

Troubleshooting de Portas de Switches e Interfaces

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Troubleshooting da Camada Física](#)

[Uso do LED para Resolver Problemas](#)

[Verificar o Cabo e os Dois Lados da Conexão](#)

[Cabos de Ethernet de Fibra Óptica e Cobre](#)

[Troubleshooting de Ethernet de Gigabit](#)

[Conectado vs Não Conectado](#)

[Os Comandos Mais Comuns de Troubleshooting de Interface e Porta para CatOS e Cisco IOS](#)

[Como Compreender a Saída do Contador Específico de Interface e Porta para CatOS e Cisco IOS](#)

[Show Port para CatOS e Show Interfaces para Cisco IOS](#)

[Contadores Show Mac para CatOS e Show Interfaces para o Cisco IOS](#)

[Show Counters para CatOS e Interface de Show Counters para o Cisco IOS](#)

[Show Controller Ethernet-Controller para Cisco IOS](#)

[Show Top para CatOS](#)

[Mensagens de Erro de Sistema Comuns](#)

[Mensagens de Erro nos Módulos WS-X6348](#)

[%%PAGP-5-PORTTO/FROMSTP e %ETHC-5-PORTTO/FROMSTP](#)

[%SPANTREE-3-PORTDEL_FAILNOTFOUND](#)

[%SYS-4-PORT_GBICBADEEPROM: //%SYS-4-PORT_GBICNOTSUPP](#)

[%AMDP2_FE-3-UNDERFLO](#)

[%INTR_MGR-DFC1-3-INTR: Mecanismo de Enfileiramento \(Blackwater\) \[1\]: FIC Fabric-A Recebeu Código de Controle Inesperado](#)

[Comando Rejeitado: \[\[Interface\] not a Switching Port](#)

[Problemas Comuns da Porta e da Interface](#)

[O Status da Interface ou da Porta é Desabilitada ou Encerrada](#)

[O Status da Porta ou da Interface é errDisable](#)

[O Status da Porta ou da Interface é Inativa](#)

[O Status da Interface ou da Porta de Uplink é Inativa](#)

[O Contador Adiado da Interface de Switch do Catalyst Começa a Incrementar](#)

[Falha intermitente para ajustar o \[value\] do temporizador da vlan \[vlan no\]](#)

[Incompatibilidade do Modo de Entroncamento](#)

[Jumbos, Giants, e Baby Giants](#)

[Não foi Possível Efetuar Ping no Dispositivo Final](#)

[Como Usar Set Port Host ou Switchport Host para Fixar Atrasos de Inicialização](#)

[Problemas de Velocidade/Duplex, Autonegociação ou Placa de Rede](#)

[Loops de Spanning Tree](#)

[UDLD: Link de Sentido Único](#)

[Frames Adiados \(Out-Lost or Out-Discard\)](#)

[Problemas de Software](#)

[Problemas de Hardware](#)

[Erros de Entrada em uma Interface da Camada 3 Conectada a um Switchport da Camada 2](#)

[Incrementação Rápida de Erros de Entrada e do Contador Rx-No-Pkt-Buff](#)

[Compreenda gotas do protocolo desconhecido](#)

[Entroncamento entre um Switch e um Roteador](#)

[Problemas de Conectividade Devido à Sobreassinatura](#)

[Subinterfaces nos Módulos SPA](#)

[Troubleshooting de rxTotalDrops](#)

[Pesquise defeitos quedas de emissor](#)

[Última entrada nunca da saída do comando show interface](#)

[Informações Relacionadas](#)

Introdução

Este documento foi criado para ajudar a determinar por que uma porta ou interface apresenta problemas. Este documento aplica-se aos switches do Catalyst Switches que executam o CatOS Software no Supervisor ou o Cisco IOS® System Software no Supervisor.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Convenções

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

Troubleshooting da Camada Física

Uso do LED para Resolver Problemas

Se você tem acesso físico ao switch, pode economizar tempo verificando os LEDs da porta, que fornecem o status do link ou podem indicar uma condição de erro (se forem vermelho ou laranja). A tabela descreve os indicadores do status do LED para os módulos de Ethernet ou switches de configuração fixa:

Plataforma	URL
Catalyst 6000 Series Switches	LEDs de Módulo Ethernet
Catalyst 5000 Series Switches	LEDs de Módulo Ethernet
Catalyst 4000 Series Switches	LEDs de Módulo Ethernet
Catalyst 3750 Series Switches	LEDs do painel dianteiro
Catalyst 3550 Series Switches	LEDs do painel dianteiro
Catalyst 2950/2955 Series Switches	LEDs do painel dianteiro
Catalyst 2900/3500XL Series Switches	LEDs do painel dianteiro
Catalyst 1900 e 2820 Series Switches	LEDs do painel dianteiro
Catalyst G-L3 Series Switches	LEDs do painel dianteiro

Assegure-se de que os dois lados tenham um link. Um único fio quebrado ou uma porta fechada pode causar o problema onde um lado tem uma luz de link, mas o outro lado não.

Uma luz de link não garante que o cabo esteja funcionando adequadamente. O cabo pode ter passado por um estresse físico que faz com que seja funcional a um nível marginal. Normalmente, você pode identificar esta situação se a porta tiver muitos erros de pacote ou se a porta oscila constantemente (perde e recupera o link).

[Verificar o Cabo e os Dois Lados da Conexão](#)

Se a luz de link para a porta não acende, você pode considerar estas possibilidades:

Possível causa	Ação corretiva
Não existe nenhum cabo conectado	Conecte o cabo do switch a um dispositivo em bom funcionamento.
Porta Errada	Assegure-se de que ambas as extremidades do cabo estejam ligadas nas portas corretas.

O dispositivo não tem energia	Assegure-se de que os dois dispositivos tenham energia.
Tipo de cabo errado	Verifique a seleção do cabo. Consulte o Guia de Cabo de Switch do Catalyst .
Cabo incorreto	Troque o cabo suspeito por um cabo em bom funcionamento. Procure por pinos quebrados ou faltantes nos conectores.
Conexões soltas	Verifique se existem conexões soltas. Às vezes, parece que um cabo está colocado na tomada, mas não está. Desconecte o cabo e reintroduza-o.
Painéis de Correção	Elimine conexões defeituosas do painel de correção. Evite o painel de correção, se possível, para excluí-lo.
Conversores de Mídia	Elimine conversores de mídia defeituosos: de fibra ótica para cobre, etc. Evite o conversor de mídia, se possível, para excluí-lo.
Conversor com erro com falha do Gigabit Interface Converter (GBIC)	Troque o GBIC suspeito por um GBIC em bom funcionamento. Verifique o suporte de Hardware e Software para este tipo de GBIC. Consulte a seção de Troubleshooting de Ethernet de Gigabit deste documento.
Porta ou Porta do Módulo com erro ou Interface ou	Mova o cabo para uma porta em bom funcionamento para resolver o problema de uma porta ou de um módulo suspeito. Use o comando show port para CatOS ou o comando show interface para que o Cisco IOS procure o status errdisable, disable ou shutdown. O comando show module pode indicar falha, que pode indicar um problema de hardware. Consulte a seção Problemas Comuns da Porta e da Interface deste documento para obter mais

Módulo não habilitado	informações.
-----------------------	--------------

Cabos de Ethernet de Fibra Óptica e Cobre

Verifique se você tem o cabo correto para o tipo de conexão que está fazendo. O cabo de cobre da categoria 3 pode ser usado para conexões de par trançado não blindado (UTP) de 10 Mbps, mas nunca deve ser usado para conexões UTP de 10/100 ou de 10/100 /1000 Mbps. Use sempre UTP de Categoria 5, Categoria 5e ou Categoria 6 conexões para de 10/100 ou de 10/100/1000 Mbps.

aviso: Os cabos da Categoria 5e e 6 podem armazenar níveis altos de eletricidade estática devido às propriedades dielétricas dos materiais usados em sua construção. Sempre aterre os cabos (especialmente em execuções com cabos novos) a uma base terra segura apropriada antes de conectá-los ao módulo.

Para a fibra óptica, assegure-se de ter o cabo correto para as distâncias envolvidas e o tipo de portas de fibra que são usadas. As duas opções são o singlemode fiber (SMF) ou a multimode fiber (MMF). Assegure-se de que ambas as portas nos dispositivos que estão conectadas sejam SMF ou portas MMF.

Nota: Para conexões de fibra óptica, assegure-se de que a transmissão de transmissão de uma porta esteja conectada à recepção de recepção da outra porta. As conexões de transmissão à transmissão e de recepção à recepção não funcionam.

Distâncias Máxima de Transmissão de Fast Ethernet e Ethernet

Velocidade do Transceptor	Tipo de cabo	Modo Duplex	Distância máxima entre estações
10 Mbps	Categoria 3 UTP	Full e semi	328 pés (100 m)
10 Mbps	MMF	Full e semi	1,2 mi (2 quilômetros)
100 Mbps	UTP Categoria 5, UTP Categoria 5e	Full e semi	328 pés (100 m)
100 Mbps	Categoria 6 UTP	Full e semi	328 pés (100 m)
100 Mbps	MMF	Half	1312 pés (400 m)
		Completo	1,2 mi (2 quilômetros)
100 Mbps	S F	Half	1312 pés (400 m)
		Completo	6,2 mi (10 quilômetros)

Para obter mais detalhes sobre os tipos de cabo/conectores diferentes, os requisitos de cabeamento, os requerimentos ópticos (distância, tipo, cabos de correção, etc.), como conectar os cabos diferentes e quais cabos são usados pela maioria dos switches e módulos Cisco, consulte o [Guia de Cabo de Switch do Catalyst](#).

Troubleshooting de Ethernet de Gigabit

Se você tem o dispositivo A conectado ao dispositivo B em um link de Gigabit e o link não funciona, acima, executa o procedimento a seguir.

Procedimento Passo a Passo

1. Verifique se o dispositivo A e o B usam o mesmo GBIC, comprimento de onda curto (SX), comprimento de onda longo (LX), longo alcance (LH), comprimento de onda estendido (ZX) ou cobre UTP (TX). Os dois dispositivos devem usar o mesmo tipo de GBIC para estabelecer o link. Um SX GBIC precisa conectar-se a um SX GBIC. Um SX GBIC não se conecta a um LX GBIC. Consulte [Nota de Instalação do Cabo de Correção de Condicionamento de Modo](#) para obter mais informações.
2. Verifique a distância e o cabo usados pelo GBIC como definido nesta tabela. **Especificações de Cabeamento das Portas 1000BASE-T e 1000BASE-XOs** números fornecidos para o cabo de fibra óptica multimodo referem-se ao diâmetro central. Para um cabo de fibra óptica de modo único, 8,3 microns refere-se ao diâmetro central. Os valores 9 microns e de 10 microns referem-se ao diâmetro de campo de (Microfarad), que é o diâmetro da parte da fibra que propaga a luz. Essa área consiste no núcleo da fibra mais uma parte pequena do revestimento circundante. O Microfarad é uma função do diâmetro central, o comprimento de onda do laser e da diferença do índice refrativo entre o núcleo e o revestimento. As distâncias têm por base a perda de fibra óptica. Várias talas e o cabo de fibra óptica de qualidade inferior reduzem as distâncias de cabeamento. Use somente com MMF. Quando você usa um LX/LH GBIC com um MMF de 62,5 microns de diâmetro, precisa instalar um cabo de correção de condição de modo (CAB-GELX-625 ou equivalente) entre os cabos GBIC e MMF nas duas extremidades de recepção e transmissão. O cabo de correção de condição de modo é exigido para distâncias de link menos de 328 pés (100 m) ou maiores que 984 pés (300 m). O cabo de correção de condição de modo impede a ultrapassagem do receptor em comprimentos pequenos de MMF e reduz o atraso de modo diferencial para comprimentos longos do MMF. Consulte [Nota de Instalação do Cabo de Correção de Condicionamento de Modo](#) para obter mais informações. Use somente com SMF. Cabo de fibra óptica do modo único de dispersão deslocada. A distância de link mínima para ZX GBIC é 6,2 milhas (10 quilômetros) com um atenuador de 8 dB instalado em cada extremidade do link. Sem atenuadores, a distância de link mínima é de 24,9 milhas (40 quilômetros).
3. Se um dos dispositivos tiver várias portas de Gigabit, conecte-as. Isso testará cada dispositivo e verificará se a interface de Gigabit está funcionando corretamente. Por exemplo, você tem um switch que tem duas portas de Gigabit. Conecte via cabo a porta de Gigabit um à porta de Gigabit dois. O link funciona? Em caso afirmativo, a porta está funcionando. O STP bloqueia a porta e impede todos os loops (a recepção (RX) da porta um vai para a transmissão (TX) da porta dois; o TX da porta um vai para o RX da porta dois).
4. Se a conexão única ou Passo 3 falham com conectores SC, faça um loop da porta de volta para ela mesma (RX da porta um vai para TX da porta um). A porta funciona? Se não, entre em contato com o TAC, porque a porta pode estar com defeito.

5. Se os passos 3 e 4 forem bem sucedidos, mas uma conexão entre os dispositivos A e B não pode ser estabelecida, faça loops nas portas com o cabo que une os dois dispositivos. Verifique se não há um cabo com falha.
6. Verifique se cada um dos dispositivos oferece suporte para a especificação de 802,3 z para a negociação automática de Gigabit. A Ethernet de Gigabit possui um procedimento de negociação automática que é mais extensivo que aquele usado pela Ethernet 10/100 (especificação de negociação automática de Gigabit: Instituto de Engenharia Elétrica e Eletrônica (Institute of Electrical and Electronics Engineers) STD 802.3z-1998). Quando você habilita a negociação de link, o sistema negocia automaticamente o controle de fluxo, o modo duplex e a informação de falha remota. Você deve habilitar ou desabilitar a negociação de enlace nas duas extremidades do enlace. As duas extremidades do link devem ser ajustadas para o mesmo valor ou o link não poderá se conectar. Foram encontrados problemas em conexões com dispositivos manufaturados antes da ratificação dos padrões do IEEE 802.3z (Instituto de Engenharia Elétrica e Eletrônica). Se um ou outro dispositivo não oferece suporte para a negociação automática de Gigabit, desabilite-a e force a ativação por link. O firmware da placa demora 300 msec para notificar o software que um link/porta de 10/100/1000BASE-TX está inativo. O temporizador do debounce padrão de 300msec vem do temporizador de polling do firmware para as placas de linha, que ocorre cada 300 milissegundos. Se o link for executado no modo 1G (1000BASE-TX), a sincronização de Gigabit, que ocorre cada 10 msec, deve poder detectar que o link está desativado mais rapidamente. Há uma diferença no tempo de detecção da falha do link em que você executa o GigabitEthernet no cobre em comparação à execução do GigabitEthernet em Fibra. Essa diferença no tempo de detecção tem por base os padrões de Instituto de Engenharia Elétrica e Eletrônica (Institute of Electrical and Electronics Engineers). **aviso:** A negociação automática de desabilitação esconde quedas de link ou problemas da camada física. A negociação automática de desabilitação é exigida somente se os dispositivos finais como as placas de rede de Gigabit anteriores que não oferecem suporte para Instituto de Engenharia Elétrica e Eletrônica (Institute of Electrical and Electronics Engineers) 802.3Z forem usados. Não desabilite a negociação automática entre switches a menos que seja absolutamente exigido, já que os problemas da camada física podem passar sem serem detectados, resultando em loops STP. A alternativa é entrar em contato com o fornecedor para obter o software/upgrade de hardware que ofereça suporte para a negociação automática de Gigabit do Instituto de Engenharia Elétrica e Eletrônica (Institute of Electrical and Electronics Engineers) 802.3Z.

Para fazer o troubleshooting da mensagem de erro: %SYS-4-PORT_GBICBADEEPROM: !%SYS-4-PORT_GBICNOTSUPP, consulte [Mensagens de Erro CatOS no Catalyst 6000/6500 Series Switches](#).

Para os requisitos de sistema do GigabitEthernet, assim como para Conversores de Interface de Gigabit (GBICs), os requisitos de sistema de Coarse Wavelength Division Multiplexing (CWDM) e Small Form-Factor Pluggable (SFP), consulte:

- [Requisitos do sistema para implementar Gigabit Ethernet em Switches Catalyst](#)
- [Matriz de compatibilidade de Switch de conversor de interface Gigabit Catalyst GigaStack](#)
- [Matriz de Compatibilidade dos Módulos de Transceptor de Ethernet de Gigabit Cisco](#)
- [Matriz de compatibilidade dos módulos do Transceivers Ethernet de Cisco 10-Gigabit](#)
- [Documentação de GBIC, SFP e CWDM](#)

Para a configuração geral e as informações de Troubleshooting, consulte [Configurar e Fazer o](#)

Conectado vs Não Conectado

O padrão da maioria dos switches Cisco é possuir uma porta no estado não conectado. Isso significa que não está conectado atualmente a nenhum dispositivo, mas que se conectará se houver uma boa conexão para outro dispositivo operacional. Se você conectar um cabo em boas condições a duas portas de switch no estado não conectado, a luz de link ficará verde para ambas as portas, e o status da porta deve indicar conectado. Isso significa que a porta estará ativa contanto que a Camada 1 (L1) esteja conectada.

Para CatOS, você pode usar o [comando show port](#) para verificar se a porta tem um status conectado ou não-conectado ou se é algum outro estado que provocaria falha na conectividade, como **disabled** ou **errdisable**.

```
Switch> (enable) sh port status 3/1 Port Name Status Vlan Duplex Speed Type -----  
-----  
3/1 disabled 1 auto auto 10/100BaseTX !--  
- The show port status {mod/port} command show the port is disabled. !--- Use the set port  
enable {mod/port}command to try and re-enable it.
```

Para o Cisco IOS, você pode usar o [comando show interfaces](#) para verificar se a quando a interface está "ativa, o protocolo de linha está ativo (conectado)". O primeiro "ativo" refere-se ao status da camada física da interface. A mensagem de "protocolo de linha ativo" mostra o status da camada de link de dados da interface e informa que a interface pode enviar e receber keepalives.

```
Router#show interfaces fastEthernet 6/1 FastEthernet6/1 is down, line protocol is down  
(notconnect) !--- The interface is down and line protocol is down. !--- Reasons: In this case,  
!--- 1) A cable is not properly connected or not connected at all to this port. !--- 2) The  
connected cable is faulty. !--- 3) Other end of the cable is not connected to an active port or  
device. !--- Note: For gigabit connections, GBICs need to be matched on each !--- side of the  
connection. !--- There are different types of GBICs, depending on the cable and !--- distances  
involved: short wavelength (SX), !--- long-wavelength/long-haul (LX/LH) and extended distance  
(ZX). !--- An SX GBIC needs to connect with an SX GBIC; !--- an SX GBIC does not link with an LX  
GBIC. Also, some gigabit !--- connections require conditioning cables, !--- depending on the  
lengths involved. Router#show interfaces fastEthernet 6/1 FastEthernet6/1 is up, line protocol  
is down (notconnect) !--- The interface is up (or not in a shutdown state), but line protocol  
down. !--- Reason: In this case, the device on the other side of the wire is a !--- CatOS switch  
with its port disabled. Router#sh interfaces fas 6/1 status Port Name Status Vlan Duplex Speed  
Type Fa6/1 notconnect 1 auto auto 10/100BaseTX !--- The show interfaces card-type [slot/port]  
status command is the equivalent !--- of show port status for CatOS.
```

Se **show port** indicar conectado ou **show interfaces** indicar protocolo de linha/ativo (conectado), mas você verificar que os erros estão aumentando na saída de qualquer um dos comandos, consulte as seções Como Compreender a Saída do Contador de Interface e Porta Especifico para CatOS ou Cisco IOS ou Problemas de Interface e Porta Comum deste documento para obter ajuda do troubleshooting.

Os Comandos Mais Comuns de Troubleshooting de Interface e Porta para CatOS e Cisco IOS

Esta tabela mostra os comandos mais comuns usados para troubleshooting de problemas de porta ou interface nos switches que executam o CatOS Software no Supervisor ou no Cisco IOS System Software no Supervisor.

Nota: Escolha um comando na coluna da esquerda para acessar a documentação para esse comando. A coluna da direita oferece uma breve descrição do que o comando faz e lista todas

quaisquer exceções de uso por plataforma.

Esses comandos são suportados pela ferramenta Output Interpreter para CatOS e podem ser usados para ajudar no troubleshooting de porta ou problemas de switch: [show version](#), [show module](#), [show port](#), [show counters](#) ou [show mac](#).

Se você tem a saída dos comandos suportados de seu dispositivo Cisco, você pode usar isso para exibir problemas e correções potenciais. Para usar o Output Interpreter, você deve ser um usuário registrado, estar conectado e ter o JavaScript ativado.

Comandos de CatOS	Comandos do Cisco IOS	Descrição
show version	show version	Para os switches que executam CatOS, esse comando exibe as informações de versão de software e de hardware por módulo e tamanhos de memória do sistema. Para os switches que executam o Cisco IOS, esse comando exibe saída similar a um roteador Cisco, como informações de nome da imagem e versão de software e de tamanhos de da memória do sistema. Útil na pesquisa por incompatibilidades de software/hardware (com Notas de Release ou Software Advisor) e bugs (com Software Bug Toolkit). Para obter mais informações sobre o comando show version , consulte a seção Problemas de Software deste documento
show module	show module	Para o Catalyst 6000, 5000, 4000 e outros switches modulares que executam CatOS ou Cisco IOS, este comando exibe quais placas estão presentes no switch, a versão de software que estão executando e em qual estado os módulos estão em: ok, com falha, etc. Úteis em diagnosticar um problema de hardware em um módulo ou porta. Para obter mais informações sobre troubleshooting de problemas de hardware com o comando show module , verifique se o Status da Porta ou da Interface está desabilitado ou inativo ou as seções de Problemas de Hardware neste documento.
show	show that	Para CatOS, esse comando indica as

confi g	run- config	<p>definições da configuração não padrão do switch (todas as alterações feitas na configuração padrão). Todas as alterações de configuração em CatOS são salvas automaticamente. Para o Cisco IOS, esse comando indica o arquivo de configuração atual do switch. As alterações são salvas na configuração no Cisco IOS com o comando write memory. Útil para determinar se um erro de configuração incorreta de módulo/porta ou interface pode causar um problema.</p>
show port	show interface s	<p>Para CatOS, o comando show port mostra se a porta está conectada, em qual VLAN ela está, em que velocidade/duplex ela é executada, informações de canal, erros etc. Para o Cisco IOS, o comando show interfaces exibe o status operacional e administrativo de uma porta de switching, de pacotes de entrada e saída, de falhas de buffer, de erros, etc. A saída desses dois comandos é discutida em mais detalhes na seção Como Compreender a Saída do Contador de Porta e Interface para CatOS e Cisco IOS deste documento.</p>
clear count ers	clear counters	<p>Para CatOS e Cisco IOS use o comando clear counters para zerar os contadores de tráfego e erro para que você possa ver se o problema é apenas temporário ou se os contadores continuam a incrementar. Nota: O switch da série Catalyst 6500/6000 não apaga os contadores de bits de uma interface com o comando clear counters. A única maneira de apagar os contadores de bits nesses switches é recarregar.</p>
show port count ers	show interface s counters	<p>Para CatOS, o comando show port <mod/port> indica os contadores de erro de porta, como FCS, alinhamentos, colisões, etc. Para o Cisco IOS no Catalyst 6000, 4000, 3550, 2950, e na série 3750, o comando equivalente é show interfaces card-type x/y counters errors. A saída desses dois comandos é discutida em mais detalhes na seção Como Compreender a Saída do Contador de Porta e Interface para CatOS e Cisco</p>

		IOS deste documento.
show counters	show counters interface show controller s ethernet-controller	Para CatOS, o comando show counters indica os contadores de hardware de 64 bits e de 32 bits para um módulo/porta ou interface específicos. Os contadores variam do tipo de módulo e da plataforma. Para o Cisco IOS, o comando show counters interface foi introduzido na versão de software 12.1(13)E apenas para a série Catalyst 6000 e é o equivalente do comando show counters para CatOS que indica contadores de erros de 32 bits e 64 bits. Para os switches da série Cisco IOS em 2900/3500XL, 2950/2955, 3550, 2970 e 3750, o comando show controllers ethernet-controller é similar ao comando show counters nas plataformas CatOS. Exibe frames descartados, frames adiados, erros de alinhamento, colisões, etc.
show mac	show interface s counters	Para CatOS, o comando show mac exibe os contadores MAC para o tráfego que passa através de cada porta como, frames recebidos, frames transmitidos, perdidos externos, perdidos internos, etc. (Este comando não lista os endereços MAC identificados em uma porta pelo software de bridging. Use o comando show cam dynamic para essas informações.) Para o Cisco IOS, o comando show interfaces card-type x/y counters é similar ao show mac para as plataformas CatOS. A saída desses dois comandos é discutida em mais detalhes na seção Como Compreender a Saída do Contador de Porta e Interface para CatOS e Cisco IOS deste documento.
show test	show diagnostic show post	Para CatOS, o comando show test exibe qualquer erro de hardware encontrado na inicialização. Para Cisco IOS, o comando equivalente é o show diagnostic que foi introduzido em 12.1(11b)E para a série Catalyst 6000 e show diagnostics (com um s) que foi introduzido na Série Catalyst 4000. Os dois comandos exibem os resultados de Power-On Self Test (POST). Para o Cisco IOS no 2900/3500XL, 2950/2955, 3550, 2970 e 3750 Series

		Switch, o comando equivalente são show post que exibe os resultados do POST do switch. Para obter mais informações sobre os erros relacionados ao troubleshooting de erros de hardware nos Switches do Catalyst, consulte a seção Problemas de Hardware deste documento.
--	--	--

[Como Compreender a Saída do Contador Específico de Interface e Porta para CatOS e Cisco IOS](#)

A maioria dos switches possuem alguma forma de rastrear os pacotes e os erros que ocorrem em uma porta ou interface. Os comandos comuns usados para encontrar esse tipo de informação são descritos na seção [Comandos de Troubleshooting Mais Comuns de Porta e Interface para CatOS e Cisco IOS](#) deste documento.

Nota: Pode haver diferenças na implementação dos contadores através das várias plataformas e releases. Embora os valores dos contadores sejam altamente exatos, não são muito precisos por design. Para obter as estatísticas exatas de tráfego, sugerimos que você use um sniffer para monitorar as interfaces de entrada e de saída necessárias.

Os erros excessivos em certos contadores, geralmente, indicam um problema. Quando você uma configuração half-duplex, alguns erros de link de dados que em Frame Check Sequence (FCS), alinhamento, runts e nos contadores de colisão são normais. Geralmente, uma proporção de um por cento dos erros no tráfego total é aceitável para conexões half-duplex. Se a razão entre erros nos pacotes de entrada seja superior a dois ou três por cento, poderá ser notada uma degradação de desempenho.

Nos ambientes half-duplex, é possível que o switch e o dispositivo conectado detectem o fio e transmitam exatamente no mesmo tempo e resultado em uma colisão. As colisões podem causar runts, FCS e erros de alinhamento devido ao frame que não está sendo totalmente para o fio, resultando em frames fragmentados.

Quando você se opera em full duplex, os erros em FCS, Verificação de Redundância Cíclica (CRC), alinhamento e contadores de runt devem ser mínimos. Se o link opera em full duplex, o contador de colisão não está ativo. Se o FCS, a Verificação de Redundância Cíclica (CRC), o alinhamento ou os contadores de runt incrementam, verifique se existe uma incompatibilidade de duplex. A incompatibilidade duplex é uma situação onde o switch opera em full duplex e o dispositivo conectado opera em half-duplex ou vice versa. O resultado de uma incompatibilidade duplex é o desempenho extremamente fraco, a conectividade intermitente e a perda de conexão. Outras causas possíveis de erros de link de dados em full duplex são cabos ruins, portas de switches com falha ou problemas de software/hardware de placa de rede. Consulte a seção [Problemas Comuns da Porta e da Interface](#) deste documento para obter mais informações.

[Show Port para CatOS e Show Interfaces para Cisco IOS](#)

O comando {mod/port} **show port** é usado quando a execução ocorre em CatOS no Supervisor. Uma alternativa a este comando é o {mod/port} [show port counters](#) que exibe somente os contadores de erro de porta. Consulte a [Tabela 1](#) para obter explicações sobre a saída do contador de erros.

```
Switch> (enable) sh port counters 3/1
```

Port	Align-Err	FCS-Err	Xmit-Err	Rcv-Err	UnderSize
3/1	0	0	0	0	0

Port	Single-Col	Multi-Coll	Late-Coll	Excess-Col	Carri-Sen	Runts	Giants
3/1	0	0	0	0	0	0	0

O comando **show interfaces card-type {slot/port}** é o comando equivalente para o Cisco IOS no Supervisor. Uma alternativa a esse comando (para os switches do Catalyst 6000, 4000, 3550, 2970 2950/2955 e 3750 Series) é o comando [show interfaces card-type {slot/port} counter erros](#) que exibe somente os contadores do erro de interface.

Nota: Para os switches das Séries 2900/3500XL use o comando **show interfaces card-type {slot/port}** com o [comando show controllers Ethernet-controller command](#).

```
Router#sh interfaces fastEthernet 6/1 FastEthernet6/1 is up, line protocol is up (connected)
Hardware is C6k 100Mb 802.3, address is 0009.11f3.8848 (bia 0009.11f3.8848) MTU 1500 bytes, BW
100000 Kbit, DLY 100 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA,
loopback not set Full-duplex, 100Mb/s input flow-control is off, output flow-control is off ARP
type: ARPA, ARP Timeout 04:00:00 Last input 00:00:14, output 00:00:36, output hang never Last
clearing of "show interface" counters never Input queue: 0/2000/0/0 (size/max/drops/flushes);
Total output drops: 0 Queueing strategy: fifo Output queue :0/40 (size/max) 5 minute input rate
0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec
```

A saída comando **show interfaces** até este ponto é explicada aqui (em ordem):

- ativo, o protocolo de linha está ativo (conectado) - o primeiro "ativo" refere-se ao status da camada física da interface. A mensagem de "protocolo de linha ativo" mostra o status da camada de link de dados da interface e informa que a interface pode enviar e receber keepalives.
- MTU - A unidade de transmissão máxima (MTU) é 1500 bytes para Ethernet à revelia (para a porção de dados máxima do quadro).
- Full duplex, 100Mb/s - Full duplex e 100 Mbps são a configuração atual da velocidade e do duplex da interface. Não indica se a negociação automática foi usada para atingir isso. Use o **comando show interfaces fas 6/1 status** para exibir o seguinte:

```
Router#sh interfaces fas 6/1
status Port Name Status Vlan Duplex Speed Type Fa6/1 connected 1 a-full a-100 10/100BaseTX
!--- Autonegotiation was used to achieve full-duplex and 100Mbps.
```
- Última entrada, saída - O número de horas, minutos e segundos desde que o último pacote foi recebido ou transmitido com sucesso pela interface. Isso é útil para saber quando uma interface inoperante falhou.
- A última limpeza dos contadores de "show interface" – a última vez que o **comando clear counters** foi emitido desde a última vez que o Switch foi reinicializado. O **comando clear counters** é usado reinicializar estatísticas de interface.**Nota:** Variáveis que podem afetar o roteamento (por exemplo, carga e confiabilidade) não são eliminadas quando os contadores são zerados.
- Fila de entrada - O número de pacotes na fila de entrada. **Tamanho/máximo/descarte** = o número atual de frames na fila / o número máximo de frames que a fila pode conter antes de começar a descartar frames / o número real de frames descartados porque o tamanho máximo da fila foi excedido. **Liberações** são usadas para contar os descartes de Selective Packet Discard (SPD) no Catalyst 6000 Series que executa Cisco IOS. (O contador de liberações pode ser usado, mas nunca incrementa no Catalyst 4000 Series que executa o Cisco IOS.) o SPD é um mecanismo que descarta rapidamente pacotes de baixa prioridade

quando a Unidade Central de Processamento está sobrecarregada a fim de salvar alguma capacidade de processamento para pacotes de alta prioridade. O contador de liberações na saída do comando `show interface` é aumentado como parte do descarte seletivo de pacotes (SPD) que implementa uma política de descarte de pacote seletivo na fila do processo IP do roteador. Conseqüentemente, aplica-se somente ao tráfego de processo comutado. A finalidade do SPD é assegurar que os pacotes de controle importantes, tais como atualizações de roteamento e keepalives, não sejam descartados quando a fila de entrada IP estiver completa. Quando o tamanho da fila de entrada IP estiver entre os limites mínimo e máximo, os pacotes IP normais serão descartados com base em uma probabilidade específica de descarte. Essas quedas aleatórias são chamadas de descargas de SPD.

- Quedas totais de saída é o número de pacotes que foram descartados porque a fila da saída está cheia. Uma causa comum desse erro é o tráfego de um enlace de largura de banda alta ser comutado para um enlace de largura de banda mais baixa ou o tráfego de vários enlaces de entrada ser comutado para um único enlace de saída. Por exemplo, se uma quantidade grande de tráfego intermitente chegar em uma interface gigabit e for comutada para uma interface de 100 Mbps, isso poderá causar cancelamentos de saída para aumentar a interface de 100 Mbps. Isso ocorre porque a fila de saída nessa interface está sobrecarregada pelo excesso de tráfego devido à incompatibilidade de velocidade entre as larguras de banda de entrada e de saída.
- Fila de saída - O número de pacotes na fila de saída. Tamanho/máximo significa o número atual de quadros na fila/no número máximo de quadros que a fila pode conter antes de ficar cheia e ter que parar de derrubar quadros.
- 5 minute input/output rate - A taxa média de entrada e saída vista pela interface nos últimos cinco minutos. Para obter uma leitura mais precisa especificando um período de tempo mais curto (para detectar melhor intermitências de tráfego, por exemplo), use o comando de interface `load-interval <seconds>` .

O restante do comando `show interfaces` exibe a saída do contador de erros que é similar ou equivalente à saída do contador de erros de CatOS. Consulte a [Tabela 1](#) para obter explicações sobre a saída do contador de erros.

```
!--- ...show interfaces command output continues. 1117058 packets input, 78283238 bytes, 0 no
buffer Received 1117035 broadcasts, 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0
frame, 0 overrun, 0 ignored 0 watchdog, 0 multicast, 0 pause input 0 input packets with dribble
condition detected 285811 packets output, 27449284 bytes, 0 underruns 0 output errors, 0
collisions, 2 interface resets 0 babbles, 0 late collision, 0 deferred 0 lost carrier, 0 no
carrier 0 output buffer failures, 0 output buffers swapped out
```

Nota: Há uma diferença entre o contador da saída do comando `show interface` para uma interface física e uma interface de VLAN. Os contadores de pacote da entrada incrementam na saída de `show interface` para uma interface de VLAN quando esse pacote é a Camada 3 (L3) processada pela Unidade Central de Processamento. O tráfego que é a Camada 2 (L2) comutada nunca alcança a Unidade Central de Processamento e não é contado nos **contadores de show interface** para a interface de VLAN. Ele seria contado na **saída show interface** para a interface física apropriada.

O comando `show interfaces card-type {slot/port} counters errors` é o equivalente do comando Cisco IOS `show port counters` para CatOS. Consulte a [Tabela 1](#) para obter explicações sobre a saída do contador de erros.

```
Router#sh interfaces fastEthernet 6/1 counters errors Port Align-Err FCS-Err Xmit-Err Rcv-Err
UnderSize OutDiscards Fa6/1 0 0 0 0 0 0 Port Single-Col Multi-Col Late-Col Excess-Col Carri-Sen
```

Tabela 1:

A saída do contador de erros de CatOS para **show port** ou **show port counters** para o Catalyst 6000, 5000 e 4000 Series. A saída do contador de erros do Cisco IOS para **show interfaces** ou **show interfaces card-type x/y counters errors** para o Catalyst 6000 e 4000 Series.

Contadores (em ordem alfabética)	Descrição e Causas Comuns de Incrementos de Contadores de Erros
Align-Err	<p>Descrição: Erros de contadores de interfaces CatOS sh port e Cisco IOS sh. Os erros de alinhamento são uma contagem do número de frames recebidos que não terminam com um número par de octetos e têm uma Verificação de Redundância Cíclica com erro (CRC).</p> <p>Causas comuns: São geralmente o resultado de uma incompatibilidade duplex (bidirecional) ou um problema físico (como cabeamento, uma porta ou uma placa de rede com erro). Quando o cabo é conectado à porta pela primeira vez, alguns desses erros podem ocorrer. Além disso, se existe um hub conectado à porta, as colisões entre outros dispositivos no hub poderão causar esses erros. Exceções da plataforma: Os erros de alinhamento não são contados no Catalyst 4000 Series Supervisor I (WS-X4012) ou Supervisor II (WS-X4013).</p>
cavacos	<p>Descrição: Contador de sh interfaces do Cisco IOS. Contador CatOS que indica que o temporizador em job de transmissão expirou. Um jabber é um frame com mais de 1518 octetos (excluindo bits de enquadramento, mas incluindo octetos FCS) que não termina com um número par de octetos (erro de alinhamento) ou que apresenta um erro crítico de FCS.</p>
Carri-Sen	<p>Descrição: Erros de contadores de interfaces CatOS sh port e Cisco IOS sh. O contador Carri-Sen (carrier sense) incrementa toda vez que um controlador de Ethernet quer enviar dados em uma conexão half duplex. O controlador percebe o fio e verifica se ele não está ocupado antes de transmitir. Causas comuns: Normal em um segmento Ethernet semidúplex.</p>
colisões	<p>Descrições: Contador de sh interfaces do Cisco IOS. O número de vezes que ocorreu uma colisão antes de a interface ter transmitido com</p>

	<p>sucesso um frame para a mídia. Causas comuns: As colisões são normais para interfaces configuradas como half duplex, mas não devem ser vistas em interfaces full duplex. Se as colisões estiverem aumentando dramaticamente, isso indica que um link está sendo muito usado ou é possível que haja uma incompatibilidade bidirecional com o dispositivo anexado.</p>
CRC	<p>Descrição: Contador de sh interfaces do Cisco IOS. Incrementa quando a Verificação de Redundância Cíclica (CRC) gerada pela estação LAN originadora ou por um dispositivo em extremidade distante não corresponde ao checksum calculado com base nos dados recebidos. Causas comuns: Isso normalmente indica problemas de ruído ou de transmissão na interface LAN da própria LAN. Um número alto de CRCs, em geral, é o resultado de colisões, mas também pode indicar um problema físico (como cabeamento, uma interface ou uma NIC inválida) ou uma incompatibilidade bidirecional.</p>
adiado	<p>Descrição: Contador de sh interfaces do Cisco IOS. O número de frames que foram transmitidos com sucesso depois que esperam porque a mídia estava ocupada. Causas comuns: Isso é visto, geralmente, nos ambientes half duplex quando a portadora já está em uso quando tenta transmitir um frame.</p>
entrada da pausa	<p>Descrição: Contador de show interfaces do Cisco IOS. Um incremento no contador de entrada da pausa significa que o dispositivo conectado solicita uma pausa de tráfego quando seu buffer de recepção está quase completo. Causas comuns: Este contador é incrementado para fins informativos, contanto que o switch aceite o frame. Os pacotes da pausa são interrompidos quando o dispositivo conectado pode receber o tráfego.</p>
condição do fluxo do packets with de entrada	<p>Descrição: Contador de sh interfaces do Cisco IOS. Um erro de bit do fluxo indica que um frame é um pouco longo demais. Causas comuns: Este contador de erro de frame é incrementado para fins informativos, desde que o interruptor aceite o quadro.</p>
Col.em excesso	<p>Descrição: Erros de contadores de interfaces CatOS sh port e Cisco IOS sh. Uma contagem dos frames em que a transmissão em uma interface particular falha devido a colisões excessivas. Uma colisão excessiva ocorre quando um pacote tem uma colisão 16 vezes</p>

	<p>seguidas. O pacote é então descartado.</p> <p>Causas comuns: Colisões excessivas são geralmente uma indicação de que a carga e o segmento precisam ser divididos em vários segmentos, mas também podem apontar uma incompatibilidade duplex com o dispositivo conectado. Colisões não devem ser vistas em interfaces configuradas como full duplex.</p>
FCS-Err	<p>Descrição: Erros de contadores de interfaces CatOS sh port e Cisco IOS sh. O número de frames de tamanho válido com erros de FCS, mas sem erros de enquadramento. Causas comuns: Esta é tipicamente um problema físico (como cabeamento, uma porta com erro, ou uma Placa de Interface de Rede com falha (placa de rede)) mas também pode indicar uma incompatibilidade duplex (bidirecional).</p>
quadro	<p>Descrição: Contador de sh interfaces do Cisco IOS. O número de pacotes recebeu incorretamente a informação de que tem um erro de Verificação de Redundância Cíclica (CRC) e um número não inteiro de octetos (erro de alinhamento). Causas comuns: Isso normalmente é o resultado de colisões ou de um problema físico (como cabeamento, porta ou NIC inválido), mas também pode indicar uma incompatibilidade dúplex.</p>
Giants	<p>Descrição: Erros de contadores de interfaces CatOS sh port e Cisco IOS sh e sh . Os frames foram informados que excederam o tamanho do frame máximo de Instituto de Engenharia Elétrica e Eletrônica (Institute of Electrical and Electronics Engineers) 802.3 (1518 bytes para Ethernet não jumbo) e que têm uma Sequência de Verificação de Frame (FCS) com erro.</p> <p>Causas comuns: Em muitos casos, este é o resultado de uma placa de rede com erro. Tente encontrar o dispositivo ofensivo e removê-lo da rede. Exceções da plataforma: O Cat4000 Series que executa o Cisco IOS anterior à versão de software 12.1(19)EW, o contador de giants incrementou em um frame > que 1518 bytes. Após 12.1(19)EW, um giant em how interfaces incrementa somente quando um frame é recebido > que 1518 bytes com um FCS com erro.</p>
ignorado	<p>Descrição: Contador de sh interfaces do Cisco IOS. O número de pacotes recebidos ignorados pela interface porque o hardware da interface teve baixa execução nos buffers internos. Causas comuns: Sobrecargas e surtos de ruído de broadcast podem provocar</p>

	aumento na contagem ignorada.
Erros de Entrada	<p>Descrição: Contador de sh interfaces do Cisco IOS. Causas comuns: Isto inclui runts, giants, sem buffer, Verificação de Redundância Cíclica (CRC), frame, overrun e contagens ignoradas. Outros erros relacionados à entrada podem igualmente causar erro na contagem dos erros de entrada e alguns datagramas podem ter mais de um erro. Portanto, essa soma não pode equilibrar com a soma de contagens de erro de entrada enumeradas. Consulte também a seção Erros de Entrada em uma Interface de Camada 3 Conectada a um Switchport de Camada 2.</p>
Colisão posterior	<p>Descrição: Erros de contadores de interfaces CatOS sh port e Cisco IOS sh e sh. O número de vezes que uma colisão é detectada em uma interface específica posteriormente no processo da transmissão. Para uma porta de 10 Mbit/s, isso é mais de 512 bits vezes na transmissão de um pacote. Quinhentos e vinte tempos de bit correspondem a 51,2 microssegundos em um sistema de 10 Mbit/s.</p> <p>Causas comuns: Esse erro pode indicar uma incompatibilidade dúplex entre outras coisas. Para o cenário de incompatibilidade bidirecional, a colisão atrasada é vista no lado do half duplex. Como o lado half duplex está transmitindo, o lado full duplex não espera sua vez e realiza uma transmissão simultânea, o que provoca uma colisão posterior. As colisões atrasadas também podem indicar um cabo Ethernet ou segmento muito longo. Colisões não devem ser vistas em interfaces configuradas como full duplex.</p>
portadora perdida	<p>Descrição: Contador de sh interfaces do Cisco IOS. O número de vezes em que a portadora foi perdida durante a transmissão. Causas comuns: Verifique para ver se há um cabo com problemas. Verifique a conexão física nos dois lados.</p>
Colisão Múltipla	<p>Descrição: Erros de contadores de interfaces CatOS sh port e Cisco IOS sh. O número de vezes que ocorreram colisões múltiplas antes de a interface ter transmitido com sucesso um frame para a mídia. Causas comuns: As colisões são normais para interfaces configuradas como half duplex, mas não devem ser vistas em interfaces full duplex. Se as colisões estiverem aumentando dramaticamente, isso indica que um link está sendo muito usado ou é possível que haja uma</p>

	incompatibilidade bidirecional com o dispositivo anexado.
sem buffer	Descrição: Contador de sh interfaces do Cisco IOS. O número de pacotes recebidos descartados porque há um espaço sem buffer. Causas comuns: Compare com a contagem ignorada. Com frequência, as tempestades de broadcasts podem ser responsáveis por esses eventos.
sem portadora	Descrição: Contador de sh interfaces do Cisco IOS. O número de vezes que a portadora não estava presente na transmissão. Causas comuns: Verifique para ver se há um cabo com problemas. Verifique a conexão física nos dois lados.
Out-Discard	Descrição: O número de pacotes de saída escolhidos para serem descartados mesmo sem erros detectados. Causas comuns: Uma razão possível para rejeitar o pacote pode ser a liberação de espaço de buffer.
buffer de saída, buffers com falha e trocados	Descrição: Contador de sh interfaces do Cisco IOS. O número de buffers com falha e o número de buffers trocados. Causas comuns: A porta cria um buffer para os pacotes no buffer de Transmissão quando a taxa de tráfego comutada à porta for alta e não for possível controlar a quantidade de tráfego. A porta começa a descartar os pacotes quando o buffer de Tx (transmissão) estiver cheio e aumentar as subutilizações e os contadores de falha do buffer de saída. O aumento nos contadores de falha do buffer de saída pode ser um sinal que as portas estão executando em uma velocidade e/ou duplex inferior ou há que existe tráfego em excesso passando pela porta. Como exemplo, considere um cenário onde um stream de multicast de 1 gig seja enviado para portas de 24 100 Mbps. Se uma interface de saída possui sobreassinaturas, é normal ver as falhas do buffer de saída aumentarem com Out-Discards. Para obter informações de Troubleshooting, consulte a seção Frames Adiados (Out-Lost ou Out-Discard) deste documento.
erros de saída	Descrição: Contador de sh interfaces do Cisco IOS. A soma de todos os erros que impediram a transmissão final dos datagramas da interface. Causa Comum: Esse problema é devido ao baixo tamanho da Fila de Saída pequeno.
sobrecarga	Descrição: O número de vezes que o hardware

rga	de receptor era incapaz de entregar dados recebidos para um buffer de hardware. Causa Comum: A taxa de entrada do tráfego excedeu a capacidade do receptor de controlar os dados.
entrada/saída dos pacotes	Descrição: Contador de sh interfaces do Cisco IOS. O total de pacotes sem erros recebidos e transmitidos na interface. Monitorar esses contadores para incrementos é útil para determinar se o tráfego flui corretamente através da interface. O contador de bytes inclui o encapsulamento de dados e MAC nos pacotes sem erros recebidos e transmitidos pelo sistema.
Rcv-Err	Descrição: O erro dos contadores de interfaces sh show port de CatOS ou show port counters do Cisco IOS (apenas para o Catalyst 6000 Series). Causas comuns: Consulte as Exceções da Plataforma. Exceções da plataforma: Catalyst 5000 Series rcv-err = falhas de buffer de recepção. Por exemplo, um runt, um giant ou um FCS-Err não incrementam o contador do rcv-err. O contador do rcv-err em um 5K incrementa somente em consequência de tráfego excessivo. No rcv-err do Catalyst 4000 Series = a soma de todos os erros de recepção, que significa, em contraste com o Catalyst 5000, que o contador rcv-err incrementa quando a interface recebe um erro como um runt, um giant ou um FCS-Err.
Runts	Descrição: Erros de contadores de interfaces CatOS sh port e Cisco IOS sh e sh. Os frames recebidos que são menores do que o tamanho mínimo de frame de Instituto de Engenharia Elétrica e Eletrônica (Institute of Electrical and Electronics Engineers) 802.3 (64 bytes para Ethernet) e com uma Verificação de Redundância Cíclica (CRC) com erro. Causas comuns: Isso pode ser causado por uma incompatibilidade duplex e por problemas físicos, por exemplo, um cabo, uma porta ou uma NIC com defeito no dispositivo conectado. Exceções da plataforma: Catalyst 4000 Series que executa o Cisco IOS Versão de Software Anterior à 12.1(19)EW, um runt = abaixo do tamanho. Abaixo do tamanho = frame < que 64 bytes. O contador de runt incrementado somente quando um frame menor que 64 bytes foi recebido. Após 12.1(19)EW, um runt = um fragmento. Um fragmento é um frame < que 64 bytes, mas com uma Verificação de Redundância Cíclica (CRC) com erro. O

	<p>resultado é que o contador de runts agora aumenta em show interfaces, junto com o contador de fragmentos em erros de contadores de show interfaces quando um frame menor que 64 bytes com uma verificação de redundância cíclica com erro é recebido.</p> <p>Switches do Cisco Catalyst 3750 Series Em releases anteriores ao Cisco IOS 12.1(19)EA1 em que dot1q é usado na interface de entroncamento no Catalyst 3750, os runts podem ser vistos nas saídas show interfaces porque os pacotes encapsulados válidos do dot1q, que vão de 61 a 64 bytes e incluem a etiqueta-q, são contados pelo Catalyst 3750 como frames abaixo do tamanho, embora esses pacotes tenham sido enviados corretamente. Além disso, estes pacotes não são relatados na categoria apropriada (unicast, multicast ou broadcast) em estatísticas de recebimento. Esse problema é solucionado no Cisco IOS release 12.1(19)EA1 ou 12.2(18)SE ou mais recente.</p>
Colisão Única	<p>Descrição: Erros de contadores de interfaces CatOS sh port e Cisco IOS sh. O número de vezes que ocorreu uma colisão antes de a interface ter transmitido com sucesso um frame para a mídia. Causas comuns: As colisões são normais para interfaces configuradas como half duplex, mas não devem ser vistas em interfaces full duplex. Se as colisões estiverem aumentando dramaticamente, isso indica que um link está sendo muito usado ou é possível que haja uma incompatibilidade bidirecional com o dispositivo anexado.</p>
reguladores de pressão	<p>Descrição: show interfaces do Cisco IOS. O número de vezes que o receptor na porta é desabilitado, possivelmente a uma sobrecarga do buffer ou do processador. Se um asterisco (*) aparece após o valor do contador dos aceleradores, significa que a interface fica obstruída no momento em que o comando é executado. Causas comuns: Os pacotes que podem aumentar a sobrecarga do processador incluem pacotes IP com opções, TTL expirado, encapsulamento de não ARPA, fragmentação, tunelling, pacotes ICMP, pacotes com falha de checksum MTU, falha de RPF, checksum de IP e erros de comprimento.</p>
subutilizações de capacidade	<p>Descrição: O número de vezes que o transmissor foi executado mais rapidamente do que o switch pode controlar. Causas comuns: Isso pode ocorrer em uma situação de</p>

ade	throughput elevado onde uma interface receba um volume alto do tráfego intermitente de muitas outras interfaces de uma vez. As reinicializações de interfaces podem ocorrer com as ausências de execução.
Subdesenvolvimento	Descrição: Erros de contadores de sh interfaces CatOS sh port e Cisco IOS sh. Os frames recebidos que são menores do que o tamanho de frame mínimo de 64 bytes de Instituto de Engenharia Elétrica e Eletrônica (Institute of Electrical and Electronics Engineers) 802.3 (que exclui bits de enquadramento, mas inclui os octetos de FCS) que são, de outra forma bem constituídos. Causas comuns: Verifique o dispositivo que envia esses frames.
Xmit-Err	Descrição: Erros de contadores de interfaces CatOS sh port e Cisco IOS sh. Isso indica que o buffer (Tx) de envio interno está cheio. Causas comuns: Uma causa comum de Xmit-Err pode ser o tráfego de um link de largura de banda alta comutado para um link de largura de banda menor ou o tráfego de vários links de entrada comutados para um único link de saída. Por exemplo, se uma grande quantidade de tráfego intermitente for transportada em uma interface de gigabit e for comutada para uma interface de 100 Mbps, isso poderá fazer com que Xmit-Err seja incrementado na interface de 100 Mbps. Isso ocorre porque o buffer de saída da interface está sobrecarregado pelo excesso de tráfego devido à incompatibilidade de velocidade entre as larguras de banda de entrada e de saída.

[Contadores Show Mac para CatOS e Show Interfaces para o Cisco IOS](#)

O comando {mod/port} **show mac** é útil quando executa CatOS no supervisor para monitorar o tráfego de entrada e de saída na porta como indicado pelos contadores de recepção (Rcv) e transmissão (Xmit) para unicast, multicast e o tráfego de broadcast. Esta saída é de um Catalyst 6000 que executa CatOS:

```
Console> (enable) sh mac 3/1
```

```

Port      Rcv-Unicast      Rcv-Multicast      Rcv-Broadcast
-----
3/1              177                256272              3694

Port      Xmit-Unicast      Xmit-Multicast      Xmit-Broadcast
-----
3/1              30                 680377              153

Port      Rcv-Octet      Xmit-Octet
-----
```

```

MAC          Dely-Exced MTU-Exced In-Discard Out-Discard -----
----- 3/1 0 0 233043 17 Port Last-Time-Cleared ----- 3/1 Sun
Jun 1 2003, 12:22:47

```

Este comando também tem os seguintes contadores de erros: **Dely-Exced**, **MTU-Exced**, **In-Discard** e **Out-Discard**.

- **Dely-Exced** - O número de quadros rejeitados por esta porta devido a um excessivo transmite o atraso através do interruptor. Esse contador nunca deve subir, a menos que a porta esteja com alto nível de utilização.
- **MTU Exceed** – É uma indicação de que um dos dispositivos nessa porta ou segmento está transmitindo mais do que o tamanho de frame permitido (1518 bytes para Ethernet não jumbo).
- **In-Discard** - O resultado de frames válidos de entrada que foram descartados porque o frame não precisava ser comutado. Isso pode ser normal se um hub estiver conectado a uma porta e dois dispositivos nesse hub fazem intercâmbio de dados. A porta de switch ainda vê os dados mas não tem precisa comutá-los (contanto que a tabela CAM exiba o endereço MAC dos dois dispositivos associados com a mesma porta) e é descartada. Esse contador também pode incrementar em uma porta configurada como um entroncamento se este bloqueia algumas VLANs ou em uma porta que seja o único membro de uma VLAN.
- **Out-Discard** – O número de pacotes externos escolhidos para serem descartados mesmo sem serem detectados erros de pacote. Uma razão possível para rejeitar o pacote pode ser a liberação de espaço de buffer.

Os switches das séries Catalyst 4000 e 5000 que executam CatOS têm dois contadores de erros adicionais no **comando show mac**. Estes são os contadores **In-Lost** e **Out-Lost**:

```

MAC          Dely-Exced MTU-Exced In-Discard Lrn-Discrd In-Lost Out-Lost -----
----- 5/1 0 0 0 0 0 0

```

- **In-Lost** - No Catalyst 4000, esse contador é a soma de todos os pacotes de erros recebidos na porta. Por outro lado, o contador **In-Lost** no Catalyst 5000 monitora a soma de todas as falhas de buffer recebidas.
- **Out-Lost** - No Catalyst 4000 e 5000, esses são os frames de saída que foram perdidos antes que fossem enviados (devido ao espaço insuficiente do buffer). Geralmente, isso é causado por sobreassinatura na porta.

O comando **show interfaces card-type {slot/port} counters** é usado quando você executa o Cisco IOS no Supervisor.

Nota: Não há nenhum contadores equivalentes aos contadores de erros de **show mac** do CatOS: **Dely-Exced**, **MTU-Exced** e **In-Discard** nesse comando. Existe, entretanto, um contador de **Out-Discard** no comando **1show interfaces counters errors** do Cisco IOS que é explicado na [Tabela 1](#).

```

Router#sh interfaces fas 6/1 counters Port InOctets InUcastPkts InMcastPkts InBcastPkts Fa6/1
47856076 23 673028 149 Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts Fa6/1 22103793 17
255877 3280 Router# !--- Cisco IOS counters used to monitor inbound and outbound unicast,
multicast !--- and broadcast packets on the interface.

```

[Show Counters para CatOS e Interface de Show Counters para o Cisco IOS](#)

O comando **[mod/port] show counters** oferece ainda mais estatísticas detalhadas para portas e interfaces. Este comando está disponível para CatOS e o comando equivalente **show counters interface card-type {slot/port}** introduzido na versão de software 12.1(13)E do Cisco IOS apenas

para o Catalyst 6000 Series. Esses comandos exibem os contadores de erros de 32 bits e 64 bits por porta ou interface. Consulte a documentação do comando CatOS de [show counters](#) para obter mais informações.

Nota: As estatísticas do contador para os switches da série Catalyst 6000 que executam o Cisco IOS estão em Hex.

```
Console> (enable) sh counters 3/1 64 bit counters 0 rxHCTotalPkts = 260555 1 txHCTotalPkts = 687411 2 rxHCUnicastPkts = 177 3 txHCUnicastPkts = 30 4 rxHCMulticastPkts = 256684 5 txHCMulticastPkts = 687228 6 rxHCBroadcastPkts = 3694 7 txHCBroadcastPkts = 153 8 rxHCOctets = 22386167 9 txHCOctets = 48850817 10 rxTxHCPkts64Octets = 228929 11 rxTxHCPkts65to127Octets = 701493 12 rxTxHCPkts128to255Octets = 285 13 rxTxHCPkts256to511Octets = 17090 14 rxTxHCPkts512to1023Octets = 168 15 rxTxHCPkts1024to1518Octets = 1 16 txHCTrunkFrames = 395217 17 rxHCTrunkFrames = 236459 18 rxHCDropEvents = 0 32 bit counters 0 rxCRCAlignErrors = 0 1 rxUndersizedPkts = 0 2 rxOversizedPkts = 0 3 rxFragmentPkts = 0 4 rxJabbers = 0 5 txCollisions = 0 6 ifInErrors = 0 7 ifOutErrors = 0 8 ifInDiscards = 233043 9 ifInUnknownProtos = 2 10 ifOutDiscards = 17 !--- Output suppressed.
```

Show Controller Ethernet-Controller para Cisco IOS

Para o catalizador 3750, 3550, a 2970, 2950/2955, 2940, e os interruptores 2900/3500XL usam o controlador de ethernet do comando show controller para indicar o contador de tráfego e o contador de erros output que é similar ao [show port](#), [mostram a relação](#), [mostram o Mac](#) e [mostram os contadores](#) output para o catalizador 6000, 5000 e 4000 Series Switch.

```
3550-1#sh controller ethernet-controller fastEthernet 0/1 !--- Output from a Catalyst 3550.
Transmit FastEthernet0/1 Receive 0 Bytes 0 Bytes 0 Unicast frames 0 Unicast frames 0 Multicast frames 0 Multicast frames 0 Broadcast frames 0 Broadcast frames 0 Discarded frames 0 No dest, unicast 0 Too old frames 0 No dest, multicast 0 Deferred frames 0 No dest, broadcast 0 1 collision frames 0 2 collision frames 0 FCS errors 0 3 collision frames 0 Oversize frames 0 4 collision frames 0 Undersize frames 0 5 collision frames 0 Collision fragments 0 6 collision frames 0 7 collision frames 0 Minimum size frames 0 8 collision frames 0 65 to 127 byte frames 0 9 collision frames 0 128 to 255 byte frames 0 10 collision frames 0 256 to 511 byte frames 0 11 collision frames 0 512 to 1023 byte frames 0 12 collision frames 0 1024 to 1518 byte frames 0 13 collision frames 0 14 collision frames 0 Flooded frames 0 15 collision frames 0 Overrun frames 0 Excessive collisions 0 VLAN filtered frames 0 Late collisions 0 Source routed frames 0 Good (1 coll) frames 0 Valid oversize frames 0 Good(>1 coll) frames 0 Pause frames 0 Pause frames 0 Symbol error frames 0 VLAN discard frames 0 Invalid frames, too large 0 Excess defer frames 0 Valid frames, too large 0 Too large frames 0 Invalid frames, too small 0 64 byte frames 0 Valid frames, too small 0 127 byte frames 0 255 byte frames 0 511 byte frames 0 1023 byte frames 0 1518 byte frames 3550-1# !--- See table for additional counter output for 2900/3500XL Series switches.
```

Contador	Descrição	Possíveis causas
Frames transmitidos		
Quadros descartados	O número total de frames cuja tentativa de transmissão é abandonada devido a recursos insuficientes. Este total inclui quadros de todos os tipos de destino.	A carga de tráfego na interface é excessiva e faz com que os frames sejam descartados. Reduza a carga de tráfego na interface se perceber um aumento no número de pacotes nesse campo.
Quadros	O número de frames que	A carga de tráfego

<p>muito antigos</p>	<p>demoram mais de dois segundos para passar através do switch. Por esse motivo, foram descartados pelo switch. Isso acontece somente sob circunstâncias extremas e de estresse elevado.</p>	<p>para esse switch é excessiva e faz com que os frames sejam descartados. Reduza a carga do switch se perceber um aumento no número de pacotes nesse campo. Você pode precisar alterar a topologia de rede para reduzir a carga de tráfego para o switch.</p>
<p>Frames em atraso</p>	<p>O número total de frames em que a primeira tentativa de transmissão foi atrasada devido ao tráfego nas mídias de rede. Esse total inclui somente apenas esses frames que são transmitidos subsequentemente sem erros e sem experimentar uma colisão.</p>	<p>A carga de tráfego destinada para esse switch é excessiva e faz com que os frames sejam descartados. Reduza a carga do switch se perceber um aumento no número de pacotes nesse campo. Você pode precisar alterar a topologia de rede para reduzir a carga de tráfego para o switch.</p>
<p>Frames de colisão</p>	<p>Os contadores de frames da colisão são o número de vezes que um pacote tentou ser transmitido e não foi bem sucedido, mas que foi bem sucedido em sua tentativa seguinte. Isso significa que se o contador de 2 frames da colisão aumentou, o switch tentou enviar duas vezes o pacote e falhou, mas foi bem sucedido em sua terceira tentativa.</p>	<p>A carga de tráfego na interface é excessiva e faz com que os frames sejam descartados. Reduza a carga de tráfego na interface se perceber um aumento no número de pacotes nesses campos.</p>
<p>Colisões excessivas</p>	<p>O contador de colisões excessivas aumenta após 16 colisões atrasadas consecutivas ocorrerem em uma linha. Depois que 16 tentativas</p>	<p>Se esse contador incrementa, é uma indicação de problema na fiação, de rede excessivamente</p>

	foram feitas para enviar o pacote, ele é descartado e o contador incrementa.	carregada ou de uma incompatibilidade duplex (bidirecional). Uma rede excessivamente carregada pode ser causada por muitos dispositivos em uma Ethernet compartilhada.
Colisões atrasada	Uma colisão posterior ocorre quando dois dispositivos transmitem ao mesmo tempo e nenhum dos lados da conexão detecta uma colisão. A razão para essa ocorrência é que o tempo de propagação do sinal de uma extremidade de rede para a outra ser mais longo que o tempo para colocar o pacote inteiro na rede. Os dois dispositivos que causam a colisão atrasada nunca vêm que o outro está enviando até que ele coloque todo o pacote na rede. As colisões posteriores não são detectadas pelo transmissor antes do tempo de slot de 64 bytes. Isso ocorre porque elas são detectadas somente nas transmissões de pacotes maiores que 64 bytes.	As colisões atrasadas são resultado do cabeamento incorreto ou de um número de hubs não compatíveis na rede. As placas de rede com falha também podem causar colisões posteriores.
Frames bons (1 colisão)	O número total de frames que experimentam exatamente uma colisão e são, em seguida, transmitidos com sucesso.	As colisões em um ambiente half-duplex são um comportamento esperado normal.
Frames bons (> de 1	O número total de frames que experimentam entre 2 e	As colisões em um ambiente half-duplex são um

colisão)	15 colisões, inclusive, e são transmitidos com sucesso.	comportamento esperado normal. Os frames que incrementam na extremidade superior desse contador correm o risco de exceder 15 colisões e de serem calculados como colisões Excessivas.
Frames descartados de VLAN	O número de frames descartados em uma interface porque o bit CFI foi configurado.	O bit do Indicador do Formato Canônico (CFI) no TCI de um frame 802.1q é definido como 0 para o formato de frame canônico de ethernet. Se o bit CFI é definido como 1, isso indica a presença de um frame não canônico RIF (Campo de Informação de Roteamento) ou de um Token Ring descartado.
Frames Recebidos		
Nenhum frame de largura de banda	<i>Apenas 2900/3500XL.</i> O número de vezes que uma porta recebeu um pacote da rede, mas o switch não tinha os recursos para recebê-la. Isso acontece somente sob condições de estresse, mas pode acontecer com explosões do tráfego em diversas portas. Assim, um pequeno número de Frames sem largura de banda não é um motivo de preocupação. (Ainda deve ser bem menos de um por cento dos frames recebidos.)	A carga de tráfego na interface é excessiva e faz com que os frames sejam descartados. Reduza a carga de tráfego na interface se perceber um aumento no número de pacotes nesse campo.
Frames sem	<i>Apenas 2900/3500XL.</i> O número de vezes que	A carga de tráfego na interface é

buffers	<p>uma porta recebeu um pacote da rede, mas o switch não tinha os recursos para recebê-la. Isso acontece somente sob condições de estresse, mas pode acontecer com explosões do tráfego em diversas portas. Assim, um pequeno número de Frames sem buffers não é um motivo de preocupação. (Ainda deve ser bem menos de um por cento dos frames recebidos.)</p>	<p>excessiva e faz com que os frames sejam descartados. Reduza a carga de tráfego na interface se perceber um aumento no número de pacotes nesse campo.</p>
Sem destino, unicast	<p>No destination unicast é o número de pacotes unicast que a porta não enviou a nenhuma outra porta.</p>	<p>Estas são descrições breves de quando os contadores No dest (unicast, multicast e broadcast) podem aumentar:</p> <ul style="list-style-type: none"> • Se uma porta é uma porta de acesso e a porta está conectada a uma porta de entroncamento Inter-Switch Link Protocol (ISL), Nenhum contador No dest é muito grande, desde que todos os pacotes ISL de entrada não sejam enviados. Configuração inválida. • Se uma porta está bloqueada pelo Spanning Tree Protocol (STP), a maioria dos pacotes não é
No dest, multicast	<p>No destination multicast é o número de pacotes multicast que a porta não encaminhou a nenhuma outra porta.</p>	
No dest, broadcast	<p>No destination broadcast é o número de pacotes de broadcast que a porta não encaminhou a nenhuma outra porta.</p>	

encaminhada, o que resulta em pacotes No dest. Se uma porta acabou de obter um link, existe um período muito breve (menos de um segundo) onde os pacotes de entrada não são enviados.

- Se a porta está em uma VLAN por si só, e nenhuma outra porta no switch pertence a essa VLAN, todos os pacotes de entrada são descartados e o contador aumenta.
- O contador também incrementa quando o endereço de destino do pacote é identificado na porta que o pacote foi recebido. Se um pacote foi recebido na porta 0/1, com endereço MAC de destino X, e o switch já detectou que o endereço MAC X reside na porta 0/1, ele

incrementa o contador e descarta o pacote. Isso pode acontecer nas seguintes situações: Se um cubo está conectado à porta 0/1 e uma estação de trabalho conectada ao hub transmite pacotes a uma outra estação de trabalho conectada ao hub, a porta 0/1 não encaminha esse pacote para nenhum lugar porque o MAC de destino reside na mesma porta. Isso também pode ocorrer se um switch é conectado à porta 0/1 e começa a inundar de pacotes todas as portas para detectar endereços MAC.

- Se um endereço estático foi instalado em uma outra porta na mesma VLAN e nenhum

		<p>endereço estático foi instalado para a porta de recepção, o pacote é descartado. Por exemplo, se um mapa estático para o endereço MAC X foi configurado na porta 0/2 para encaminhar o tráfego à porta 0/3, o pacote deve ser recebido na porta 0/2 ou será descartado. Se um pacote é enviado de qualquer outra porta, na mesma VLAN que a porta 0/2, o pacote será descartado.</p> <ul style="list-style-type: none"> • Se a porta é uma porta segura, os pacotes com endereços MAC de origem não permitida não serão encaminhados e incrementarão o contador.
Erros de alinhamento	Os erros de alinhamento são o número de frames recebidos que não terminam com um número par de octetos e possuem uma Verificação de	Os erros de alinhamento são causados por um frame que não está sendo copiado completamente para o fio, o que resulta

	Redundância Cíclica (CRC) com erro.	em frames fragmentados. Os erros de alinhamento são o resultado de colisões de modo half duplex, uma incompatibilidade duplex, hardware com erro (placa de rede, cabo ou porta) ou um dispositivo conectado gerando frames que não terminam em um octeto e que têm um FCS com erro.
Erros de FCS	A contagem de erros de FCS é o número de frames que foram recebidos com um checksum inválido (valor de Verificação de Redundância Cíclica (CRC)) no Quadro Ethernet. Esses quadros são descartados e não são propagados para outras portas.	Os erros de FCS são o resultado de colisões em incompatibilidade half duplex, duplex, hardware com erro (placa de rede, cabo ou porta) ou de um dispositivo conectado que gera frames com FCS inválido.
Frames subdesenvolvidos	São o número total de pacotes recebidos que tinham menos de 64 octetos de comprimento (que excluem bits de frame, mas incluem FCS) e têm um valor FCS apropriado.	Isso é uma indicação de um quadro defeituoso gerado pelo dispositivo conectado. Verifique se o dispositivo conectado está operando corretamente.
Frames acima do tamanho	Número de pacotes recebidos pela porta da rede com os pacotes que tinham mais de 1514 bytes.	Isso pode ser uma indicação de falha de hardware, dot1q ou problemas de configuração do entroncamento ISL.
Fragmentos da colisão	O número total de frames cujo comprimento é menor que de 64 octetos (que exclui os bits de framing, mas que incluem o FCS) e tem um valor FCS	Se esse contador incrementa, é uma indicação que as portas estão configuradas em half-duplex. Mude a configuração duplex

	inapropriado.	para full duplex.
Frames de sobrecarga	O número de vezes que o hardware de receptor era incapaz de entregar dados recebidos para um buffer de hardware.	A taxa de entrada do tráfego excedeu a capacidade do receptor de controlar os dados.
Frames filtrados de VLAN	O número total de frames que são filtrados devido ao tipo de informações de VLAN contidas no frame.	A porta pode ser configurada para filtrar frames etiquetados 802.1Q. Quando um frame é recebido e contém uma etiqueta 802.1Q, ele é filtrado e essa estatística é incrementada.
Frames roteados da origem	O número total de frames recebidos que são descartados devido ao bit da rota de origem ter sido configurado no endereço de origem do frame nativo.	Esse tipo de roteamento de origem é definido somente para Token Ring e FDDI. A especificação de ethernet Instituto de Engenharia Elétrica e Eletrônica (Institute of Electrical and Electronics Engineers) proíbe esse bit de ser configurado em um Quadro Ethernet. Consequentemente, o switch descarta esses frames.
Frames acima do tamanho válidos	O número total de frames recebidos cujo tamanho excede o MTU de Sistema e que, entretanto possui valores FCS adequados.	Essa estatística conta os frames que excedem o Sistema configurado MTU, mas que pode ter sido aumentado de 1518 bytes para permitir os encapsulamentos Q-em-Q ou MPLS.
Frames de erro de símbolo	A Ethernet de Gigabit (1000 Base-X) utiliza Codificação 8B/10B para converter dados de 8 bits de subcamada MAC (camada 2) para um	Um erro de Símbolo significa que a interface detecta um Símbolo (inválido) indeterminado recebido. As

	Símbolo de 10 bits a ser enviado via cabo. Quando uma porta recebe um Símbolo, extrai os dados de 8 bits do Símbolo (10 bits).	quantidades pequenas de erros de símbolos podem ser ignoradas. As grandes quantidades de erros de símbolos podem indicar um dispositivo, um cabo, ou um hardware com erro.
Frames inválidos, muito grandes	Os frames giant ou frames recebidos que excederam o tamanho do frame máximo de Instituto de Engenharia Elétrica e Eletrônica (Institute of Electrical and Electronics Engineers) 802.3 (1518 bytes para Ethernet não jumbo) e que têm uma Sequência de Verificação de Frame (FCS) com erro.	Em muitos casos, este é o resultado de uma placa de rede com erro. Tente encontrar o dispositivo ofensivo e removê-lo da rede.
Frames inválidos, muito pequenos	Os frames runt ou os frames recebidos menores de 64 bytes (que incluem os bits FCS e excluem o cabeçalho de frame) e têm um erro de FCS ou um erro de alinhamento.	Isso pode ser causado por uma incompatibilidade duplex e por problemas físicos, por exemplo, um cabo, uma porta ou uma NIC com defeito no dispositivo conectado.

[Show Top para CatOS](#)

O comando show top permite que você colete e analise dados para cada porta física em um switch. O comando exibe estes dados para cada porta física:

- Utilização de porta (Uti %)
- Número bytes (Bytes) de entrada e de saída
- Número de pacotes (Pcts) de entrada e de saída
- Número de pacotes de broadcast (Bcst) de entrada e de saída
- Número de pacotes multicast (Mcst) de entrada e de saída
- Número de erros (Erro) de entrada
- Número de erros de excesso (Excesso) de buffer

```
Console> (enable) sh top Start Time: Mar 28 2007 06:58:41 End Time: Mar 28 2007 06:59:11
PortType: all Metric: util Port Band- Uti Bytes Pkts Bcst Mcst Error Over width % (Tx + Rx) (Tx
+ Rx) (Tx + Rx) (Tx + Rx) (Rx) flow -----
```

```
----- ----- 3/11 a-10 0 334187 1561 22 1536 0 0 3/12 a-100 0 333608 1557 22 1532 0 0
3/25 a-100 0 333622 1555 22 1533 0 0 6/2 1000 0 0 0 0 0 0 6/1 1000 0 0 0 0 0 0 4/8 1000 0 0
0 0 0 0 0 4/7 1000 0 0 0 0 0 0 4/6 1000 0 0 0 0 0 0 4/5 1000 0 0 0 0 0 0 4/4 1000 0 0 0 0
0 0 0 4/3 1000 0 0 0 0 0 0 4/2 1000 0 0 0 0 0 0 4/1 1000 0 0 0 0 0 0 3/48 auto 0 0 0 0 0 0
0 3/47 auto 0 0 0 0 0 0 3/46 auto 0 0 0 0 0 0
```

Nota: Quando você calcula a utilização de porta, o comando empacota as linhas de Tx e RX alinha no mesmo contador e também verifica a largura de banda full duplex quando calcula a porcentagem da utilização. Por exemplo, uma porta de Ethernet de Gigabit é full duplex de 2000 Mbps.

Com erros é a soma de todos os pacotes com erro recebidos nessa porta.

O Excesso de Buffer indica que a porta recebe mais tráfego do que pode armazenar em seu buffer. Isso pode ser causado por uma explosão de tráfego ou por sobrecarga de buffers. A ação sugerida é diminuir a transmissão do dispositivo de origem.

Consulte também os contadores “In-Lost” e “Out-Lost” do comando `show mac`.

[Mensagens de Erro de Sistema Comuns](#)

O Cisco IOS às vezes apresenta um formato diferente para mensagens de sistema. Você pode examinar mensagens de sistema de CatOS e mensagens de sistema do Cisco IOS para fazer uma comparação. Você pode consultar o **Guia de Mensagens e Procedimentos de Recuperação** para o release do software que você executa. Por exemplo, você pode verificar as [Mensagens e Procedimentos de Recuperação](#) para o Release de Software 7.6 do CatOS e comparar com as [Mensagens e Procedimentos de Recuperação](#) para os Releases do Cisco IOS 12.1 E.

[Mensagens de Erro nos Módulos WS-X6348](#)

Verifique estas mensagens de erro:

- Checksum do cabeçalho de auge de bobina
- Erro de máquina de estado de bobina Mdtif
- Erro CRC de pacote de bobina Mdtif
- Erro de baixo fluxo de Coil Pb Rx
- Erro de paridade Pb Rx da bobina

Você pode ver as mensagens de syslog com um desses erros listados:

```
%SYS-5-SYS_LCPERR5:Module 9: Coil Pinnacle Header Checksum Error - Port #37
```

Se você receber esse tipo de mensagem ou notar que grupos de 10/100 portas que falham nos módulos WS-X6348, consulte este documento para obter informações adicionais de troubleshooting com base no sistema operacional que você usa:

- [Troubleshooting de Conectividade do WS-X6348 Module Port para Catalyst 6000 usando CatOS](#)
- [Fazendo Troubleshooting na Conectividade da Porta do Módulo WS-X6348 em um Catalyst 6500/6000 que executa o Software de Sistema do Cisco IOS](#)

[%%PAGP-5-PORTTO/FROMSTP e %ETHC-5-PORTTO/FROMSTP](#)

Para CatOS, use o [comando show logging buffer](#) para ver as mensagens de log armazenadas.

Para o Cisco IOS, use o comando **show logging**.

```
Console> (enable) sh logging buffer 2003 Jun 02 20:12:43 %PAGP-5-PORTTOSTP:Port 3/2 joined  
bridge port 3/2 2003 Jun 02 20:59:56 %PAGP-5-PORTFROMSTP:Port 3/1 left bridge port 3/1 !--- This  
is the command to view the logging buffer on switches that run CatOS.
```

Essa mensagem pode causar preocupação para clientes, mas para a grande maioria ela é informacional por natureza.

```
%PAGP-5-PORTTO / FROMSTP and %ETHC-5-PORTTO / FROMSTP
```

O Protocolo de Agregação de Porta (PAgP) negocia links de EtherChannel entre switches. Sempre que um dispositivo ingressa ou deixa uma porta de ponte, uma mensagem informativa é exibida na console. Na maioria dos casos esta mensagem é completamente normal, mas se você vir essas mensagens nas portas que não deveriam oscilar por qualquer razão, você deve investigar mais.

Na versão 7.x e mais recente de software do CatOS, "PAGP-5" foi alterado para "ETHC-5" para tornar a mensagem mais compreensível.

Esta mensagem é específica para os switches séries Catalyst 4000, 5000 e 6000 que executam CatOS. Não há nenhuma mensagem de erro para os switches que executam o Cisco IOS equivalente a esta mensagem. Para obter mais informações, sobre mensagens de erro nos switches que executam CatOS, consulte os seguintes documentos para sua plataforma:

- [Mensagens de erro comuns de CatOS em Switches da série Catalyst 4000](#)
- [Mensagens de erro comuns de CatOS em Switches da série Catalyst 5500 ou 5000](#)
- [Mensagens de erro comuns de CatOS em Switches da série Catalyst 6500 ou 6000](#)

[%SPANTREE-3-PORTDEL_FAILNOTFOUND](#)

Esta mensagem não indica um problema com o switch. Ela ocorre normalmente com mensagens %PAGP-5-PORTFROMSTP.

O Protocolo de Agregação de Porta (PAgP) negocia links de EtherChannel entre switches. Sempre que um dispositivo ingressa ou deixa uma porta de ponte, uma mensagem informativa é exibida na console. Na maioria dos casos esta mensagem é completamente normal, mas se você vir essas mensagens nas portas que não deveriam oscilar por qualquer razão, você deve investigar mais.

Esta mensagem é específica para os switches séries Catalyst 4000, 5000 e 6000 que executam CatOS. Não há nenhuma mensagem de erro para os switches que executam o Cisco IOS equivalente a esta mensagem. Para obter mais informações sobre mensagens de erro nos switches que executam CatOS, consulte os seguintes documentos para sua plataforma:

- [Mensagens de erro comuns de CatOS em Switches da série Catalyst 4000](#)
- [Mensagens de erro comuns de CatOS em Switches da série Catalyst 5500 ou 5000](#)
- [Mensagens de erro comuns de CatOS em Switches da série Catalyst 6500 ou 6000](#)

[%SYS-4-PORT_GBICBADEEPROM://%SYS-4-PORT_GBICNOTSUPP](#)

A causa mais comum dessa mensagem é quando um não Cisco GBIC não certificado é inserido em um módulo de ethernet de gigabit. O GBIC não tem um Cisco SEEPROM que resulta na geração de uma mensagem de erro.

Os módulos de GBIC WS-G5484, WS-G5486 e WS-G5487 usados com um WS-X6408-GBIC também podem causar essas mensagens de erro, mas não há um problema real com a placa ou GBICs e existe uma correção de upgrade de software.

Consulte [Mensagens de Erro CatOS comuns nos Switches das Séries do Catalyst 6000/6500](#) para obter mais informações.

[%AMDP2_FE-3-UNDERFLO](#)

Esta mensagem de erro é causada quando um frame é transmitido e o buffer local do buffer local do chip do controlador recebe dados insuficientes. Os dados não podem ser transferidos ao chip suficientemente rápido para acompanhar a taxa de saída. Normalmente, tal condição é temporária, dependente das cargas de pico transientes dentro do sistema. O problema ocorre quando uma quantidade excessiva de tráfego é processada pela interface Ethernet Rápida. A mensagem de erro é recebida quando o nível de tráfego alcança aproximadamente 2,5 Mb. Essa restrição de nível de tráfego força é devido à limitação do hardware. Devido a isso, existe uma possibilidade existe para o dispositivo conectado ao switch do Catalyst descartar os pacotes.

A solução é que, normalmente, o sistema se recupere automaticamente. Nenhuma ação é exigida. Se o switch sobrecarrega a interface Ethernet, verifique as configurações de velocidade e duplex. Use também um programa sniffer para analisar os pacotes que entram e saem da interface Ethernet rápida do roteador. A fim evitar que os pacotes sejam descartados no dispositivo conectado ao switch do Catalyst, emita o [comando ip cef](#) na interface Ethernet rápida do dispositivo conectado ao switch.

[%INTR_MGR-DFC1-3-INTR: Mecanismo de Enfileiramento \(Blackwater\) \[1\]: FIC Fabric-A Recebeu Código de Controle Inesperado](#)

A razão para essa mensagem de erro é o recibo de um pacote de switch fabric, onde o valor de CRC no cabeçalho de construção nesse pacote não corresponde ao valor de Verificação de Redundância Cíclica (CRC) calculado pelo subblock do Controlador da Interface de Construção (FIC) do Blackwater ASIC. Isso indica que o pacote foi corrompido durante a transferência e o Blackwater recebeu o pacote corrompido.

[Comando Rejeitado: \[\[Interface\] not a Switching Port](#)

Nos switches que oferecem suporte para as interfaces L3 e switchport L2, a mensagem *Comando rejeitado: [[interface] not a switching port* é exibida quando você tenta inserir um comando relacionado à camada 2 em uma porta configurada como uma interface da camada 3.

Para converter a interface do modo da camada 3 para mergulhar o modo 2, emita o comando **switchport** de configuração de interface. Após emitir esse comando, configure a porta para qualquer propriedade da camada 2.

[Problemas Comuns da Porta e da Interface](#)

[O Status da Interface ou da Porta é Desabilitada ou Encerrada](#)

Uma causa óbvia, mas às vezes ignorada da falha da conectividade de porta é uma configuração incorreta do switch. Se uma porta tem uma luz laranja sólida, significa que o software do switch

desabilitou a porta, pela interface do usuário ou por processos internos.

Nota: Alguns LEDs de porta da plataforma trabalham de forma diferente em relação ao STP. Por exemplo, o Catalyst 1900/2820 torna as portas laranjas quando estão no modo de bloqueio STP. Nesse caso, uma luz laranja pode indicar as funções normais do STP. O Catalyst 6000/5000/4000 não faz com que a luz da porta fique laranja quando bloqueia para STP.

Assegure-se de que a porta ou o módulo não tenham sido desabilitados ou desligados por qualquer motivo. Se uma porta ou um módulo são desabilitados manualmente em um lado ou outro do link, o link não é ativado até que você habilite a porta novamente. Verifique o status de porta em ambos os lados.

Para CatOS, verifique se **show port**, e se a porta estiver **desabilitada**, habilite-a novamente:

```
Port Name Status Vlan Duplex Speed Type
-----
3/1 disabled 1 auto auto 10/100BaseTX !--- Use the set port enable
mod/port command to re-enable this port.
```

Use o comando **show module** para determinar se o módulo está desabilitado. Se estiver, habilite-o novamente:

```
Mod Slot Ports Module-Type Model Sub Status
---
2 2 2 1000BaseX Supervisor WS-X6K-SUP1A-2GE yes ok
16 2 1 Multilayer Switch Feature WS-F6K-MSFC no ok
3 3 48 10/100BaseTX Ethernet WS-X6348-RJ-45 no disable !--- Use the set module
enable mod/port command to re-enable this port.
```

Para o Cisco IOS, use o comando **show run interface** e verifique se a interface está em um **estado de desligamento**:

```
Switch#sh run interface fastEthernet 4/2 ! interface FastEthernet4/2 switchport trunk
encapsulation dot1q switchport mode trunk shutdown duplex full speed 100 end !--- Use the no
shut command in config-if mode to re-enable this interface.
```

Se a porta entra no modo de desligamento imediatamente após uma reinicialização do switch, a causa provável é a configuração de segurança da porta. Se a inundação unicast é permitida nessa porta, pode fazer com que a porta seja desligada após uma reinicialização. A Cisco recomenda que você desabilite a inundação unicast porque isso também garante que nenhuma inundação ocorra na porta uma vez alcançado o limite de endereço MAC.

[O Status da Porta ou da Interface é errDisable](#)

Por padrão, os processos de software dentro do switch podem desligar uma porta ou interface se certos erros forem detectados.

Quando você verifica o comando **show port** para CatOS o status pode ser **errdisable**:

```
switch>(enable) sh port 4/3 Port Name Status Vlan Duplex Speed Type -----
-----
4/3 errdisable 150 auto auto 10/100BaseTX !---
The show port command displays a status of errdisable.
```

Ou use o comando de status **show interface card-type {slot/port}** para Cisco IOS:

```
Router#show int fasteth 2/4 status Port Name Status Vlan Duplex Speed Type Gi2/4 err-disabled 1
full 1000 1000BaseSX !--- The show interfaces card-type {slot/port} status command for Cisco IOS
!--- displays a status of errdisabled. !--- The show interfaces status errdisabled command shows
all the interfaces !--- in this status.
```

O [comando show logging buffer](#) para CatOS e o [comando show logging](#) para o Cisco IOS também exibem mensagens de erro (o formato de mensagem exato varia) que se relacionam ao estado errdisable.

As portas ou entrelaçamentos que estão sendo desabilitados em consequência do errdisable são referidos como motivos em CatOS e causas no Cisco IOS. As razões ou as causas para esse acontecimento variam de configuração incorreta de EtherChannel que causa um flap PAgP, uma incompatibilidade duplex (bidirecional), a proteção de porta e o portfast BPDU configurados ao mesmo tempo, o UDLD que detecta um link de sentido único, etc.

Você tem que reabilitar a porta ou interface manualmente para tirá-la do estado errdisable, a menos que você configure uma opção de recuperação de errdisable. No software CatOS 5.4(1) e mais recente, é possível reabilitar automaticamente uma porta após uma quantidade de tempo configurável gasto no estado errdisable. O Cisco IOS na maioria dos switches também tem essa funcionalidade. A linha inferior é que mesmo que você configure a interface para recuperar-se de errdisable o problema continua ocorrendo até que a causa raiz seja determinada.

Para obter mais informações sobre as causas de recuperação do status errdisable para os switches que executam CatOS, consulte [Recuperação do Estado de Porta errDisable nas Plataformas CatOS](#).

Nota: Use este link como uma referência para o status errdisable nos switches que executam o Cisco IOS, contanto que as causas raiz sejam as mesmas, não importa qual sistema operacional você executa.

Esta tabela mostra uma comparação dos comandos usados para configurar, verificar e fazer troubleshooting do status errdisable nos switches que executam CatOS e Cisco IOS. Escolha um comando para acessar a documentação do comando.

Comandos do errdisable de CatOS	Ação	Comandos do errdisable do Cisco IOS
set errdisable-timeout {enable disable} {reason}	defina ou configure	errdisable detect cause errdisable recovery cause
set errdisable-timeout interval {interval}	defina ou configure	errdisable recovery {interval}
show errdisable-timeout	verifique e faça o troubleshooting	show errdisable detect show interfaces status err-disabled

[O Status da Porta ou da Interface é Inativa](#)

Uma causa comum de portas inativas nos switches que executam CatOS é quando a VLAN a que eles pertencem desaparece. O mesmo problema pode ocorrer nos switches que executam o Cisco IOS quando as interfaces são configuradas como os switchports da camada 2 que usam o [comando switchport](#).

Cada porta em um switch de Camada 2 pertence a uma VLAN. Cada porta em um switch de

Camada 3 configurado para ser um switchport L2 também deve pertencer a uma VLAN. Se essa VLAN for excluída, a porta ou a interface torna-se inativa.

Nota: Alguns switches mostram uma luz laranja(âmbar) em cada porta quando isso acontece.

Para CatOS, use o **show port** ou o comando **show port status** junto com o comando **show vlan** para verificar:

```
Switch> (enable) sh port status 2/2 Port Name Status Vlan Duplex Speed Type -----
----- 2/2 inactive 2 full 1000 1000BaseSX !---
Port 2/2 is inactive for VLAN 2. Switch> (enable) sh vlan VLAN Name Status IfIndex Mod/Ports,
Vlans ----- 1 default
active 5 2/1 !--- VLANs are displayed in order and VLAN 2 is missing.
```

Para o Cisco IOS, use o comando **show interfaces card-type {slot/port} switchport** com **show vlan** para fazer a verificação.

```
Router#sh interfaces fastEthernet 4/47 switchport Name: Fa4/47Switchport: Enabled Administrative
Mode: static access Operational Mode: static access Administrative Trunking Encapsulation:
negotiate Operational Trunking Encapsulation: native Negotiation of Trunking: Off Access Mode
VLAN: 11 ((Inactive)) !--- FastEth 4/47 is inactive. Router#sh vlan VLAN Name Status Ports ----
----- 1 default active
Gi1/1, Gi2/1, Fa6/6 10 UplinkToGSR's active Gi1/2, Gi2/2 !--- VLANs are displayed in order and
VLAN 11 is missing. 30 SDTsw-1ToSDTsw-2Link active Fa6/45
```

Se o switch que excluiu a VLAN é um servidor VTP para o domínio VTP, cada switch e servidor do cliente no domínio também tem a VLAN removida de sua tabela VLAN. Quando você adiciona a VLAN à tabela VLAN novamente a partir de um switch de servidor VTP, as portas dos switches no domínio que pertencem à VLAN restauradas se tornam ativas novamente. Uma porta recorda qual VLAN é atribuída, mesmo se a própria VLAN for excluída.

Consulte [Como Compreender e Configurar o Protocolo VLAN Trunk \(VTP\)](#) para obter mais informações sobre o VTP.

Nota: Se a saída do comando **show interface <interface number> switchport** exibe a porta como uma porta de entroncamento mesmo após ela ser configurada como uma porta de acesso com o comando **switchport access vlan <vlan no: >** comando, emita o comando **switchport mode access** para tornar a porta uma porta de acesso.

[O Status da Interface ou da Porta de Uplink é Inativa](#)

Em uma série Catalyst 4510R, para habilitar a Ethernet de 10 Gigabits e as portas de uplink SFP de Ethernet de Gigabit, existe uma configuração opcional. Para permitir o uso simultâneo da Ethernet de 10 Gigabits e das interfaces SFP de Ethernet de Gigabit, emita o comando **hw-module uplink select all**. Depois que você emitir o comando, reinicialize o switch ou então a saída do comando **show interface status module module number** exibirá a porta de the uplink como inativa.

O Release de Software Cisco IOS 12.2(25)SG oferece suporte para o uso simultâneo de Ethernet de 10 Gigabits e para as interfaces de SFP de Ethernet de Gigabit nos switches do Catalyst 4500.

Nota: Nos switches das séries Catalyst 4503, 4506 e 4507R, essa capacidade é habilitada automaticamente.

[O Contador Adiado da Interface de Switch do Catalyst Começa a Incrementar](#)

O problema ocorre porque a carga de tráfego destinada para o switch é excessiva e faz com que os frames sejam descartados. Normalmente, os frames adiados são o número de frames que foram transmitidos com sucesso após ter esperado pela mídia porque ela estava ocupada. Isso é visto, geralmente, nos ambientes half duplex quando a portadora já está em uso quando tenta transmitir um frame. Mas em ambientes full duplex o problema ocorre quando a carga excessiva é destinada para o switch.

Esta é a solução:

- Faça o hardcode das duas extremidades do link para full duplex de modo que a incompatibilidade da negociação possa ser evitada.
- Altere o cabo e o fio do painel para assegurar-se de que o cabo e os fios de correção não estejam com defeito.

Nota: Se o erro do Contador Adiado incrementa em um GigabitEthernet de um supervisor 720, ative a negociação de velocidade na interface como uma solução alternativa.

[Falha intermitente para ajustar o \[value\] do temporizador da vlan \[vlan no\]](#)

O problema ocorre quando a Lógica de Reconhecimento de Endereço Codificado (EARL) é incapaz de ajustar o tempo de envelhecimento de CAM para a VLAN para o número requerido de segundos. Aqui, o tempo de envelhecimento da VLAN é ajustado para veloz.

Quando a VLAN já está em envelhecimento veloz, o EARL não pode ajustar a VLAN para envelhecimento veloz, e o processo de ajuste do temporizador de envelhecimento é bloqueado. O tempo de envelhecimento de CAM padrão é cinco minutos, o que significa que o switch descarta a tabela de endereços MAC reconhecidos a cada cinco minutos. Isto assegura que a tabela de endereços MAC (a tabela CAM) contenha as entradas mais recentes.

O envelhecimento veloz ajusta temporariamente o tempo de envelhecimento de CAM para o número de segundos que o usuário especifica, e é usado conjuntamente com o processo do Topology Change Notification (TCN). A ideia é que quando uma alteração de topologia ocorre, esse valor seja necessário para descartar mais rapidamente a tabela CAM a fim de compensar a alteração de topologia.

Emita o comando **show cam aging** para verificar o tempo de envelhecimento de CAM no switch. Os TCN e o envelhecimento veloz são razoavelmente raros. Como resultado, a mensagem tem um nível de severidade 3. Se as VLAN estão frequentemente no envelhecimento veloz, verifique o motivo.

O motivo mais comum para TCNs são os PCs clientes conectados diretamente a um switch. Quando você liga ou desliga o PC, a porta de switch muda o estado, e o switch começa o processo TCN. Isso ocorre porque o switch não sabe que o dispositivo conectado é um PC; o switch sabe somente que a porta mudou o estado.

Para resolver esse problema, a Cisco desenvolveu o recurso Portfast para portas de host. Uma vantagem do PortFast é que esse recurso suprime TCN para uma porta de host.

Nota: O PortFast também ignora os cálculos de spanning tree na porta e é, conseqüentemente, apropriado apenas para o uso em uma porta de host.

Para permitir o PortFast na porta, configure um destes comandos:

set spantree portfast mod/port enable | disable

ou

set port host mod/port A Cisco recomenda esse comando se o switch executa CatOS5.4 ou versões mais recentes.

Incompatibilidade do Modo de Entroncamento

Verifique o modo de entroncamento em cada lado do enlace. Assegure-se de que os dois lados estejam no mesmo modo (ambos em entroncamento com o mesmo método: ISL ou 802.1q, ou ambos sem entroncamento). Se você ativa o modo de entroncamento (em oposição a automático ou desejável) para uma porta e a outra porta tem o modo de entroncamento ajustado para off, elas não poderão se comunicar. O entroncamento muda o formato do pacote. As portas precisam estar em acordo a respeito de qual formato elas usam no link ou não conseguirão se comunicar.

Para CatOS, use o comando {mod/port} **show trunk** para verificar o status de entroncamento e as correspondências de VLAN Nativa (para dot1q) nos dois lados.

```
Switch> (enable) sh trunk 3/1 * - indicates vtp domain mismatch Port Mode Encapsulation Status
Native vlan -----
trunking 1 Port Vlans allowed on trunk -----
----- 3/1 1-1005,1025-4094 !--- Output truncated.
```

Para o Cisco IOS, use o comando de entroncamento **show interfaces card-type {mod/port}** para verificar a configuração de entroncamento e a VLAN Nativa.

```
Router#sh interfaces fastEthernet 6/1 trunk Port Mode Encapsulation Status Native vlan Fa6/1
desirable 802.1q trunking 1 Port Vlans allowed on trunk Fa6/1 1-4094 !--- Output truncated.
```

Consulte os seguintes documentos para obter mais informações sobre os modos de entroncamento, as diretrizes e as limitações diferentes:

- [Requisitos de sistema para implementar o entroncamento](#)
- [Página de suporte à tecnologia de truncamento](#)

Jumbos, Giants, e Baby Giants

A Unidade Máxima de Transmissão (MTU) da parte de dados de um quadro ethernet é de 1500 bytes por padrão. Se o tráfego transmitido MTU excede o MTU suportado, o switch não encaminha o pacote. Além disso, dependente do hardware e do software, algumas plataformas do switch incrementam os contadores de erro da porta e da interface em consequência.

- Os jumbo frames não são definidos como parte do padrão Ethernet do Instituto de Engenharia Elétrica e Eletrônica (Institute of Electrical and Electronics Engineers) e são dependentes do fornecedor. Eles podem ser definidos como todo frame maior que o quadro ethernet padrão de 1518 bytes (que inclui o cabeçalho de L2 e a Verificação de Redundância Cíclica (CRC)). Os jumbos têm tamanhos de frame maiores, tipicamente > que 9000 bytes.
- Os frames giant são definidos como qualquer frame acima do o tamanho máximo de um quadro ethernet (maior que 1518 bytes) que tenha um FCS com erro.
- Os frames do Baby Giant são apenas levemente maiores que o tamanho máximo de um quadro ethernet. Tipicamente, isso significa frames de até 1600 bytes de tamanho.

O suporte para jumbo e baby giants nos switches do Catalyst varia por plataforma de switch, à

vezes até mesmo por módulos dentro do switch. A versão de software é igualmente um fator.

Consulte [Configurar o Suporte de Frame Jumbo/Giant nos Switches do Catalyst](#) para obter mais informações sobre os requisitos do sistema, configuração e troubleshooting para problemas de jumbo e baby giant.

[Não foi Possível Efetuar Ping no Dispositivo Final](#)

Verifique o dispositivo final efetuando ping diretamente do switch conectado primeiro e, a seguir, vá de porta para porta, interface por interface, entroncamento por entroncamento, até encontrar o problema de conectividade. Assegure-se de que cada switch possa detectar o endereço MAC do dispositivo final em sua tabela de CAM (Memória de Conteúdo Endereçável).

Para CatOS, use o comando {mod/port} [show cam dynamic](#) .

```
Switch> (enable) sh cam dynamic 3/1 * = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry. X = Port Security Entry $ = Dot1x Security Entry VLAN Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type] -----  
----- 2 00-40-ca-14-0a-b1 3/1 [ALL] !--- A workstation on VLAN 2 with MAC address 00-40-ca-14-0a-b1 is seen in the CAM table !--- on the trunk port of a switch running CatOS.  
Total Matching CAM Entries Displayed =1 Console> (enable)
```

Para o Cisco IOS, use o [comando how mac address-table dynamic](#) ou substitua a palavra-chave da interface.

```
Router# sh mac-address-table int fas 6/3 Codes: * - primary entry vlan mac address type learn qos ports -----+-----+-----+-----+-----+----- * 2  
0040.ca14.0ab1 dynamic No -- Fa6/3 !--- A workstation on VLAN 2 with MAC address 0040.ca14.0ab1 is directly connected !--- to interface fastEthernet 6/3 on a switch running Cisco IOS.
```

Uma vez que você souber que o switch tem realmente o endereço MAC do dispositivo em sua tabela CAM, determine se esse dispositivo está na mesma VLAN ou em uma VLAN diferente de onde você está tentando fazer o ping.

Se o dispositivo final estiver em uma VLAN diferente de onde você esteja fazendo o ping, um switch ou roteador L3 deve ser configurado para permitir que os dispositivos se comuniquem. Assegure-se de que seu endereçamento L3 no dispositivo final e no switch do router/ L3 esteja configurado corretamente. Verifique o endereço IP, a máscara de sub-rede, o gateway padrão, a configuração do protocolo de roteamento dinâmico, as rotas estáticas, etc.

[Como Usar Set Port Host ou Switchport Host para Fixar Atrasos de Inicialização](#)

Se as estações não podem se comunicar com seus servidores principais ao conectarem-se através de um switch, o problema pode envolver atrasos na porta de switch que se torna ativa depois que o link da camada física for ativado. Em alguns casos, esses atrasos podem durar até 50 segundos.

Algumas estações de trabalho simplesmente não podem esperar tudo isso antes de encontrar seu servidor sem desistir. Esses atrasos são causados pelo STP, pelas negociações de entroncamento (DTP) e pelas negociações de EtherChannel (PAgP). Todos esses protocolos podem ser desabilitados para as portas de acesso onde não são necessários, para que a porta de switch ou da interface comece a encaminhar pacotes alguns segundos depois que estabelece um link com seu dispositivo vizinho.

[O comando set port host foi introduzido na versão CatOS 5.4.](#) Este comando define os modos de

canal e entroncamento como desativados e coloca a porta em um estado de encaminhamento STP.

```
Switch> (enable) set port host 3/5-10 Port(s) 3/5-10 channel mode set to off. !--- The set port host command also automatically turns off etherchannel on the ports. 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. !--- Notice the switch warns you to only enable port host on access ports. Spanntree ports 3/5-10 fast start enabled. Dot1q tunnel feature disabled on port(s) 3/5-10. Port(s) 3/5-10 trunk mode set to off. !--- The set port host command also automatically turns off trunking on the ports.
```

Nota: Para versões CatOS mais recentes do que a versão 5.4, o [comando set spanntree portfast {mod/port} enable](#) foi usado. Nas versões atuais do CatOS, você ainda tem a opção de usar somente esse comando, mas ele exige que você desligue o entroncamento e o etherchannel separadamente para ajudar a fixar atrasos de inicialização da estação de trabalho. Os comandos adicionais que fazem isso são: [set port channel {mod/port} off](#) e [set trunk {mod/port} off](#).

Para o Cisco IOS, você pode usar o [comando switchport host](#) para desabilitar a canalização e habilitar o portfast de spanning tree e o [comando switchport nonegotiate](#) para desligar pacotes da negociação de DTP. Use o [comando nterface-range](#) para fazer isso em várias interfaces de uma vez.

```
Router6k-1(config)#int range fastEthernet 6/13 - 18 Router6k-1(config-if-range)#switchport  
Router6k-1(config-if-range)#switchport host switchport mode will be set to access spanning-tree  
portfast will be enabled channel group will be disabled !--- Etherchannel is disabled and  
portfast is enabled on interfaces 6/13 - 6/18. Router6k-1(config-if-range)#switchport  
nonegotiate !--- Trunking negotiation is disabled on interfaces 6/13 - 6/18. Router6k-1(config-  
if-range)#end Router6k-1#
```

O Cisco IOS tem a opção de usar o **comando padrão global spanning-tree portfast** para aplicar automaticamente o portfast em qualquer interface configurada como um switchport de acesso da camada 2. Verifique a Referência de Comandos de seu release de software para verificar a disponibilidade desse comando. Você pode usar também o [comando spanning-tree portfast](#) por interface, mas ele exige que você desligue o entroncamento e o etherchannel separadamente para ajudar a corrigir atrasos de inicialização da estação de trabalho.

Consulte [Utilização de Portfast e de Outros Comandos para Corrigir Atrasos da Conectividade de Inicialização de Estação de Trabalho](#) para obter mais informações sobre como corrigir atrasos de inicialização.

[Problemas de Velocidade/Duplex, Autonegociação ou Placa de Rede](#)

Se você tem uma grande quantidade de erros de alinhamento, erros de FCS ou de colisões posteriores, isso pode indicar o seguinte:

- Incompatibilidade duplex
- Cabo com erro ou danificado
- Problemas de Placa de Rede

Incompatibilidade duplex

Um problema comum com velocidade/duplex é quando as configurações duplex são mal combinadas entre dois switches, entre um switch e um roteador ou entre o switch e uma estação de trabalho ou um servidor. Isso pode ocorrer quando o hardcode da velocidade ou do duplex é feito manualmente ou devido a problemas de negociação automática entre os dois dispositivos.

Se a má combinação ocorre entre dois dispositivos Cisco com o Cisco Discovery Protocol (CDP) habilitado, você vê as mensagens de erro de CDP na console ou no buffer de registro dos dois dispositivos. O CDP é útil para detectar erros, assim como para estatísticas de sistema e de porta em dispositivos Cisco próximos. O CDP é propriedade da Cisco e funciona enviando pacotes a um endereço MAC bem conhecido 01-00-0C-CC-CC-CC.

O exemplo mostra as mensagens de log que resultam de uma incompatibilidade duplex entre dois switches da série Catalyst 6000: um que executa CatOS e o outro que executa o Cisco IOS. Essas mensagens, geralmente, informam qual é a incompatibilidade e onde ocorre.

```
2003 Jun 02 11:16:02 %CDP-4-DUPLEXMISMATCH:Full/half duplex mismatch detected on port 3/2
!--- CatOS switch sees duplex mismatch. Jun 2 11:16:45 %CDP-4-DUPLEX_MISMATCH: duplex mismatch
discovered on FastEthernet6/2 (not half duplex), with TBA04251336 3/2 (half duplex). !--- Cisco
IOS switch sees duplex mismatch.
```

Para CatOS, use o comando de detalhes [show cdp neighbor \[mod/port\]](#) para exibir informações de CDP para dispositivos Cisco próximo.

```
Switch> (enable) sh cdp neighbor 3/1 detail Port (Our Port): 3/1 Device-ID: Router Device
Addresses: IP Address: 10.1.1.2 Holdtime: 133 sec Capabilities: ROUTER SWITCH IGMP Version:
Cisco Internetwork Operating System Software IOS (tm) c6sup2_rp Software (c6sup2_rp-PK2S-M),
Version 12.1(13)E6, EARLY DEPL OYMENT RELEASE SOFTWARE (fc1) TAC Support:
http://www.cisco.com/tac Copyright (c) 1986-2003 by cisco Systems, Inc. Compiled Fri 18-Apr-03
15:35 by hqluong Platform: cisco Catalyst 6000 Port-ID (Port on Neighbors's Device):
FastEthernet6/1 !--- Neighbor device to port 3/1 is a Cisco Catalyst 6000 Switch on !--- FastEth
6/1 running Cisco IOS. VTP Management Domain: test1Native VLAN: 1 Duplex: full !--- Duplex is
full. System Name: unknown System Object ID: unknown Management Addresses: unknown Physical
Location: unknown Switch> (enable)
```

Para Cisco IOS, use o comando de detalhe [show cdp neighbors card-type {slot/port}](#) para exibir informações de CDP para dispositivos Cisco próximos.

```
Router#sh cdp neighbors fastEthernet 6/1 detail ----- Device ID: TBA04251336
Entry address(es): IP address: 10.1.1.1 Platform: WS-C6006, Capabilities: Trans-Bridge Switch
IGMP Interface: FastEthernet6/1, Port ID (outgoing port): 3/1 Holdtime : 152 sec Version : WS-
C6006 Software, Version McpSW: 6.3(3) NmpSW: 6.3(3) Copyright (c) 1995-2001 by Cisco Systems !-
- Neighbor device to FastEth 6/1 is a Cisco Catalyst 6000 Switch !--- on port 3/1 running CatOS.
advertisement version: 2 VTP Management Domain: 'test1' Native VLAN: 1 Duplex: full !--- Duplex
is full. Router#
```

Configurar a velocidade/duplex automática em um lado e 100/Full duplex no outro lado também é um erro de configuração e pode conduzir a uma incompatibilidade de duplex. Se a porta de switch recebe um lote de colisões posteriores, isso, geralmente, indica um problema de incompatibilidade duplex e pode fazer com que a porta seja colocada em um status errdisable. O lado half duplex espera somente pacotes em horários específicos e, não a qualquer hora e, portanto, conta os pacotes recebidos na hora errada como colisões. Existem outras causas para colisões posteriores além da incompatibilidade duplex, mas esse é um dos motivos mais comuns. Sempre configure os dois lados da conexão para negociar automaticamente a velocidade/duplex ou configurar a velocidade/duplex manualmente nos dois lados.

Para CatOS, use o comando de [mod/port] [show port](#) status para exibir o status da velocidade e do duplex, assim como outras informações. Use os [comandos set port speed](#) e [set port duplex](#) para fazer o hardcode dois lados para 10 ou 100 e half ou full, conforme necessário.

```
Switch> (enable) sh port status 3/1 Port Name Status Vlan Duplex Speed Type -----
-----
3/1 connected 1 a-full a-100 10/100BaseTX
Switch> (enable)
```

Para Cisco IOS, use o comando de status [show interfaces](#) card-type {slot/port} para exibir configurações de velocidade e duplex, assim como outras informações. Use os [comandos speed and duplex](#) do modo de configuração da interface para fazer o hardcode dos dois lados como 10

ou 100 e half ou full, conforme necessário.

```
Router#sh interfaces fas 6/1 status Port Name Status Vlan Duplex Speed Type Fa6/1 connected 1 a-  
full a-100 10/100BaseTX
```

Se você usa o comando **show interfaces** sem a opção de **status**, verá uma configuração de velocidade e duplex, mas não saberá se essa velocidade e duplex foram ou não alcançados com a negociação automática.

```
Router#sh int fas 6/1 FastEthernet6/1 is up, line protocol is up (connected) Hardware is C6k  
100Mb 802.3, address is 0009.11f3.8848 (bia 0009.11f3.8848) MTU 1500 bytes, BW 100000 Kbit, DLY  
100 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set  
Full-duplex, 100Mb/s !--- Full-duplex and 100Mbps does not tell you whether autoneg was used to  
achieve this. !--- Use the sh interfaces fas 6/1 status command to display this.
```

Cabo com erro ou danificado

Verifique sempre o cabo para ver se há dano ou falha marginal. Um cabo pode ser bom o suficiente para conectar-se na camada física, mas corrompe pacotes em consequência de dano sutil à fiação ou aos conectores. Verifique ou troque o cabo de cobre ou de fibra. Troque o GBIC (se removível) para conexões de fibra ótica. Descarte quaisquer conexões do painel de correção ou conversores de mídia com erro entre a origem e o destino. Teste o cabo em outra porta ou interface se um estiver disponível e veja se o problema continua.

Problemas de auto negociação e Placa de Rede

Os problemas ocorrem, às vezes entre switches Cisco e determinadas Placas de Rede de terceiros. Por padrão, as portas e as interfaces de switch do Catalyst são configuradas para negociação automática. É comum para dispositivos como laptops ou os outros dispositivos ser configurados para fazer a negociação automática também, embora ocorram problemas de negociação automática algumas vezes.

Para pesquisar problemas de negociação automática recomenda-se frequentemente tentar fazer o hardcoding nos dois lados. Se nem a negociação automática ou hardcoding funcionarem, pode haver um problema com o firmware ou com o software em sua Placa de Rede. Faça o upgrade do driver da Placa de Rede para a versão mais recente disponível no site do fabricante para resolver isso.

Consulte [Configurar e Fazer o Troubleshooting de Negociação Automática Half/Full Duplex de Ethernet de 10/100/1000 MB](#) para obter detalhes sobre como resolver problemas de velocidade/duplex e de negociação automática.

Consulte [Troubleshooting dos Switches do Cisco Catalyst para Problemas de Compatibilidade de Placa de Rede](#) para obter detalhes sobre como resolver problemas de placa de rede de terceiros.

Loops de Spanning Tree

Os loops de Spanning Tree Protocol (STP) podem causar problemas graves de desempenho que passam por problemas de porta ou de interface. Nessa situação, sua largura de banda é usada pelos mesmos frames a toda hora, que deixam pouco espaço para o tráfego legítimo.

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

necessariamente a porta de bloqueio de STP) não recebe mais BPDUs de STP. Nessa operação, o STP depende da recepção contínua ou da transmissão dos BPDUs com base na função da porta. A porta designada transmite BPDUs e a porta não designada recebe BPDUs.

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

O recurso protetor de loop faz verificações adicionais. Se os BPDUs não são recebidos em uma porta não designada, e o protetor de loop está habilitado, a porta muda para o estado de bloqueio inconsistente de loop de STP, em vez do estado de escuta/aprendizagem/ encaminhamento. Sem o recurso protetor de loop, a porta assume a função de porta designada. A porta muda para o estado de encaminhamento STP e cria um loop. Consulte [Aprimoramentos de Spanning-Tree Protocol Usando os Recursos de Detecção de Desvio BPDUs](#) para obter mais informações sobre o recurso protetor de loop.

Este documento aborda os motivos que fazem o STP falhar, quais informações procurar para identificar a origem do problema e que tipo de design minimiza os riscos STP.

Os loops também podem ser causados por um link unidirecional. Para obter mais informações, consulte UDLD: Seção dos problemas do link de sentido único deste documento.

[UDLD: Link de Sentido Único](#)

Um link unidirecional é um link onde o tráfego sai de um caminho, mas nenhum tráfego é recebido de volta. O switch não sabe que o link que volta tem erros (a porta pensa que o link está ativo e funcionando).

Um cabo de fibra quebrado ou outros problemas de porta/cabeamento podem ocasionar essa comunicação apenas em sentido único. Esses links parcialmente funcionais podem causar problemas tais como loops STP quando os switches envolvidos não sabem que o link está parcialmente quebrado. O UDLD pode pôr uma porta no estado errdisable quando detecta um link unidirecional. O comando `udld aggressive-mode` pode ser configurado nos switches que executam CatOS e Cisco IOS (verifique as notas de release para a disponibilidade do comando) para conexões ponto a ponto entre os switches onde os links que não funcionam direito não podem ser tolerados. O uso desse recurso pode ajudá-lo a identificar problemas de link unidirecional difíceis de encontrar

Consulte [Como Compreender e Configurar o Protocolo de Detecção de Link Unidirecional \(UDLD\)](#) para obter informações de configuração sobre o UDLD.

[Frames Adiados \(Out-Lost or Out-Discard\)](#)

Se você tem um grande número de frames adiados ou Out-Discard (também referidos como Out-Lost em algumas plataformas), significa que os buffers de saída do switch estão acima da capacidade e o switch precisou descartar esses pacotes. Isso pode ser um sinal que esse segmento está sendo executado em uma velocidade e/ou duplex inferior ou há tráfego demais atravessando a porta.

Para CatOS, use o comando `show mac` para o módulo e a porta ou o módulo inteiro para verificar out-discards:

```

MAC          Dely-Exced MTU-Exced  In-Discard Out-Discard
-----
2/1          0          -          0          10175888 2/2 0 - 0 9471889 2/3 0 - 0 9095371 2/4 0 -
0 8918785 !--- The show mac command run on mod 2 at different intervals shows !--- the out-
discard counter incrementing.

```

Para o Cisco IOS, use o [comando show interfaces counters error](#).

```

Router#show interfaces counters error Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize
OutDiscards Fa7/47 0 0 0 0 0 0 Fa7/48 0 0 0 0 0 2871800 Fa8/1 0 0 0 0 0 2874203 Fa8/2 103 0 0
103 0 2878032 Fa8/3 147 0 0 185 0 0 Fa8/4 100 0 0 141 0 2876405 Fa8/5 0 0 0 0 0 2873671 Fa8/6 0
0 0 0 0 2 Fa8/7 0 0 0 0 0 0 !--- The show interfaces counters errors command shows certain
interfaces !--- incrementing large amounts of OutDiscards while others run clean.

```

Investigue as causas comuns de falhas do buffer de saída:

Speed/Duplex Inferior para a Quantidade de Tráfego

Sua rede pode enviar muitos pacotes através dessa porta para que a porta controle em sua configuração de velocidade/duplex atual. Isso pode acontecer onde existem várias portas de alta velocidade fluindo para uma única porta (geralmente mais lenta). Você pode mover o dispositivo que fica parado nessa porta para uma mídia mais rápida. Por exemplo, se a porta é de 10 Mbps, mova esse dispositivo para uma porta de Gigabit ou de 100 Mbps. Você pode mudar a topologia para rotear os frames de forma diferente.

Problemas de congestionamento: Segmento Muito Ocupado

Se o segmento é compartilhado, os outros dispositivos nesse segmento podem transmitir tanto que o switch não tem nenhuma oportunidade de transmitir. Evite os hubs com encadeamento em margarida sempre que possível. O congestionamento pode conduzir à perda de pacotes. A perda de pacotes causa retransmissões na camada de transporte que faz com que os usuários experimentem a latência no nível do aplicativo. Você pode fazer upgrade de links de 10Mbps para 100Mbps para links de Ethernet de Gigabit quando possível. Você pode remover alguns dispositivos dos segmentos aglomerados para outros segmentos menos povoados. Faça com que sua prioridade seja evitar o congestionamento da rede.

Aplicativos

Às vezes, as características da transmissão de tráfego das aplicações usadas podem causar problemas no buffer de saída. Transferências de arquivo NFS que vêm de um servidor de Gigabit anexado e que usa o protocolo UDP com um tamanho de janela de 32K são um exemplo de uma configuração de aplicativo que pode trazer para esse tipo de problema. Se você verificou ou tentou as outras sugestões deste documento (verificou a velocidade/duplex, nenhum erro físico no link, todo o tráfego é tráfego válido normal, e assim por diante) então, reduzir o tamanho da unidade que é enviada pelo aplicativo pode ajudar a aliviar esse problema.

[Problemas de Software](#)

Se você vê o comportamento que pode somente ser considerado “estranho,” pode isolar o comportamento em um local específico e verificou tudo o que foi sugerido até agora, isso pode indicar problemas de software ou hardware. Geralmente, é mais fácil fazer o upgrade do software do que do hardware. Mude o software primeiro.

Para CatOS, use o [comando show version](#) para verificar a versão de software atual e a memória flash livre para o upgrade.


```
Switch> (enable) sh ver WS-C6006 Software, Version NmpSW: 6.3(3) Copyright (c) 1995-2001 by
Cisco Systems NMP S/W compiled on Oct 29 2001, 16:50:33 System Bootstrap Version: 5.3(1)
Hardware Version: 2.0 Model: WS-C6006 Serial #: TBA04251336 PS1 Module: WS-CAC-1300W Serial #:
SON04201377 PS2 Module: WS-CAC-1300W Serial #: SON04201383 Mod Port Model Serial # Versions ---
----- 1 2 WS-X6K-SUP1A-2GE
SAD041901PP Hw : 3.6 Fw : 5.3(1) Fw1: 5.4(2) Sw : 6.3(3) Sw1: 6.3(3) WS-F6K-PFC SAD041803S3 Hw :
2.0 !--- Output truncated. DRAM FLASH NVRAM Module Total Used Free Total Used Free Total Used
Free ----- 1 65408K 47274K
18134K 16384K 14009K 2375K 512K 308K 204K !--- Typical CatOS show version output. !--- Verify
free memory before upgrading. Uptime is 32 days, 4 hours, 44 minutes Console> (enable)
```

Para o Cisco IOS, use o [comando show version](#) para verificar a versão de software atual junto com o **dir flash:** ou **dir bootflash:** (dependendo da plataforma) o comando para verificar a memória Flash disponível para o upgrade:

```
Router#sh ver Cisco Internetwork Operating System Software IOS (tm) Catalyst 4000 L3 Switch
Software (cat4000-IS-M), Version 12.1(13)EW, EA RLY DEPLOYMENT RELEASE SOFTWARE (fcl) TAC
Support: http://www.cisco.com/tac Copyright (c) 1986-2002 by cisco Systems, Inc. Compiled Fri
20-Dec-02 13:52 by eaarmas Image text-base: 0x00000000, data-base: 0x00E638AC ROM: 12.1(12r)EW
Dagobah Revision 71, Swamp Revision 24 trunk-4500 uptime is 2 weeks, 2 days, 6 hours, 27 minutes
System returned to ROM by redundancy reset System image file is "bootflash:cat4000-is-mz.121-
13.EW.bin" !--- Typical Cisco IOS show version output. Router#dir bootflash: Directory of
bootflash:/ 1 -rw- 8620144 Mar 22 2002 08:26:21 cat4000-is-mz.121-13.EW.bin 61341696 bytes total
(52721424 bytes free) !--- Verify available flash memory on switch running Cisco IOS. Router
```

Como Fazer o Upgrade do Software

Para obter informações sobre o upgrade de software para os switches do Catalyst, escolha sua plataforma em LAN & Switches de Modo de Transferência Assíncrona (Asynchronous Transfer Mode) e verifique a seção Configuração de Software> Upgrade de Software e o Trabalho com os Arquivos de Configuração.

Incompatibilidade de Hardware e Software

Pode haver uma situação onde o software não seja compatível com o hardware. Isso acontece quando o novo hardware é lançado exige suporte especial do software. Para obter mais informações sobre compatibilidade de software, use a ferramenta Software Advisor.

Bugs de software

O sistema operacional pode ter um bug. Se você carregar uma versão de software mais nova, ela pode, frequentemente, corrigir isso. Você pode procurar bugs de software conhecido com Software Bug Toolkit.

Imagens corrompidas

Uma imagem pode ter se tornado corrompida ou está faltando. Para obter informações sobre recuperação das imagens corrompidas, escolha sua plataforma em LAN & Switches Modo de Transferência Assíncrona (Asynchronous Transfer Mode) e verifique a seção Troubleshooting > Recuperação de Software Corrompido ou Ausente.

[Problemas de Hardware](#)

Verifique os resultados de [módulo show](#) para ver se há switches das séries Catalyst 6000 e 4000 que executam CatOS ou Cisco IOS.

```
Switch> (enable) sh mod Mod Slot Ports Module-Type Model Sub Status ---
----- 1 1 2 1000BaseX Supervisor WS-X6K-S2U-MSFC2 yes ok
```

15 1 1 Multilayer Switch Feature WS-F6K-MSFC2 no ok 3 3 8 1000BaseX Ethernet WS-X6408A-GBIC no **faulty** 5 5 48 10/100BaseTX Ethernet WS-X6348-RJ-45 no **faulty** !--- Status of "faulty" indicates a possible hardware problem. !--- This could be a line card problem, but since two mods are effected, !--- perhaps there's a problem with the supervisor. !--- Use the **reset** command (CatOS) or **hw-module{mod}reset** command (Cisco IOS), !--- or try physically reseating the modules and the supervisor. !--- Also, try moving the supervisor to slot 2.

Verifique os resultados dos resultados de POST do switch para ver se existe alguma falha indicada para parte do switch. Falhas de algum teste de um módulo ou porta exibem um "F" nos resultados.

Para CatOS, use o [comando show test](#) para ver todos os resultados do teste. A fim ver os resultados de teste por módulo, use o comando {mod} show test :

```
Switch> (enable) sh test 3 Diagnostic mode: complete (mode at next reset: minimal) !--- The
diaglevel is set to complete which is a longer but more thorough test. !--- The command to do
this for CatOS is set test diaglevel complete. Module 3 : 16-port 1000BaseX EthernetLine Card
Status for Module 3 : PASS Port Status : Ports 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 -----
----- . . . . . GBIC Status : Ports
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 ----- . .
. . . N . . . . . N N Line Card Diag Status for Module 3 (. = Pass, F = Fail, N = N/A)
Loopback Status [Reported by Module 1] : Ports 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 -----
----- F F F F F F F F F F F F F F F F F F F F !--- The failed
loopback tests mean the ports are currently unusable. !--- Use the reset {mod} command or, if
necessary, physically reseate the !--- module to try and fix this problem. !--- If these steps
fail, open a case with Cisco Technical Support.
```

Para o Cisco IOS, em switches modulares como o Cat6000 e o 4000, use o comando show diagnostics. Para ver os resultados de POST por módulo, use o comando [{mod} show diagnostics module](#).

```
ecsj-6506-d2#sh diagnostic module 3 Current Online Diagnostic Level = Minimal !--- The
diagnostic level is set to minimal which is a shorter, !--- but also less thorough test result.
!--- You may wish to configure diagnostic level complete to get more test results. Online
Diagnostic Result for Module 3 : MINOR ERROR Online Diagnostic Level when Line Card came up =
Minimal Test Results: (. = Pass, F = Fail, U = Unknown) 1 . TestLoopback : Port 1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 -----
----- . . . . . F F F F F F !--- Notice the
MINOR ERROR test result and failed loopback test which means !--- these ports are currently
unusable. !--- Use the hw-module{mod}reset command or, if necessary, physically reseate the !---
module to try and fix this problem. !--- If these steps fail, open a case with Cisco Technical
Support.
```

Nota: Para os switches das Séries Catalyst 3750, 3550, 2970, 2950/2955 e 2900/3500XL use o **comando show post**, que indica uma passagem ou uma falha simples para o status do hw. Use os LEDs desses switches para ajudá-lo a compreender os resultados do POST. Consulte [Como Compreender Resultados de Post](#).

Para obter mais informações sobre troubleshooting de problemas de hardware nos switches do Catalyst que executam CatOS e Cisco IOS, vá para as páginas de suporte [LAN e Switches de Modo de Transferência Assíncrona \(Asynchronous Transfer Mode\)](#) , escolha sua plataforma e examine a seção **Troubleshooting > Hardware**.

Para possíveis problemas relativos aos Field Notices, consulte [Field Notices](#) para LAN e Switches do Modo de Transferência Assíncrona (Asynchronous Transfer Mode).

[Erros de Entrada em uma Interface da Camada 3 Conectada a um Switchport da Camada 2](#)

Por padrão, todas as portas de camada 2 estão no modo dinâmico desejável para que a porta da

camada 2 tente formar um link de truncamento ou pacotes de DTP para o dispositivo remoto. Quando uma interface da camada 3 é conectada a um switchport da camada 2, não pode interpretar esses frames que resultam em erros de Entrada, erros WrongEncap e quedas de fila de Entrada.

Para resolver isso, altere o modo da porta de switch para acesso estático ou entroncamento, conforme necessário.

```
Switch2(config)#int fa1/0/12
Switch2(config-if)#switchport mode access
OU
```

```
Switch2(config)#int fa1/0/12
Switch2(config-if)#switchport trunk encapsulation dot1q Switch2(config-if)#switchport mode trunk
```

[Incrementação Rápida de Erros de Entrada e do Contador Rx-No-Pkt-Buff](#)

O contador do Rx-No-Pkt-Buff pode aumentar em portas onde possui blades, tais como WS-X4448-GB-RJ45, WS-X4548-GB-RJ45 e WS-X4548-GB-RJ45V. Da mesma forma, alguma incrementação de descarte de pacotes é normal e é o resultado de estouro de tráfego.

Esses tipos de erros aumentam rapidamente, especialmente quando o tráfego que passa por esse link está elevado ou tem dispositivos, tais como servidores conectados à interface. Essa carga elevada de tráfego causa sobreassinatura nas portas, o que esgota os buffers de entrada e faz com que o contador Rx-No-Pkt-Buff e os erros de entrada aumentem rapidamente.

Se um pacote não pode ser recebido completamente porque o switch está fora dos buffers de pacotes, esse contador é incrementado uma vez para cada pacote descartado. Esse contador indica o estado interno dos Switching ASICs no Supervisor e não indica necessariamente uma condição de erro.

Frames de Pausa

Quando a parte receptora (RX) da porta tem sua fila de FIFO RX completa e alcança o nível mais elevado, a parte transmissora (Tx) da porta começa a gerar frames de pausa com um valor de intervalo mencionado. Espera-se que o dispositivo remoto pare/reduza a transmissão de pacotes para o tempo de intervalo mencionado no frame de pausa.

Se o RX pode apagar a fila de RX ou alcançar um nível baixo dentro desse intervalo, o Tx envia um frame de pausa especial que mencione o intervalo como zero (0x0). Isso permite que o dispositivo remoto comece a transmitir pacotes.

Se o RX ainda funciona na fila, uma vez que o tempo de intervalo expire, o Tx envia um frame de pausa novo outra vez com um valor diferente de intervalo.

Se Rx-No-Pkt-Buff for zero ou não incrementa e o contador de TxPauseFrames incrementa, indica que nosso switch gera frames de pausa e a extremidade remota obedece e por isso, a fila de FIFO RX se esgota.

Se o TxPauseFrames incrementa e o TxPauseFrames também, significa que a extremidade remota negligencia os frames de pausa (não suporta o controle de fluxo) e continua a enviar o tráfego apesar dos frames de pausa. Para superar essa situação, configure manualmente a velocidade e o duplex e desabilite o controle de fluxo, se for necessário.

Esses tipos de erros na interface são relacionados a um problema de tráfego com as portas com sobreassinatura. Os módulos de switching WS-X4448-GB-RJ45, WS-X4548-GB-RJ45 e WS-X4548-GB-RJ45V têm 48 portas com sobreassinaturas em seis grupos de oito portas cada:

- Portas 1, 2, 3, 4, 5, 6, 7, 8
- Portas 9, 10, 11, 12, 13, 14, 15, 16
- Portas 17, 18, 19, 20, 21, 22, 23, 24
- Portas 25, 26, 27, 28, 29, 30, 31, 32
- Portas 33, 34, 35, 36, 37, 38, 39, 40
- Portas 41, 42, 43, 44, 45, 46, 47, 48

As oito portas dentro de cada grupo usam os circuitos comuns que multiplexam eficazmente o grupo em uma única conexão sem bloqueio de Ethernet de Gigabit full duplex para switch fabric interno. Para cada grupo de oito portas, os frames que são recebidos são colocados no buffer e enviados ao link de Ethernet de Gigabit comum para o switch fabric interno. Se a quantidade de dados recebidos para uma porta começa a exceder a capacidade do buffer, o controle de fluxo envia frames de pausa à porta remota para parar o tráfego temporariamente e impedir a perda de frame.

Se os frames recebidos em qualquer grupo excedem a largura de banda de 1 Gbps, o dispositivo começa a descartar os frames. Esses descartes não são óbvios porque são descartados no ASIC interno em vez das interfaces reais. Isso pode retardar o throughput dos pacotes através do dispositivo.

O Rx-No-Pkt-Buff não depende da taxa do tráfego total. Depende da quantidade de pacotes que estão armazenados no buffer FIFO RX do módulo ASIC. O tamanho desse buffer é somente 16 KB. Está contado com fluxos curtos de estouro de tráfego quando alguns pacotes enchem esse buffer. Assim, o Rx-No-Pkt-Buff em cada porta pode ser contado quando a taxa do tráfego total desse grupo de porta ASIC excede 1 Gbps, desde que WS-X4548-GB-RJ45 seja um módulo com sobreassinaturas de 8:1.

Quando você tem os dispositivos que precisam carregar uma grande quantidade de tráfego através dessa interface, considere o uso de uma porta de cada grupo de modo que os circuitos comuns que compartilham um único grupo não sejam afetados por essa quantidade de tráfego. Quando o módulo de switching de Ethernet de Gigabit não é utilizado inteiramente, você pode conectar conexões de porta de equilíbrio através dos agrupamentos de porta para maximizar a largura de banda disponível. Por exemplo, com o módulo de switching WS-X4448-GB-RJ45 10/100/1000, você pode conectar portas de grupos diferentes, tais como as portas 4, 12, 20 ou 30 (em qualquer ordem), antes que você conecte portas do mesmo grupo, como as portas 1, 2, 3, 5, 6, 7 e 8.

Se isso não resolver o problema, você precisa considerar um módulo sem nenhuma sobreassinatura das portas.

[Compreenda gotas do protocolo desconhecido](#)

As gotas do protocolo desconhecido são um contador na relação. É causada pelos protocolos que não são compreendidos pelo roteador/interruptor.

Este exemplo do comando do [show running-config interface](#) mostra às gotas do protocolo desconhecido no Ethernet Gigabit 0/1 de relação.

```
Switch#sh run int Gig 0/1 GigabitEthernet0/1 is up, line protocol is up Hardware is BCM1125
```

```
Internal MAC, address is 0000.0000.0000 (via 0000.0000) MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation 802.1Q Virtual LAN, Vlan ID 1., loopback not set Keepalive set (10 sec) Full-duplex, 1000Mb/s, media type is RJ45 output flow-control is XON, input flow-control is XON ARP type: ARPA, ARP Timeout 04:00:00 Last input 00:00:05, output 00:00:03, output hang never Last clearing of "show interface" counters 16:47:42 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing strategy: fifo Output queue: 0/40 (size/max) 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec 3031 packets input, 488320 bytes, 0 no buffer Received 3023 broadcasts, 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored 0 watchdog, 63107 multicast, 0 pause input 0 input packets with dribble condition detected 7062 packets output, 756368 bytes, 0 underruns 0 output errors, 0 collisions, 0 interface resets 2015 unknown protocol drops 4762 unknown protocol drops 0 babbles, 0 late collision, 0 deferred 0 lost carrier, 0 no carrier, 0 pause output 0 output buffer failures, 0 output buffers swapped out
```

As gotas do protocolo desconhecido são deixadas cair normalmente porque a relação onde estes pacotes são recebidos não é configurada para este tipo de protocolo, ou pode ser todo o protocolo que o roteador não reconhecer.

Por exemplo, se você tem dois roteadores conectados e você desabilita o CDP em uma interface do roteador, isto conduz às gotas do protocolo desconhecido nessa relação. Os pacotes de CDP são reconhecidos já não, e são deixados cair.

[Entroncamento entre um Switch e um Roteador](#)

Os links de entroncamento entre um switch e um roteador podem fazer o switchport ser desativado. O entroncamento pode ser ativado depois que você desabilitar e habilitar o switchport, mas eventualmente o switchport pode ser desabilitado outra vez.

Para resolver esse problema, siga estas etapas:

1. Assegure-se de que o Cisco Discovery Protocol (CDP) seja executado entre o switch e o roteador e de que um detecte o outro.
2. Desabilite os **keepalives** na interface do roteador.
3. Reconfigure o encapsulamento de entroncamento em ambos os dispositivos.

Quando os keepalives estão desabilitados, o CDP permite que o link opere normalmente.

[Problemas de Conectividade Devido à Sobreassinatura](#)

Quando você usa os módulos WS-X6548-GE-TX ou WS-X6148-GE-TX, há uma possibilidade de a utilização da porta individual ocasionar problemas de conectividade ou perda de pacotes nas interfaces próximas. Consulte [Problemas de Conectividade de Interface/Módulo](#) para obter mais informações sobre a sobreassinatura.

[Subinterfaces nos Módulos SPA](#)

Nos módulos SPA, depois que você cria uma subinterface com o 802.1Q, a mesma VLAN não é útil no switch. Uma vez encapsulado o dot1q em uma subinterface, você não poderá mais usar essa VLAN no sistema porque o 6500 ou o 7600 internamente alocam a VLAN e fazem dessa subinterface seu único membro.

Para resolver esse problema, crie portas de entroncamento em vez de subinterfaces. Dessa maneira, a VLAN pode ser vista em todas as interfaces.

Troubleshooting de rxTotalDrops

Se todos os contadores restantes estiverem zerados e o único contador de erro que reporta for o rxTotalDrops, a causa mais provável é que Spanning Tree bloqueia uma ou mais VLANs na porta de uplink e faz com que Color Blocking Logic (CBL) seja descartada.

```
6509> (enable) show counters 1/2
64 bit counters
0  rxHCTotalPkts           =          32513986812
1  txHCTotalPkts           =          29657802587
2  rxHCUnicastPkts         =          18033363526
3  txHCUnicastPkts         =          29498347453
4  rxHCMulticastPkts       =          13469995420
5  txHCMulticastPkts       =           21719352
6  rxHCBroadcastPkts       =           757199011
7  txHCBroadcastPkts       =           137735782
8  rxHCOctets              =        25149393527621
9  txHCOctets              =        23336028193116
10 rxTxHCPkts64Octets      =           387871
11 rxTxHCPkts65to127Octets =        13704213656
12 rxTxHCPkts128to255Octets =        16915931224
13 rxTxHCPkts256to511Octets =        1068961475
14 rxTxHCPkts512to1023Octets =        1945427146
15 rxTxHCPkts1024to1518Octets =        11340361825
16 txHCTrunkFrames         =        29657506751
17 rxHCTrunkFrames         =        32513986812
18 rxHCDropEvents          =              0

32 bit counters
0  rxCRCAlignErrors        =              0
1  rxUndersizedPkts        =              0
2  rxOversizedPkts         =              0
3  rxFragmentPkts          =              0
4  rxJabbers                =              0
5  txCollisions             =              0
6  ifInErrors               =              0
7  ifOutErrors              =              0
8  ifInDiscards             =              0
9  ifInUnknownProtos       =              0
10 ifOutDiscards            =              98
11 txDelayExceededDiscards  =              0
12 txCRC                    =              0
13 linkChange               =              1
14 wrongEncapFrames         =              0
0  dot3StatsAlignmentErrors =              0
1  dot3StatsFCSErrors       =              0
2  dot3StatsSingleColFrames =              0
3  dot3StatsMultiColFrames  =              0
4  dot3StatsSQETestErrors   =              0
5  dot3StatsDeferredTransmissions =              0
6  dot3StatsLateCollisions  =              0
7  dot3StatsExcessiveCollisions =              0
8  dot3StatsInternalMacTransmitErrors =              0
9  dot3StatsCarrierSenseErrors =              0
10 dot3StatsFrameTooLongs   =              0
11 dot3StatsInternalMacReceiveErrors =              0
12 dot3StatsSymbolErrors    =              0
0  txPause                   =              0
1  rxPause                    =              0
0 rxTotalDrops = 253428855 1 rxFIFOFull = 0 2 rxBadCode = 0 Last-Time-Cleared -----
----- Sat Oct 27 2007, 08:24:35 6509> (enable)
```

Quando a porta bloqueia as VLANs em um lado, mas o lado remoto faz encaminhamentos para

essa VLAN, a interface incrementa os contadores rxTotalDrops.

Compare as VLANs permitidas no entroncamento em ambos os lados do link. Verifique também o estado de spanning tree para as VLANs permitidas em ambos os lados. Os BPDUs ainda são enviados para VLANs ativamente configuradas, para que o switch A envie BPDUs para todas as portas configuradas e de encaminhamento, mas o switch B as descarta porque não possui essas VLANs configuradas. Em outras palavras, o switch B obtém pacotes para as VLANs para as quais não está configurado e simplesmente as descarta. Esses não são realmente erros, mas uma simples questão de configuração incorreta.

os **ifOutDiscards** ocorrem geralmente quando o buffer transmitir (Tx) obtém completamente (talvez devido à sobreassinatura) e começa então deixar cair os pacotes.

[Pesquise defeitos quedas de emissor](#)

Tipicamente, as quedas de emissor ocorrerão se QoS é configurado e não está fornecendo a largura de banda suficiente a determinada classe de pacotes. Igualmente ocorre quando nós estamos batendo a sobreassinatura.

Por exemplo, aqui você vê uma quantidade elevada de quedas de emissor no gigabitethernet 8/9 da relação em um Catalyst 6500 Series Switch:

```
Switch#show interface GigabitEthernet8/9 GigabitEthernet8/9 is up, line protocol is up
(connection) Hardware is C6k 1000Mb 802.3, address is 0013.8051.5950 (bia 0013.8051.5950)
Description: Connection To Bedok_Core_R1 Ge0/1 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 18/255, rxload 23/255 Encapsulation ARPA, loopback not set Keepalive
set (10 sec) Full-duplex, 1000Mb/s, media type is SX input flow-control is off, output flow-
control is off Clock mode is auto ARP type: ARPA, ARP Timeout 04:00:00 Last input 00:00:28,
output 00:00:10, output hang never Last clearing of "show interface" counters never Input queue:
0/2000/3/0 (size/max/drops/flushes); Total output drops: 95523364 Queueing strategy: fifo Output
queue: 0/40 (size/max) 5 minute input rate 94024000 bits/sec, 25386 packets/sec 5 minute output
rate 71532000 bits/sec, 24672 packets/sec 781388046974 packets input, 406568909591669 bytes, 0
no buffer Received 274483017 broadcasts (257355557 multicasts) 0 runts, 0 giants, 0 throttles 3
input errors, 2 CRC, 0 frame, 0 overrun, 0 ignored 0 watchdog, 0 multicast, 0 pause input 0
input packets with dribble condition detected 749074165531 packets output, 324748855514195
bytes, 0 underruns 0 output errors, 0 collisions, 3 interface resets 0 babbles, 0 late
collision, 0 deferred 0 lost carrier, 0 no carrier, 0 PAUSE output 0 output buffer failures, 0
output buffers swapped out
```

A fim analisar o problema, recolha a saída destes comandos:

- [mostre o det da utilização de construção](#)
- [mostre erros de tela](#)
- [mostre a capacidade do hardware da plataforma](#)
- [show catalyst6000 traffic-meter](#)
- [mostre a gota do Engine de reescrita da capacidade do hardware da plataforma](#)

[Última entrada nunca da saída do comando show interface](#)

Este exemplo do comando show interface mostra a **última entrada nunca na relação** TenGigabitEthernet1/15.

```
Switch#show interface TenGigabitEthernet1/15 TenGigabitEthernet1/15 is up, line protocol is up
(connection) Hardware is C6k 10000Mb 802.3, address is 0025.84f0.ab16 (bia 0025.84f0.ab16)
Description: lsnbuprod1 solaris MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec, reliability
255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive set (10 sec)
```

Full-duplex, 10Gb/s input flow-control is off, output flow-control is off ARP type: ARPA, ARP Timeout 04:00:00 **Last input never**, output 00:00:17, output hang never Last clearing of "show interface" counters 2d22h Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing strategy: fifo Output queue: 0/40 (size/max) 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 46000 bits/sec, 32 packets/sec 52499121 packets input, 3402971275 bytes, 0 no buffer Received 919 broadcasts (0 multicasts) 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored 0 watchdog, 0 multicast, 0 pause input 0 input packets with dribble condition detected 118762062 packets output, 172364893339 bytes, 0 underruns 0 output errors, 0 collisions, 3 interface resets 0 babbles, 0 late collision, 0 deferred 0 lost carrier, 0 no carrier, 0 PAUSE output 0 output buffer failures, 0 output buffers swapped out

Isto mostra o número de horas, de minutos, e de segundos desde que o último pacote foi recebido com sucesso por uma relação e processado localmente no roteador. Isto é útil de saber quando uma relação inoperante falhou. Este contador é atualizado somente quando os pacotes são switches de processo, não quando os pacotes estão comutados rapidamente.

A **última entrada nunca** significa que não havia nenhuma transferência de pacote de informação bem sucedida da relação ao outro ponto final ou terminal. Geralmente isto significa que não havia nenhuma transferência de pacote de informação relativa a essa entidade.

[Informações Relacionadas](#)

- [Troubleshooting de Compatibilidade entre Catalyst Switches e NIC](#)
- [Utilização de Portfast e outros comandos para reparar retardos de conectividade da inicialização de estação de trabalho](#)
- [Configuração e Troubleshooting da Negociação Automática de Ethernet 10/100/1000 Mb Half/Full-Duplex](#)
- [Recuperação de um estado de porta errDisable em plataformas CatOS](#)
- [Atualizando imagens de Software e trabalhando com arquivos de configuração nos Switches Catalyst](#)
- [Recuperando Switches Catalyst executando CAtOS a partir de falhas de inicialização](#)
- [Recuperação a partir da imagem de Software corrompido ou ausente em Cisco Catalyst 2900XL e 3500XL Series Switches](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)