porta não é parte de um laço, continua ao estado de aprendizagem que envolve aprender que endereços MAC vivem fora desta porta. Este processo de inicialização da árvore de abrangência leva aproximadamente 30 segundos.

Se você conecta uma estação de trabalho ou um server com um único cartão NIC a uma porta de switch, esta conexão não pode criar um laço físico. Essas conexões são consideradas nós folhas. Não há nenhuma razão para fazer a estação de trabalho esperar 30 segundos quando o interruptor verificar para ver se há laços quando a estação de trabalho não pode causar um laço. Assim Cisco adicionou uma característica chamada "Portfast" ou a "inicialização rápida", que significa a medida - a árvore para esta porta suporá que a porta não é parte de um laço e se moverá imediatamente para o estado de encaminhamento, sem atravessar a obstrução, escutando, ou estados de 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.

**Nota:** Os recursos de portfast devem nunca ser usados nas portas de switch que conectam ao outro Switches ou Hubs ou Roteadores. Estas conexões podem causar laços físicos, e é muito importante que medindo - a árvore examina o procedimento de inicialização completo nestas situações. Um loop de spanning tree pode interromper o funcionamento da sua rede. Se o portfast é girado sobre para uma porta que seja parte de um laço físico, pode causar um indicador do tempo onde os pacotes poderiam possivelmente continuamente ser enviados (e para multiplicar mesmo) de tal maneira que a rede não pode recuperar. No Catalyst Operating System Software mais atrasado (5.4(1)), há uma característica chamada o protetor de BPDU de portfast, que detecta a recepção dos BPDU nas portas que têm Portfast permitiram. Desde que isto deve nunca acontecer, o protetor de BPDU põe a porta no estado do "errdisable".

## EtherChannel

Outros caracterizam um interruptor podem ter são chamados EtherChannel (ou Fast EtherChannel, ou Gigabit EtherChannel). Esta característica permite que os links múltiplos entre os mesmos dois dispositivos trabalhem como se eram um link rápido, com a carga de tráfego equilibrada entre os links. Um interruptor pode formar estes pacotes automaticamente com um vizinho com um protocolo chamado Port Aggregation Protocol (PAgP). As portas de switch que podem executar o padrão PAgP geralmente a um modo passivo chamaram o "automóvel" que significa que pode formar um pacote se o dispositivo vizinho através do link o pede a. Se você executa o protocolo no modo automático, pode fazer com que uma porta atrase para até 15 segundos antes que passe o controle ao algoritmo de Spanning Tree (o PAgP é executado em uma porta antes de medir - a árvore faz). Não há nenhuma razão para que o PAgP seja executado em uma porta conectada a uma estação de trabalho. Se você ajusta o modo de PAgP da porta de switch a "fora," elimina este atraso.

## Entroncamento

Uns outros recursos de switch são a capacidade de uma porta para formar um tronco. Um tronco é configurado entre dois dispositivos quando eles precisam levar o tráfego de várias redes de área local virtual (VLANs). Um VLAN é algo comuta cria para fazer um grupo das estações de trabalho parecer ser no seus próprios "segmento" ou "domínio de transmissão." As portas de tronco fazem estes VLAN estender através dos switch múltiplos, de modo que um único VLAN possa cobrir um terreno inteiro. Fazem esta com a adição de etiquetas aos pacotes; isto indica a que VLAN o pacote pertence.

Há diferentes tipos de protocolos de truncamento. Se uma porta pode se transformar um tronco, pode igualmente ter a capacidade ao tronco automaticamente, e negocia em alguns casos mesmo que tipo de entroncamento a se usar 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 estes protocolos estão sendo executado podem atrasar uma porta no interruptor que torna-se ativo.



Em geral, uma porta conectada a uma estação de trabalho pertence a apenas uma VLAN e, portanto, não precisa de tronco. Se uma porta tem a capacidade para negociar a formação de um tronco opta geralmente o "auto" modo. Se a porta é mudada a um modo de entroncamento de "OFF" reduz mais o atraso de uma porta de switch que torna-se ativa.

## Negociação de Velocidade e Duplex

Apenas girar sobre Portfast e desligar o PAgP (se presente) são geralmente bastante resolver o problema, mas se você precisa de eliminar cada segundo possível você poderiam igualmente ajustar a velocidade de porta e duplex manualmente no interruptor se é uma porta de várias velocidades (10/100). A autonegociação é uns recursos agradáveis mas girá-la fora poderia salvar o 2 segundos em um catalizador 5000 (não ajuda muito nos 2800 ou no 2900XL).

Pode haver umas complicações, embora, se você desliga a autonegociação no interruptor mas lhe deixa o active na estação de trabalho. Desde que o interruptor não negocia com o cliente, o cliente não pôde escolher a mesma configuração bidirecional que o interruptor usa. Veja do "a metade/auto-negociação half/full duplex dos Ethernet 10/100Mb Troubleshooting" para obter informações adicionais sobre das advertências da autonegociação.

## [Como reduzir o atraso de inicialização no Switch Catalyst 4000/5000/6000](#)

Estes cinco comandos show como girar sobre Portfast, como desligar a negociação de PAGP, desligam a negociação de entroncamento (DISL, DTP) e desligam a negociação de velocidade/bidirecional. **O portfastcommand do spantree do grupo** pode ser feito em uma faixa de porta imediatamente (**ajuste o portfast de árvore de abrangência 2/1-12 permitem**). Geralmente o **canal do set port** deve ser desligado com um grupo válido de portas de canal apto. Neste caso o módulo dois tem a capacidade para canalizar com portas 2/1-2 ou com portas 2/1-4, assim que qualquer um destes grupos de portas seria válido usar-se.

**Nota:** A versão 5.2 do Cat OS para o Catalyst 4000/5000 tem um comando new chamado o **host do set port** que é um macro que combine estes comandos em um comando fácil de usar (a não ser que não muda os ajustes da velocidade e duplexação).

## 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, etc. 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 de switch usado neste documento é 4.5(1). Para o resultado completo da versão e do módulo show da mostra refira esta seção de teste de cronometragem.

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

Este comando mostra como ver o estado atual de uma porta a propósito da medida - árvore. Atualmente a porta consiste na medida - o estado de encaminhamento da árvore (que enviam e que recebem pacotes) e a coluna da inicialização rápida mostram que o portfast está desabilitado atualmente. Em outras palavras, a porta demorará pelo menos 30 segundos para entrar no estado de encaminhamento 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 nós permitimos o portfast nesta porta de switch. O interruptor avverte-nos que este comando deve somente ser usado nas portas que são conectadas a um host único (uma estação de trabalho, um server, etc.) e nunca ser usado nas portas conectadas ao outro Hubs ou Switches. A razão que nós permitimos o portfast é assim que o começo da porta de enviar imediatamente. Nós podemos fazer este porque uma estação de trabalho ou um server não causam um laço da rede, assim que porque verificação do tempo do desperdício? Mas um outro hub ou switch pode causar um laço, e nós queremos atravessar sempre os estágios de audição e de aprendizagem normais quando nós conectamos a estes 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, etc. to a fast start port can cause temporary spanning tree loops. Use with caution.
Spantree port 2/1 fast start enabled.
```

A fim verificar que Portfast está permitido para esta porta faça 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. Mais tarde na seção de cronometragem deste documento, nós mostramos como mandar o interruptor relatar cada fase da medida - a árvore que move completamente no tempo real. Esta saída igualmente mostra o tempo de retardo de encaminhamento (15 segundos). Este é o tempo que a árvore expandida ficará no estado de escuta e também indica o tempo de duração do estado de aprendizagem de cada porta do 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**. Seja certo e especifique o número de módulo (2 neste caso) de modo que o comando lhe mostre o modo de canal mesmo se não há nenhum canal formado. Se nós fazemos o canal do **show port** sem os canais formados, apenas não diz nenhuma canalização das portas. Queremos ir além 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 ...
```

A fim verificar que a negociação de entroncamento está, use o comando **set trunk off**. Nós mostramos o estado padrão. Em seguida, desative o entroncamento. Em seguida mostramos o estado resultante. Especificamos o número de módulo 2 para que possamos ver o modo de canal atual para as portas nesse 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 deve ser necessário exceto no mais raro dos casos desligar a auto-negociação de velocidade/bidirecional ou ajustar manualmente a velocidade e duplexação no interruptor. Nós damos um exemplo de como fazer isto nos testes de cronometragem com e sem o DTP, PAgP, e Portfast em uma seção do catalizador 5000 se você a sente é necessário para sua situação.

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

Este teste mostra o que acontece com cronometragem de inicialização da porta de switch enquanto os vários comandos são aplicados. As configurações padrão da porta são utilizadas primeiramente para o teste de desempenho do sistema. Têm o portfast desabilitado, o modo pagp (etherchannel) é ajustado ao automático (canaliza se pedido para canalizar), e o modo de entroncamento (DTP) é ajustado ao automático (ele troncos se perguntado ao tronco). O teste continua então ao portfast da volta sobre e mede o tempo, a seguir gerencie o PAgP para fora e mede o tempo, a seguir desliga o entroncamento e mede o tempo. Finalmente, desligamos a auto negociação e medimos o tempo. Todos estes testes são feitos em um catalizador 5000 com um cartão do Fast Ethernet de 10/100 que apoie o DTP e o PAgP.

**Nota:** O portfast de gerencio não está ligada a mesma coisa que girando a medida - árvore fora (como referido no documento). Com portfast sobre, medindo - a árvore ainda é executado na porta; apenas não obstrui, escuta, ou aprende, e vai imediatamente ao estado de encaminhamento. Girando a medida - a árvore não é recomendada fora porque afeta o VLAN inteiro e pode deixar a rede vulnerável aos laços da topologia física, que podem causar problemas de rede graves.

### 1. Mostre a Versão do IOS do interruptor e a configuração (versão da mostra, módulo

```
show).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
```

### 2. Ajuste o registro para medir - árvore ao mais verboso (ajuste o spantree 7 do nível de registro). Este é o nível de registro do padrão (2) para medir - a árvore, assim que significam que somente as situações crítica estão 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 para medir - a árvore é mudada a 7 (debugar), assim que nós podemos ver a mudança de estados de Spanning Tree 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 -----
```

3. Inicie pela porta no fechamento do Catalyst.

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

4. Agora o tempo e permite a porta. Queremos ver por quanto tempo a porta fica 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.
```

Observação da saída que tomou aproximadamente 22 segundos (20:17 20:39) para que a porta comece a medida - árvore que obstrui a fase. Este era o tempo onde tomou para negociar o link e para fazer tarefas DTP e PAgP. Quando obstruir começa, nós consistimos agora na medida - reino da árvore. De obstruir a porta, foi imediatamente à 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). **Nota:** Tecnicamente, os estágios de escuta e aprendizagem devem ter 15 segundos, que é como o parâmetro de retardo de encaminhamento está definido para esse VLAN. O estágio de aprendizagem realiza-se provavelmente mais perto de 15 segundos do que 14 segundos se nós tivemos mais medidas precisas. Nenhuma dessas medições são perfeitamente precisas. Nós apenas tentamos dar uma tomada das coisas da sensação durante quanto tempo.

5. Nós sabemos da saída e do comando **show spantree** que medindo - a árvore é ativa nesta porta. Deixe-nos olhar outras coisas que poderiam retardar a porta enquanto alcança o estado de encaminhamento. O comando **show port capabilities** mostra que essa porta tem a capacidade de truncar e criar um EtherChannel. O comando **show trunk** diz que essa porta está no modo automático e que está configurada para negociar o tipo de entroncamento a ser utilizado (ISL ou 802.1q, negociado por meio do Protocolo de Entroncamento Dinâmico (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
```

6. Primeiramente, nós permitiremos Portfast na porta. A negociação de entroncamento (DTP) está ainda no modo automático, e no EtherChannel (PAgP) reage ainda do modo automático.

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

```
spanntree portfast 2/1 enable Warning: Spanntree port fast start should only be enabled on
ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc.
to a fast start port can cause temporary spanning tree loops. Use with caution. Spanntree
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
```

%SPANNTREE-6-PORTFWD: port 2/1 state in vlan 1 change to **forwarding**. Agora, temos um tempo total de 21 segundos! Demora 20 minutos para se unir ao grupo de ligação (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). Economizamos 29 segundos habilitando o Portfast. Vamos analisar se podemos reduzir ainda mais o retardo.

7. Agora nós gerenciamos o modo de PAgP para “fora.” Nós podemos ver do comando show port channel que o modo de PAgP está ajustado ao *automóvel*, que significa que canaliza se perguntado por um vizinho que fale o 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.
```

8. 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 %SPANNTREE-6-PORTFWD: port 2/1 state in vlan 1 changed to **forwarding**. Observe acima que agora leva apenas 9 segundos atingir o estado de encaminhamento (56:23 a 56:32) em vez dos 21 segundos como no teste anterior. O PAgP de gerencio do *automóvel a fora* neste teste salvar aproximadamente 12 segundos.

9. Gire o entroncamento para fora (em vez do automóvel) e veja como esse afeta o tempo onde toma para que a porta alcance o estado de encaminhamento. Nós gerenciamos outra vez a porta de vez em quando, e gravamos 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 %SPANNTREE-6-PORTFWD: port
2/1 state in vlan 1 change for forwarding. Economizamos alguns segundos no início, pois
foram necessários apenas 4 segundos para alcançar o estado de encaminhamento da
árvore de abrangência (00:19 a 00:22). Nós salvar sobre os segundos 5 mudando o modo
de entroncamento do automóvel a fora.
```

10. (Opcional) se o tempo de inicialização da porta de switch era o problema deve ser resolvido até agora. Se você tem que barbear alguns mais segundos fora do tempo, você poderia ajustar a porta a velocidade e duplexação manualmente em vez de usar a negociação automática.Se você ajusta a velocidade e duplexação manualmente em nosso lado, exige que você ajusta a velocidade e duplexação no outro lado, também. Isto é porque ajustando a velocidade de porta e a autonegociação das inutilizações do duplex na porta, e o dispositivo de conexão não vê parâmetros da autonegociação. O dispositivo de conexão conecta somente em metade-frente e verso e nos resultados da incompatibilidade duplex (bidirecional) da resultante no desempenho ruim e nos erros de porta. 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.A fim ver o status de porta após ter ajustado a velocidade e duplexação faça o **show port**.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
cronometragem: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 %SPAN TREE-6-PORTFWD: port 2/1 state in vlan 1 changed to forwarding. O resultado
final oferece um período de 2 segundos (0528 a 0530).
```

11. Nós fizemos um outro visualmente teste programado (nós olhamos nossos relógios) começando um ping contínuo (ping - t) dirigido ao interruptor em um PC anexado ao interruptor. Nós desligamos então o cabo do interruptor. Os sibilos começaram a falhar. Então nós reconectamos o cabo ao interruptor e verificamos nossos relógios para ver quanto tempo tomou para que o interruptor responda aos sibilos do PC. Levou cerca de 5 a 6 segundos com autonegociação para a velocidade e o duplex ligarem, e cerca de 4 segundos com autonegociação para a velocidade e o duplex desligarem. Há muitas variáveis neste teste (iniciação PC, software PC, porta de Console do interruptor que respondem aos pedidos, etc.), mas nós apenas quisemos obter alguma sensação durante quanto tempo tomaria para obter uma resposta do ponto de vista PC. Todos os testes eram do interno debugam o ponto de vista da mensagem do Switches.

## [Como reduzir o retardo na inicialização no Switch Catalyst 2900XL/3500XL](#)

Os modelos 2900XL e 3500XL podem ser configurados de um navegador da Web, ou pelo SNMP, ou pelo comando line interface(cli). Nós usamos o CLI. Este é um exemplo onde nós ver o estado de Spanning Tree de uma porta, gerencie sobre o portfast, e verifica então que está ligada. O 2900XL/3500XL apoia o EtherChannel e o entroncamento, mas não apoia a criação dinâmica do EtherChannel (PAgP) ou a negociação do tronco dinâmico (DTP) na versão que nós testamos (11.2(8.2)SA6), assim que nós não temos nenhuma necessidade de girá-los fora neste teste. Também, depois que nós gerenciemos sobre o portfast, o tempo transcorrido para que a porta venha acima é já menos de 1 segundo, tão lá não é muito ponto a tentar mudar ajustes da negociação de velocidade/bidirecional para apressar acima coisas. Esperamos que um segundo represente ser rápido o suficiente! À revelia, o portfast está fora nas portas de switch. Estes são os comandos girar sobre 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
```

Esta plataforma é como o roteador IO; você deve salvar a configuração (começo da corrida de cópia) se você a quer ser salvar permanentemente.

### Verificação

A fim verificar que Portfast está permitido, faça 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
```

Olhe a configuração de switch.

```
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

Estes são os testes de cronometragem no Catalyst 2900XL.

1. A versão de software 11.2(8.2)SA6 foi usada no 2900XL para estes testes. Switch#**show version** Cisco Internetwork Operating System Software 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
2. Nós queremos o interruptor dizer nos que o que acontece e quando acontece, assim que nós incorporamos estes comandos: 2900XL(config)#**service timestamps debug uptime** 2900XL(config)#**service timestamps log uptime** 2900XL#**debug spanntree events** Spanning Tree event debugging is on 2900XL#**show debug** General spanning tree: Spanning Tree event debugging is on
3. Em seguida, fechamos 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#
4. Neste momento nós colamos estes comandos da prancheta no interruptor. Estes comandos exibem a hora no 2900XL e ativam a porta novamente: **show clock conf t int f0/1 no shut**
5. 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 Portfast. A segunda maneira é olhar a configuração running onde você não vê o comando **spanning-tree portfast** sob a relação. 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...] !
6. 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 Tempo total da parada programada até que a transmissão começada porta estiver **30 segundos (27:27 27:57)**
7. A fim girar sobre Portfast, faça isto: 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# **A fim verificar**



que Portfast está permitido, 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 ...
```

8. Faça agora o teste de cronometragem com Portfast permitiu
- ```
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 menos de 1 segundo. Se o atraso da inicialização de porta no interruptor era o problema, o portfast deve resolvê-lo. Recorde, o interruptor não apoia atualmente a negociação de tronco, assim que nós não precisamos de desligá-la. Nem apoia o PAgP para o entroncamento, assim que nós não precisamos de desligá-lo, qualquer um. O interruptor apoia a negociação automática da velocidade e duplexação, mas desde que o atraso é tão pequeno esta não seria uma razão desligá-la.
9. Nós igualmente fizemos o teste de ping de uma estação de trabalho ao interruptor. Tomou aproximadamente 5-6 segundos para que a resposta venha do interruptor, se a auto negociação para a velocidade e duplexação era de ligar/desligar.

## [Como reduzir o retardo na inicialização no Switch Catalyst 1900/2800](#)

O 1900/2820 referem Portfast por um outro nome: Início-transmissão de Spantree. Para a versão de software nós somos executado (V8.01.05), o padrão do Switches a este: Portfast é permitido nas portas dos Ethernet (10Mbps), e Portfast é desabilitado nas portas rápidas dos Ethernet (uplink). Assim, quando você **mostrar a corrida** para ver a configuração, se uma porta Ethernet não diz nada sobre Portfast, a seguir Portfast está permitido. Se não diz "nenhuma início-transmissão do spantree" na configuração, Portfast está desabilitado. Em um FastEthernet (100Mbps) mova, o oposto é verdadeiro: Para uma porta FastEthernet, a Portfast está ativada apenas se a porta exibir "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 salvar automaticamente a configuração depois que as mudanças foram feitas. Recorde, você não quereria Portfast permitido em toda a porta que conectar a um outro interruptor ou hub, simplesmente se a porta anexa 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, o Ethernet de interface 0/1 tem o portfast desligado (você pode ver o comando o desligar), os Ethernet de interface 0/2 tem o portfast sobre (você não vê nada - que significa que está ligada), e o FastEthernet 0/26 da relação (mova A no sistema de menu) tem o portfast sobre (você pode ver o comando o girar sobre).

```
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 escolhe (P) para a configuração de porta do menu principal, a seguir escolha uma porta, a saída indica se o modo rápido da porta está permitido. Esta saída é para o FastEthernet 0/26 da porta, que é a porta "A" neste interruptor.

```
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 Menu -----
```

```
----- [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 cronometrando são mais duros de verificar em um 1900/2820 devido à falta das ferramentas para debug, assim que nós apenas começamos um sibilo de um PC conectado ao interruptor dirigido ao interruptor próprio. Nós desligamos e então reconectamos o cabo e gravamos em quanto tempo tomou para que o interruptor responda ao sibilo com o Portfast e com Portfast fora. Para uma porta Ethernet com Portfast sobre (o estado padrão), o PC recebeu uma resposta dentro de **5-6 segundos**. Com Portfast desativado, o PC recebeu uma resposta em 34 a 35 segundos.

## Um benefício adicional ao Portfast

Há outro que mede - árvore - benefício relacionado ao uso de Portfast em sua rede. Todas as vezes um link transforma-se active e move-se para o estado de encaminhamento na medida - a árvore, o interruptor envia um pacote de Spanning Tree especial chamado um Topology Change Notification (TCN). A notificação de TCN é passada até a raiz da medida - a árvore, onde é propagada a todo o Switches no VLAN. Isto faz com que todo o Switches envelheça para fora sua tabela de endereços MAC com o parâmetro de retardo de encaminhamento. O parâmetro de retardo de encaminhamento geralmente é definido como 15 segundos. Cada vez que uma estação de trabalho se junta ao grupo de bridge, os endereços MAC em todo o Switches estão envelhecidos para fora após 15 segundos em vez do normal 300 segundos.

Desde que quando uma estação de trabalho se torna ativa não muda realmente a topologia a qualquer grau significativo tanto quanto todo o Switches no VLAN, é desnecessário para ele ter que atravessar o período de TCN do fast aging. Se você gerencie sobre o portfast, o interruptor não envia pacotes de TCN quando uma porta se torna ativa.

## Os comandos usar-se para verificar a configuração trabalham

Esta é uma lista de comandos usar-se quando você verifica se a configuração trabalha.

### 4000/5000/6000

- show port spantree 2/1 – veja se "Fast-Start" (Portfast) está ativado ou desativado
- show spantree 1 - veja todas as portas no VLAN 1 e se elas têm "Inicialização rápida" habilitada
- show port channel –verifica se você tem qualquer canal ativo
- show port channel 2 – Consulte o modo de canal (automático, desligado e assim por diante) de cada porta do módulo 2
- show trunk 2 – Consulte o modo de entroncamento (automático, desligado e assim por diante) de cada porta do módulo 2
- **show port** - veja o estado (conectado, não-conectado, e assim por diante), velocidade, duplex para todas as portas no interruptor

### 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

- **executar-configuração da mostra** - para considerar as configurações atual (alguns comandos são invisíveis quando representarem as configurações padrão do interruptor)
- Use o sistema de menu à tela de status de porta

## Comandos usar-se para pesquisar defeitos a configuração

Esta é uma lista de comandos usar-se para pesquisar defeitos a 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 no VLAN 1 e se elas têm "Inicialização rápida" habilitada
- show port channel –verifica se você tem qualquer canal ativo
- show port channel 2 – Consulte o modo de canal (automático, desligado e assim por diante) de cada porta do módulo 2
- show trunk 2 – Consulte o modo de entroncamento (automático, desligado e assim por diante) de cada porta do módulo 2
- **show port** - veja o estado (conectado, não-conectado, e faça sobre), velocidade, duplex para todas as portas no interruptor

- **registro da mostra** - veja que tipo de mensagem gerencie saídas de registro
- **ajuste o spantree 7 do nível de registro** - ajusta o interruptor para registrar a porta de Spanning Tree, tempo real dos estados 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)
- **o tempo da mostra** - mostre as horas atual nos segundos (usados no início de um teste de cronometragem)
- **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** - ajuste a porta a 100Mbps e desligue a auto negociação
- **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** - mostre quando a porta se mover com da medida - fases da árvore
- **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)
- **fechado** - para desligar uma porta do software
- **no shut** Para ativar uma porta no software

### 1900/2800

- **executar-configuração da mostra** - para considerar as configurações atual (alguns comandos são invisíveis quando representarem as configurações padrão do interruptor)

## [Configurar e pesquise defeitos o Multi-Layer Switching \(MLS\) IP](#)

### [Objetivos](#)

Este documento esboça o Troubleshooting básico do switching multicamada (MLS) para o IP. Esta característica transformou-se um método muito desejado com que para acelerar o desempenho do roteamento com o uso dos circuitos integrados característicos da aplicação dedicados (ASIC). O roteamento tradicional é feito através de um CPU central e de um software; O MLS offloads uma porção significativa de roteamento (reescrita de pacote de informação) ao hardware e foi denominado igualmente interruptor. MLS e switching de terceira camada são termos equivalentes. O NetFlow feature dos IO é distinto, e não coberto neste documento. O MLS igualmente inclui o apoio para IPX (IPX MLS) e multicasting (MPLS), mas este documento concentra-se exclusivamente no Troubleshooting de IP básico MLS.

### [Introdução](#)

A necessidade por maior desempenho aumenta à medida que demandas maiores são exigidas das redes. Os PC são conectados cada vez mais aos LAN, aos WAN e ao Internet, e seus usuários exigem o acesso rápido aos bases de dados, aos arquivos/Web pages, aos aplicativos

conectados por rede, aos outros PC, e à vídeo fluente. A fim manter conexões rápidas e seguras, as redes devem poder ajustar às mudanças e às falhas e encontrar rapidamente o melhor caminho, tudo quando permanecerem tão invisíveis como possível aos utilizadores 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 este pode ser um processo intensivo de CPU; um aumento de desempenho significativo é ganhado offloading uma parcela desta função ao hardware de switching. Este é o ponto da característica MLS.

Há três componentes principais do MLS: dois deles são o MLS-RP e o MLS-SE. O MLS-RP é o roteador ativado por MLS, que executa a função tradicional do roteamento entre as sub-redes/VLAN. O MLS-SE é um interruptor MLS-permitido, que exige normalmente um roteador distribuir entre as sub-redes/VLAN, mas com hardware especial e software, pode segurar a reescrita 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. A confusão pode elevar aqui, desde que parece que um dispositivo da camada dois está tomando em uma tarefa da camada três; realmente, o interruptor está reescrevendo somente a informação da camada três, e “está comutando” entre as sub-redes/VLAN--o roteador é ainda responsável para cálculos com base em padrões da rota e determinação do melhor caminho. Muita desta confusão puder ser evitada se você mantém mentalmente as funções de roteamento e de switching separadas, especialmente quando, como é geralmente o caso, são contidas dentro do mesmo chassi (que com um mls-rp interno). Pense do MLS como um formulário muito mais avançado da rota que põe em esconderijo, com o esconderijo mantido separa do roteador em um interruptor. 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 através de um cabo a uma porta de tronco no interruptor). Os exemplos de MLS-RP internos são o módulo route-switch (RS) e o Route Switch Feature Card (RSFC), que são instaladas em um entalhe ou em um supervisor de um membro do Catalyst 5xxx Family, respectivamente; o mesmo aplica-se ao Multilayer Switch Feature Card (MSFC) para o Catalyst 6xxx Family. Exemplos de MLS-RPs externos incluem qualquer membro dos Cisco 7500, 7200, 4700, 4500 ou 3600 Series Routers. Geralmente, para apoiar a característica IP MLS, todos os MLS-RP exigem uma Versão do IOS mínima nos trens 11.3WA ou 12.0WA; consulte a documentação de versão para específicos. Também, o **MLS deve ser permitido** para que um roteador seja um MLS-RP.

O MLS-SE é um interruptor com hardware especial. Para um membro do Catalyst 5xxx Family, o MLS exige que o supervisor tem um Netflow Feature Card (NFFC) instalado; o Supervisor IIG e o IIG têm um à revelia. Além disso, um mínimo limitado do software Catalyst OS 4.1.1 também é necessário. Note que o trem 4.x tem “o general deployment (GD) ido,” ou critérios do utilizador final e alvos rigorosos passados da experiência de campo para a estabilidade, assim que verifique a site da Cisco na Web para ver se há as liberações as mais atrasadas. 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). Note que o IPX MLS e MLS para multicasting pode ter exigências diferentes do hardware e software (IO e OS do catalizador). Mais plataformas Cisco suportam/suportarão o recurso MLS. Também, o **MLS deve ser permitido** para que um interruptor seja um MLS-SE.

O terceiro componente principal do MLS é o protocolo multilayer switching (MLSP). Como a compreensão dos fundamentos de MLSP vai ao cerne de MLS e é essencial ao Troubleshooting eficaz de MLS, descreveremos MLSP aqui mais detalhadamente. O MLSP é utilizado pelo MLS-RP e pelo MLS-SE para comunicar-se um com o outro; as tarefas incluem a possibilidade do MLS; instalando, atualizando ou suprimindo de fluxos (informação de cache); e gerenciar e

exportar estatísticas de fluxo (a Exportação de Dados Netflow é discutida 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 manda o Multicast “olá!” pacotes cada 15 segundos com MLSP; Se forem perdidos três desses intervalos, o MLS-SE reconhecerá que o MLS-RP falhou ou que a conectividade com ele foi perdida.

O diagrama ilustra três fundamentos que devem ser terminados (com MLSP) para que um atalho seja criado: o candidato, enabler e etapas pôr em esconderijo. As verificações MLS-SE para uma entrada de MLS posta em esconderijo; se a entrada de cache de MLS e a informação do pacote combinam (uma batida), o encabeçamento do pacote está reescrito localmente no interruptor (um atalho ou um desvio do roteador) em vez do enviado sobre ao roteador como acontece normalmente. Os pacotes que não combinam e são enviados sobre ao MLS-RP são pacotes do candidato; isto é, há uma possibilidade de comutá-los localmente. Depois que passa o pacote do candidato com a máscara de fluxo de MLS (explicada em uma seção mais tarde) e reescreve a informação contida no encabeçamento do pacote (a porção de dados não está tocada), o roteador envia-a para o salto seguinte ao longo do caminho de destino. O pacote é denominado pacote habilitador. Se o pacote retorna ao mesmo MLS-SE de que saiu, um atalho de MLS é criado e colocado no cache MLS; a reescrita para esse pacote e todos os pacotes similares que seguem (chamou um fluxo) é feita agora localmente pelo hardware do interruptor em vez pelo software do roteador. O mesmo MLS-SE deve ver ambos, o pacote candidato e o habilitador em relação a um fluxo específico, para que seja criado um atalho MLS (por isso a topologia de rede é importante para o MLS). Recorde, o ponto do MLS é permitir o trajeto de comunicação entre dois dispositivos nos VLAN diferentes, conectados fora do mesmo interruptor, para contornar o roteador, e aumentam o desempenho da rede.

Pelo uso da máscara de fluxo (essencialmente uma lista de acessos) o administrador pode ajustar o grau de similaridade destes pacotes, e ajusta o espaço dos fluxos: endereço de destino; endereços de destino e de origem; ou informações de destino, de origem e da camada quatro. Note que o primeiro pacote de um fluxo passa sempre através do roteador; é comutado desde então localmente. Cada fluxo é unidirecional; uma comunicação entre PC, por exemplo, exige a instalação e o uso de dois atalhos. O propósito principal do MLSP é setup, criar, e manter estes atalhos.

Estes três componentes (o MLS-RP, o MLS-SE e MLSP) livram acima recursos de roteador vitais permitindo que outros componentes de rede tomem em algumas de suas funções. O dependente em cima da topologia e da configuração, MLS fornece um simples e altamente um método efetivo do desempenho de rede crescente no LAN.

## [Troubleshooting com o IP MLS Technology](#)

Um diagrama de fluxo para o Troubleshooting básico IP MLS é incluído e discutido. É derivado da maioria de tipos comuns de casos MLS-IP abertos com o Web site do Suporte técnico de Cisco e enfrentados por nossos clientes e engenheiros de suporte técnico até o tempo que este documento esteve criado. O MLS é uns recursos robustos, e você deve não ter nenhum problema com ele; se uma edição elevava, esta deve ajudá-lo a resolver os tipos de problemas com MLS que IP você pôde provavelmente enfrentar. Algumas suposições essenciais são feitas:

- Você é familiar com os passos básicos de configuração exigidos para permitir IP MLS no roteador e no Switches, e terminou estas etapas: veja os recursos alistados na extremidade deste documento para o material excelente.



- Roteamento IP é permitido no MLS-RP (está ligada à revelia): se o comando no ip routing aparece na configuração global de uma **corrida da mostra**, esteve desligada, e o IP MLS não funciona.
- A conectividade IP existe entre o MLS-RP e o MLS-SE: **sibile os** endereços IP de Um ou Mais Servidores Cisco ICM NT do roteador do interruptor, e procure os pontos de exclamação (chamados "golpes ") para indicar em retorno.
- As relações MLS-RP estão em um estado do "Up/Up" no roteador: digite show ip interface brief no roteador para confirmar isso.

**aviso:** Sempre que você faz alterações de configuração a um roteador pretendido ser permanente, recorde salvar aquelas mudanças com um **copy running-config starting-config** (versões encurtadas deste **mem do começo** e do **wr da corrida de cópia do** comando include). Todas as modificações de configuração são perdidas se os recarregamentos de roteador ou restauradas. O RS, o RSFC e o MSFC são Roteadores, não Switches. Ao contrário, as mudanças feitas na alerta do interruptor de um Catalyst 5xxx ou o membro da família 6xxx salvar automaticamente.

Esta seção pesquisa defeitos a tecnologia de MLS IP.

1. 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 relações do NON-em tronco, a conexão ao MLS-SE é geralmente através das interfaces de VLAN (como com um RS) ou do entroncamento do apoio (pode ser configurado para levar a informação de vlan múltipla configurando o ISL ou o 802.1q). Também, recorde que, até à data do tempo da publicação, simplesmente os membros do 7500, 7200, 4700, 4500, e famílias do 3600 Router apoiam o MLS externamente. Atualmente, somente estes roteadores externos e o Roteadores que cabem nas famílias do Catalyst 5xxx ou 6xxx Switch (como o RS e o RSFC para o Catalyst 5xxx Family, e o MSFC para o Catalyst 6xxx Family) podem ser MLS-RP. O MSFC requer também o PFC (Placa de Recurso de Política), ambos instalados no Catalyst 6xx Supervisor. O MLS para IP é agora um recurso padrão no software do roteador IOS 12.0 e posterior. O IOS Software mais baixo do que IO 12.0 exige geralmente um trem especial; para tal apoio IP MLS, instale as imagens as mais atrasadas nos IO 11.3 que têm as letras "WA" em seus nomes de arquivo.Para o MLS-SE, um Netflow Feature Card (NFFC) é exigido para um membro do Catalyst 5xxx Family; este cartão é instalado no módulo do supervisor do Catalyst Switch, e incluído como o hardware padrão em uns supervisores mais novos do Catalyst 5xxx Series (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 software que suportam IP MLS sendo lançados, é importante verificar a documentação e as notas de versão e instalar de modo geral a versão mais recente com o menor treinamento para satisfazer 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.Os comandos fundidos para verificar o hardware e software instalado são **versão da mostra no roteador** e **módulo show no interruptor****Nota:** O Catalyst 6xxx Family do Switches não apoia um MLS-RP externo neste tempo. O MLS-RP deve ser um MSFC.



2. Estão os dispositivos de origem e de destino em VLAN diferentes fora do mesmo MLS-SE, compartilhando de uma única terra comum MLS-RP? Esse é um requisito de topologia básico de MLS que o roteador têm um caminho para cada uma das VLANs. Recorde que o ponto do MLS é criar um atalho entre dois VLAN, de modo que o “roteamento” entre os dois dispositivos finais possa ser executado pelo interruptor, assim livrando o roteador para outras tarefas. O interruptor não distribui realmente; reescreve os quadros de modo que pareça aos dispositivos finais que falam através do roteador. Se os dois dispositivos estão no mesmo VLAN, o MLS-SE comuta o quadro localmente sem o uso do MLS, como o Switches faz em tal transparentemente ambiente interligado, e nenhum atalho de MLS é criado. Um pode ter switch múltiplos e Roteadores na rede, e mesmo switch múltiplos ao longo do trajeto do fluxo, mas o trajeto entre os dois dispositivos finais para qual deseja um atalho de MLS deve incluir um único MLS-RP nesse VLAN para esse trajeto. 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 estes critérios não são encontrados, o pacote está distribuído normalmente sem o uso do MLS. Refira os documentos sugeridos na extremidade deste documento para diagramas e discussões com respeito ao apoiado e topologias de rede não suportada.
3. O MLS-RP contém uma instrução `mls rp ip` em sua configuração global e de interface? Se não houver um presente, adicione as instruções `mls rp ip` corretamente 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. **Nota:** Quando você configura o MLS-RP, igualmente recorde colocar o **comando `mls rp management-interface`** sob uma de suas relações IP MLS. Este passo requerido diz o MLS-RP fora de que relação deve enviar a mensagens `mlsp` para se comunicar com o MLS-SE. Mais uma vez, é necessário colocar este comando apenas em uma interface.
4. Existem recursos configurados no MLS-RP que desativam automaticamente o MLS nessa interface? Há diversas opções de configuração no roteador que não são compatíveis com MLS. Isto inclui relatório de IP, criptografia, compressão, segurança de IP, Tradução de endereços de rede (NAT) e Taxa de acesso confirmada (CAR). Para mais informações, refira os links com respeito à configuração de MLS IP incluída na extremidade deste documento. Os pacotes que atravessam uma interface do roteador configurada com qualquer uma das características devem ser distribuídos normalmente; nenhum atalho de MLS é criado. Para que o MLS trabalhe, desabilite estas características na relação MLS-RP. Outra função importante que afeta o MLS é as listas de acesso, de entrada e saída. Um exame mais adicional desta opção é incluído sob “máscaras de fluxo.”
5. O MLS-SE reconhece o endereço de MLS-RP? Para que o MLS funcione, o interruptor deve reconhecer o roteador como um 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-RP externos, um deve explicitamente informar o interruptor do endereço do roteador. Este endereço não é realmente um endereço IP de Um ou Mais Servidores Cisco ICM NT, embora em MLS-RP externos seja escolhido da lista de endereços IP de Um ou Mais Servidores Cisco ICM NT configurados nas relações do roteador; é simplesmente uma identificação do roteador de fato, para MLS-RP internos, o MLS-ID é normalmente nem sequer um endereço IP de Um ou Mais Servidores Cisco ICM NT configurado no roteador;

desde que os MLS-RP internos são incluídos automaticamente, é geralmente um endereço de loopback (127.0.0.x). Para que o MLS funcione, inclua no MLS-SE o MLS-ID encontrado no MLS-RP. Use os **mls rp da mostra no roteador** para encontrar o MLS-ID. Configurar então esse ID no interruptor com o comando do **set mls include <MLS-ID>**. Este é um passo de configuração requerida quando você usa MLS-RP externos. **Nota:** Se você muda o endereço IP de Um ou Mais Servidores Cisco ICM NT do MLS-RP conecta e recarregue então o roteador, ele pode fazer com que o processo MLS no roteador escolha um MLS-ID novo. Este MLS-ID novo pode ser diferente do MLS-ID que foi incluído manualmente no MLS-SE, que pode fazer com que o MLS pare; este é uma não falha de software, mas um efeito do interruptor que tenta comunicar-se com um MLS-ID que seja já não válido. Seja certo incluir este MLS-ID novo no interruptor para que o MLS trabalhe mais uma vez. Pode ser necessário desabilitar/permite IP MLS, também. **Nota:** Quando o MLS-SE não é conectado diretamente ao MLS-RP, como com esta topologia, o endereço que deve ser incluído no MLS-SE pode aparecer enquanto o endereço de loopback mencionou: um interruptor conectou entre o MLS-SE e o MLS-RP. Você deve incluir o MLS-ID mesmo que o MLS-RP seja interno. Ao segundo interruptor, o MLS-RP aparece como um roteador externo desde que o MLS-RP e o MLS-SE não são contidos no mesmo chassi.

6. As interfaces MLS-RP e MLS-SE estão no mesmo domínio habilitado para VTP? O MLS exige que os componentes MLS, incluindo as estações final, devem estar no mesmo domínio do protocolo virtual trunking (VTP). O VTP é um protocolo da camada-dois usado controlando VLAN em diversos Catalyst Switches de um switch central. Permite que um administrador crie ou suprima de um VLAN em todo o Switches em um domínio sem ter que fazer assim em cada interruptor nesse domínio. O protocolo MLSP (Protocolo de Switching Multicamada), utilizado pelo MLS-SE e pelo MLS-RP para se comunicarem entre si, não atravessa um limite de domínio VTP. Se o administrador de rede tem o VTP permitido no Switches (o VTP está permitido em membros do Catalyst e 6xxx Family à revelia), use o **comando show vtp domain no** interruptor aprender em que VTP domain o MLS-SE foi colocado. À exceção do catalizador 6xxx MSFC, em que o MLS é essencialmente uns *recursos de plugue-and-play*, você deve em seguida adicionar o VTP domain a cada um das relações MLS do roteador. Isto permite Multicast MLSP mover-se entre o MLS-RP e o MLS-SE e permite que o MLS funcione. No modo de configuração da interface do MLS-RP, incorpore estes comandos: no mls rp ip Desabilitar MLS na interface MLS-RP afetada antes de modificar o domínio VTP. o **Domain Name do VTP-domínio <VTP rp dos mls >** o Domain Name VTP em cada interface habilitada de MLS devem combinar aquele do interruptor. o **#> do ID de VLAN <VLAN rp dos mls** exigido somente para o entroncamento diferente de ISL, MLS-RP externo conecta. mls rp management-interface Faça isso para apenas uma interface no MLS-RP. Esse passo requerido informa ao MLS-RP de qual interface ele deve enviar as mensagens de MLSP. os **mls rp IP** permitem o MLS mais uma vez na relação do MLS-RP. A fim mudar o Domain Name VTP do MLS-SE, use este comando no interruptor Cactos permitem a alerta: **set vtp domain name <nome do domínio VTP>** Para que o MLS trabalhe, seja certo que o VTP está permitido no interruptor: **set vtp enable**
7. As máscaras de fluxo concordam com MLS-RP e MLS-SE? Uma máscara de fluxo é um filtro configurado por um administrador de rede e usada pelo MLS para determinar se um atalho deve ser criado. Apenas como uma lista de acessos, mais detalhados os critérios que você se estabelece, o mais profundo no pacote o processo MLS deve olhar a fim verificar se o pacote encontra aqueles critérios. A fim ajustar o espaço de atalhos MLS-criados, a máscara de fluxo pode ser feita mais ou menos específica; a máscara de fluxo é essencialmente um dispositivo de *ajustamento*. Há três tipos de modos MLS IP: IP de destino, destination-

source-ip, e full-flow-ip. O modo do IP de destino, o padrão, está no uso quando nenhuma lista de acessos é aplicada à interface habilitada de MLS do roteador. O modo do source-destination-ip está no uso 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 é escolhido, o usuário pode assim configurar o MLS de modo que somente o endereço de destino deva combinar para que um atalho de MLS seja criado, ou fonte e destino, ou mesmo a informação da 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 o source-destination-ip ou os modos MLS do full-flow-ip são julgados para ser exigidos, é o melhor configurar-lo no roteador aplicando a lista de acessos apropriada. O MLS escolhe sempre a máscara a mais específica. Ele dá à máscara de fluxo configurada na precedência de MLS-RP sobre a máscara encontrada no MLS-SE. **SEJA CUIDADOSO** se você muda o modo MLS do interruptor do IP de destino do padrão: você deve certificar-se de que combina o modo MLS no roteador para que o MLS trabalhe. Para o source-destination-ip e os modos do full-flow-ip, recorde aplicar a lista de acessos à interface do roteador apropriada; sem a lista de acessos aplicada, mesmo se configurado, o modo MLS é simplesmente IP de destino, o padrão. **aviso:** Sempre que a máscara de fluxo for alterada, seja no MLS-RP ou no MLS-SE, todos os fluxos de MLS em cache são removidos e o processo de MLS é reiniciado. Uma remoção igualmente pode ocorrer ao aplicar o comando clear ip route-cache no roteador. Se você aplica o comando global router configuration **nenhum Roteamento IP**, que desliga Roteamento IP e transforma essencialmente o roteador em um Transparent Bridge, causa uma remoção e o desabilitação MLS (recorde, distribuindo é uma condição prévia do MLS). Cada um destes pode temporariamente, mas seriamente, desempenho de roteador da influência em uma rede de produção. O roteador experimenta um ponto em sua carga até que os atalhos novos estejam criados porque deve agora segurar todos os fluxos que foram processados previamente pelo interruptor. **Nota:** Especialmente com um membro do Catalyst 5000 Family como o MLS-SE, você deve evitar o uso muito largo das máscaras de fluxo que são configuradas com informação da camada-quatro. Se o roteador é forçado a espreitar tão profundamente em cada pacote na relação, muito dos benefícios pretendidos do MLS está contorneado. Este é muito menos de uma edição quando você usa um membro do Catalyst 6xxx Family como o MLS-SE desde que as portas de switch elas mesmas podem reconhecer a informação da camada-quatro. **Nota:** Até recentemente, o MLS não apoiou máscaras de fluxo configurou de entrada em uma relação MLS-RP, somente de partida. Se você usa o **comando mls rp ip input-acl** além do que comandos configuration normais MLS-RP em uma interface do roteador, uma máscara de fluxo de entrada está apoiada.

8. São mais do que um par MLS Mensagens de Erro *demais dos movimentos* vistos continuamente no interruptor? Como a nota menciona, para mudar uma máscara de fluxo, cancele o cache de rota, ou gire globalmente fora Roteamento IP causa uma remoção do esconderijo. Outras circunstâncias podem igualmente causar completamente ou muitas remoções da única entrada e fazer com que o MLS queixe-se de *movimentos demais*. Há diversas formas desta mensagem, mas cada uma contém estas três palavras. Com exceção do que tem sido mencionado já, a maioria de causa comum deste erro é quando o interruptor aprende o endereço de controle de acesso de mídia (MAC) de Ethernet idêntica múltipla dentro do mesmo VLAN; Os padrões de Ethernet não permitem endereços MAC idênticos dentro do mesmo VLAN. Se visto raramente, ou apenas algumas vezes em seguido, não há nenhum motivo de preocupação; O MLS é uns recursos robustos, e a

mensagem pode simplesmente ser causada por eventos da rede normal, como uma conexão PC que está sendo movida entre portas, por exemplo. Se visto continuamente por diversos minutos, é provável um sintoma de mais questão grave. Quando tal situação elevara, sua causa de raiz é geralmente devido à presença de dois dispositivos com o mesmo MAC address conectado realmente a um VLAN, ou a um laço físico dentro do VLAN (ou dos vlan múltiplos se construindo uma ponte sobre através destes domínios de transmissão). Use o Troubleshooting de Spanning-Tree (coberto em outros documentos) e a ponta para encontrar o laço e para eliminá-lo. Além disso, qualquer alteração rápida na topologia pode causar uma instabilidade temporária na rede (e no MLS), como interfaces do roteador não sincronizadas, uma placa de interface de rede (NIC) inadequada, etc. **Dica:** Use os **comandos show mls notification and show looktable no** interruptor apontá-lo na direção do endereço MAC duplicado ou do laço físico. O primeiro fornece um valor TA. **O value>** do comando show looktable <TA retorna um MAC address possível que possa ser seguido à raiz do problema.

### [Comandos ou capturas de tela](#)

Para descrições e exemplos detalhados do roteador de MLS e dos comandos switch IP, refira a documentação alistada sob a [informação relacionada](#)