

# Mensagens de erro comuns do CatOS nos switches Catalyst 4500/4000 Series

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Mensagens de erro nos Switches das séries Catalyst 4500/4000](#)

[%C4K\\_HWPORTMAN-4-BLOCKEDTXQUEUE:Fila de transmissão bloqueada HwTxQId\[dec\]on \[char\], count=\[dec\]](#)

[%CDP-4-NVLANMISMATCH: Incompatibilidade de vlan nativa detectada em porta \[DEC\]/\[DEC\]](#)

[DTP-1-ILGLCFG: Configuração ilegal \(on, isl--on,dot1q\) na porta \[mod/port\]](#)

[%IP-3-UDP SOCKOVFL:excesso de soquete UDP](#)

[%IP-3-UDP BADCKSUM:Soma de verificação de UDP inválida](#)

[%KERNEL-5-UNALIGNACCESS:Correção de alinhamento realizada](#)

[%MCAST-4-RX\\_JNRANGE:IGMP: Relatório Rcvd no intervalo](#)

[MGMT-5-LOGIN\\_FAIL:Usuário falhou ao fazer login a partir do Console](#)

[%PAGP-5-PORTFROMSTP / %PAGP-5-PORTTOSTP](#)

[%SPANTREE-3-PORTDEL\\_FAILNOTFOUND](#)

[%SYS-3-P2\\_ERROR: 1/Módulo desconhecido](#)

[%SYS-3-P2\\_ERROR: 1/Tiver ficado sem vbufs \(buffers internos\)](#)

[%SYS-3-P2\\_ERROR: Host xx:xx:xx:xx:xx:xx is flapping between ports](#)

[%SYS-4-P2\\_AVISO: 1/Fila bloqueada \(tx\) na porta \[char\]](#)

[%SYS-4-P2\\_AVISO: 1/endereço MAC de Ethernet de filtragem com valor zero](#)

[%SYS-4-P2\\_AVISO: 1/crc inválido, pacote descartado, contagem = xx](#)

[%SYS-4-P2\\_AVISO: 1/Tráfego inválido do endereço de origem multicast](#)

[%SYS-4-P2\\_AVISO: 1/Astro\(mod/port\)](#)

[%SYS-4-P2\\_AVISO: 1/Tag 0](#)

[convert\\_post\\_SAC CiscoMIB:Nvram block \[#\] unconvertible](#)

[Global checksum failed error](#)

[Informações Relacionadas](#)

## [Introduction](#)

Este documento fornece uma breve explicação das mensagens do log do sistema (Syslog) e de erro comuns emitidas pelos Cisco Catalyst 4500/4000 Series Switches com o Catalyst OS (CatOS) Software.

Se você não encontrar os detalhes de alguma mensagem de erro específica neste documento, use a ferramenta [Error Message Decoder](#) (somente clientes [registrados](#)). Essa ferramenta fornece o significado das mensagens de erro geradas pelo Cisco IOS® Software e pelo CatOS Software.

**Nota:**O formato exato das mensagens do Syslog e de erro descritas neste documento pode variar. A variação depende do release do software executado no Supervisor Engine do switch.

**Nota:**Esta é a configuração mínima de log recomendada nos Catalyst 4500/4000 Series Switches:

- Defina a data e a hora do switch ou configure o switch para utilizar o Network Time Protocol (NTP) a fim de obter a data e a hora de um servidor NTP.**Nota:**Execute o comando **set time para definir a data e a hora no switch**.
- Certifique-se de que o registro e as marcas de data e hora do registro estejam habilitadas, que é o padrão.
- Configure o switch para registrar em um servidor syslog, se possível.

As mensagens de erro neste documento podem ocorrer nos Catalyst 4500/4000 Series Switches e em seus derivados, como os Catalyst 2948G, 2980G e 4912G Switches.

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

Este documento não é restrito a versões de software ou hardware específicas.

### Conventions

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

## Mensagens de erro nos Switches das séries Catalyst 4500/4000

**%C4K\_HWPORTMAN-4-BLOCKEDTXQUEUE:Fila de transmissão bloqueada  
HwTxQId[dec]on [char], count=[dec]**

### **Problema**

O switch gera erros %C4K\_HWPORTMAN-4-BLOCKEDTXQUEUE:Blocked transmit queue HwTxQId[dec]on[char], count=[dec].

### **Descrição**

Essa mensagem de taxa limitada indica que uma fila de transmissão em uma porta está

bloqueada por razões diferentes de "em pausa". Em outras palavras, o tráfego nessa porta está sendo limitado e bloqueado. Você verá as mensagens de bloqueio da fila de transmissão se o Supervisor Engine não for capaz de enviar pacotes às placas de linha devido à recepção de um bit de ocupado da placa de linha. Problemas de hardware ou uma incompatibilidade de velocidade/duplex podem causar esse problema. A solução é configurar os dois lados do link para fazer a negociação automática de velocidade e de duplex. Execute o comando **shut/no shut** para recuperar a porta. Caso o problema persista, mova o dispositivo conectado para uma outra porta e veja se o problema continua a ocorrer. Como uma medida final para desbloquear a fila de transmissão (Tx), execute o comando **hw-module reset** para reinicializar o switch ou redefinir as placas de linha.

## [%CDP-4-NVLANMISMATCH: Incompatibilidade de vlan nativa detectada em porta \[DEC\]/\[DEC\]](#)

### Problema

O switch gera mensagens %CDP-4-NVLANMISMATCH freqüentes no Syslog.

### Descrição

Este exemplo mostra a saída do console exibida quando esta mensagem de erro ocorre no switch:

```
%CDP-4-NVLANMISMATCH:Native vlan mismatch detected on port 4/1
```

O switch gera essa mensagem sempre que a porta do switch está fisicamente conectada a outro switch ou roteador. Essa mensagem é gerada no switch porque a VLAN nativa configurada na porta é diferente daquela definida no switch ou na porta do roteador conectado.

Uma porta de tronco configurada com marcas IEEE 802.1Q pode receber tráfego marcado ou não. Por padrão, o switch encaminha o tráfego não marcado com a VLAN nativa configurada para a porta. Se um pacote possuir o mesmo ID de VLAN da porta de saída, ele será transmitido sem marcas. Se os IDs das VLANs não forem os mesmas, o switch transmitirá o pacote com uma marca.

Certifique-se de que o VLAN nativo para um tronco 802.1q é o mesmo nas duas extremidades no enlace do tronco. Se uma VLAN nativa em uma extremidade do tronco for diferente da VLAN nativa na outra extremidade, o tráfego de VLANs nativas em ambos os lados não poderá ser transmitido corretamente no tronco. Essa falha em transmitir corretamente pode implicar em alguns problemas de conectividade em sua rede.

Para verificar a VLAN nativa configurada no switch, execute o comando **show trunk mod/port**. Neste comando, o *mod/port* é a porta de tronco. Aqui está um exemplo de saída do comando:

```
Console> (enable) show trunk 5/24
```

Port	Mode	Encapsulation	Status	Native vlan
5/24	desirable	dot1q	not-trunking	1

```
Port Vlans allowed on trunk
```

```

5/24      1-1005

Port      Vlans allowed and active in management domain
-----
5/24      1

Port      Vlans in spanning tree forwarding state and not pruned
-----
5/24

```

Console> (enable)

Para alterar a VLAN nativa configurada na porta de tronco, execute o comando **set vlan *vlan-id* *mod/port***. Neste comando, o *mod/port* é a porta de tronco.

## [DTP-1-ILGLCFG: Configuração ilegal \(on, isl--on,dot1q\) na porta \[mod/port\]](#)

### Problema

O switch gera erros DTP-1-ILGLCFG: `Illegal config (on, isl--on,dot1q) on Port [mod/port]`.

### Descrição

Essa mensagem pode ocorrer se ambos os lados do truncamento estiverem definidos como ligados, mas os tipos de encapsulamento (isl, dot1q) não corresponderem. Se os modos do tronco estiverem definidos como desirable, o tronco não será estabelecido devido a essa configuração errada. Para fazer o troubleshooting, verifique a saída do comando **show trunk** em ambas as extremidades. Certifique-se de que os tipos de encapsulamento sejam idênticos.

## [%IP-3-UDP\\_SOCKOVFL:excesso de soquete UDP](#)

### Problema

O switch gera mensagens do Syslog `%IP-3-UDP_SOCKOVFL:UDP socket overflow` periódicas.

### Descrição

Este exemplo mostra a saída do console que você vê quando este erro ocorre:

**Observação:** o número do soquete do User Datagram Protocol (UDP) exibido pode variar ou ser consistentemente o mesmo.

```

%IP-3-UDP_SOCKOVFL:UDP socket 2353 overflow
%IP-3-UDP_SOCKOVFL:UDP socket 2353 overflow
%IP-3-UDP_SOCKOVFL:UDP socket 2353 overflow
%IP-3-UDP_SOCKOVFL:UDP socket 2353 overflow

```

O switch gera essa mensagem do Syslog quando o buffer alocado para os pacotes recebidos no soquete especificado (a porta de destino UDP) está cheio. O buffer enche porque a taxa do tráfego destinado ao soquete é alta demais. Por exemplo, essa condição pode ocorrer quando uma estação de gerenciamento de rede envia um grande número de consultas SNMP (Simple Network Management Protocol). Quando o estouro de UDP ocorrer, tente reduzir o número de consultas SNMP. Execute uma destas ações:

- Aumente o intervalo de consulta periódica da estação de gerenciamento de rede.
- Reduza o número de objetos de MIB consultados.

No exemplo desta seção, o switch recebeu um número excessivo de pacotes destinados ao endereço IP do switch (ou o endereço de broadcast) com o soquete UDP de destino 2353. Como o buffer de entrada para esse soquete no switch está cheio, o switch gera uma mensagem syslog. Execute o comando **show netstat udp** para ver o número de vezes que o switch atingiu a condição de estouro.

Essas mensagens do Syslog indicam que uma ou mais estações estão enviando uma grande quantidade de tráfego de UDP nas portas UDP de destino especificadas para o switch. Se o switch gerar um número excessivo dessas mensagens, use um analisador de rede para identificar a origem do tráfego e reduzir sua taxa. Consulte [Exemplo de Configuração do Catalyst Switched Port Analyzer \(SPAN\)](#) para obter mais informações.

**Nota:** Não se preocupe com o contador no **such port**. Esse contador mostra o número de pacotes de UDP recebidos pelo switch com destino a portas inexistentes.

## [%IP-3-UDP\\_BADCKSUM:Soma de verificação de UDP inválida](#)

### Problema

O switch gera mensagens do Syslog **%IP-3-UDP\_SOCKETOVFL:UDP socket overflow** periódicas.

### Descrição

Este exemplo mostra a saída do console que você vê quando este erro ocorre:

**Observação:** o número do soquete UDP exibido pode variar ou ser consistentemente o mesmo.

```
%IP-3-UDP_BADCKSUM:UDP bad checksum
```

O switch gera essa mensagem do Syslog ao detectar uma soma de verificação inválida em datagrama de UDP, como pacotes SNMP. O cabeçalho do datagrama de UDP transporta uma soma de verificação que o dispositivo de rede receptor examina para verificar se o datagrama foi corrompido durante o trânsito. Se a soma de verificação recebida não corresponder ao valor existente no cabeçalho, o datagrama será descartado e uma mensagem de erro será registrada. Execute o comando **show netstat udp** para ver o número de vezes que o switch detectou um datagrama com soma de verificação incorreta.

```
6500-b (enable) show netstat udp
```

```
udp:  
0 incomplete headers  
0 bad data length fields  
0 bad checksums  
0 socket overflows  
110483 no such ports
```

Essa é uma mensagem meramente informativa. Um dispositivo de rede que envia pacotes corrompidos para o switch é o causador dessa mensagem. Use um analisador de rede para identificar a origem do tráfego. Consulte [Exemplo de Configuração do Catalyst Switched Port Analyzer \(SPAN\)](#) para obter mais informações.

**Nota:** Não se preocupe com o contador no `such port`. Esse contador mostra o número de pacotes de UDP recebidos pelo switch com destino a portas inexistentes.

## [%KERNEL-5-UNALIGNACCESS: Correção de alinhamento realizada](#)

### Problema

O switch gera mensagens do Syslog `%KERNEL-5-UNALIGNACCESS: Alignment correction made` periódicas.

### Descrição

Este exemplo mostra a saída do Syslog exibida quando este erro ocorre:

```
%KERNEL-5-UNALIGNACCESS: Alignment correction made at 0x80056B3C reading 0x81B82F36
```

Essas mensagens do Syslog indicam que a CPU do switch detectou e corrigiu um erro de alinhamento quando o switch tentou acessar dados na DRAM. Essas mensagens são apenas informativas. Elas não indicam um problema no switch e não afetam o desempenho do sistema.

Em alguns casos, um número excessivo dessas mensagens pode ser exibido. Por exemplo, essas mensagens podem inundar o arquivo de log do seu servidor de Syslog ou o console do switch. Se você receber mensagens em excesso, considere atualizar o software do switch para o release de manutenção mais recente da sua linha de release de software. Outra opção é executar o comando `set logging level kernel 4 default` para modificar o nível de log do recurso Kernel para 4 ou inferior.

Se você atualizar para o release de manutenção mais recente e continuar a receber essas mensagens do Syslog, [crie uma solicitação de serviço](#) (somente clientes [registrados](#)) no [Suporte Técnico da Cisco](#).

## [%MCAST-4-RX\\_JNRANGE:IGMP: Relatório Rcvd no intervalo](#)

### Problema

Um switch com snooping de Internet Group Management Protocol (IGMP) ativo exibe a mensagem de erro `%MCAST-4-RX_JNRANGE:IGMP: Rcvd Report in the range 01-00-5e-00-00-xx`.

### Descrição

Este exemplo mostra a saída do Syslog exibida quando este erro ocorre:

```
%MCAST-4-RX_JNRANGE:IGMP: Rcvd Report in the range 01-00-5e-00-00-xx
```

A mensagem do Syslog `Rcvd Report in the range` é meramente informativa. O switch gera essa mensagem ao receber pacotes de relatório de IGMP com um endereço MAC de multicast iniciado por `01-00-5e-00-00-xx`. Essa faixa de endereços da Camada 2 (L2) é equivalente à faixa de endereços multicast da Camada 3 (L3) entre `224.0.0.0` e `224.0.0.255`. Esses endereços são reservados para o uso de protocolos de roteamento e outros protocolos de descoberta de

topologia ou manutenção de baixo nível. Exemplos desses protocolos incluem a descoberta de gateways e os relatórios de associação a grupos.

Use uma ferramenta de captura de pacotes, como um sniffer, e filtre as mensagens de IGMP para fazer o troubleshooting deste problema. Além disso, você pode usar a função Catalyst SPAN para copiar pacotes de uma porta que você suspeita estar recebendo essas mensagens de um dispositivo de rede. Para suprimir essas mensagens, execute o comando **set logging level mcast 2 default**. Esse comando altera o nível de registro de mensagens multicast para 2.

Use as portas mostradas pelo comando **show multicast router** e qualquer uplink para o núcleo da rede como as portas de origem do SPAN. Se essas portas forem de tronco, configure a porta de destino do SPAN também como uma porta de tronco. Execute o comando **show trunk** para verificar se as portas são portas de tronco.

## [MGMT-5-LOGIN\\_FAIL:Usuário falhou ao fazer login a partir do Console](#)

### Problema

O switch gera erros MGMT-5-LOGIN\_FAIL:User failed to log in from Console.

### Descrição

Essa mensagem pode indicar um problema com o servidor de terminal conectado à porta de console do switch. Quando o console do switch estiver conectado a uma linha assíncrona de um servidor de terminal e uma reinicialização por software for feita no switch, um fluxo de lixo (texto aleatório) passará pela tela por vários minutos. Se o TACACS estiver habilitado no switch, os vários minutos poderão se transformar em muitos dias enquanto o TACACS coloca o lixo no buffer e o processa um pedaço de cada vez. A solução é executar o comando **no exec** na linha assíncrona à qual o switch está conectado.

**Nota:** Mesmo após a execução do comando **no exec**, as mensagens continuarão até o buffer ser limpo.

**Nota:** Se você receber a mensagem de erro **%MGMT-5-LOGIN\_FAIL:User failed to log via Telnet - max attempt reached**, tente limitar o número de usuários com permissão para fazer Telnet no switch.

## [%PAGP-5-PORTFROMSTP / %PAGP-5-PORTTOSTP](#)

### Problema

O switch gera mensagens do Syslog **%PAGP-5-PORTFROMSTP** and **%PAGP-5-PORTTOSTP** com frequência.

### Descrição

Este exemplo mostra a saída do console quando o switch gera essas mensagens do Syslog:

```
%PAGP-5-PORTFROMSTP:Port 3/3 left bridge port 3/3
```

```
%PAGP-5-PORTTOSTP:Port 3/3 joined bridge port 3/3
```

O recurso de log do Port Aggregation Protocol (PAgP) relata os eventos que envolvem o PAgP. Use o PAgP para negociar links EtherChannel entre os switches. O switch gera a mensagem do Syslog %PAGP-5-PORTFROMSTP sempre que um link é perdido em uma porta do switch. O switch gera a mensagem do Syslog %PAGP-5-PORTTOSTP sempre que um link é detectado em uma porta do switch. Essas mensagens do Syslog são mensagens informativas normais que indicam a adição ou remoção de uma porta da spanning tree.

**Nota:** Não é necessário habilitar os canais para que essas mensagens sejam exibidas.

No exemplo desta seção, o switch primeiro perdeu o link na porta 3/3, o que removeu a porta da spanning tree. Em seguida, o switch detectou novamente o link na porta, o que a adicionou de volta à spanning tree.

Se você vir essas mensagens freqüentemente para uma porta específica, o link está oscilando, o que significa que ele é perdido e recuperado constantemente. Investigue a causa. As causas típicas da não sincronização de enlace em uma porta de Switch incluem:

- Incompatibilidade de velocidade/duplex
- Cabo defeituoso
- placa de interface de rede (NIC) defeituosa ou outro problema de estação final
- Porta do Switch defeituosa
- Outros erros de configurações

Para suprimir essas mensagens do Syslog, execute o comando **set logging level pagp 4 default** para modificar o nível de log do recurso PAgP para 4 ou menos. O nível de log padrão do PAgP é 5.

## [%SPANTREE-3-PORTDEL\\_FAILNOTFOUND](#)

### Problema

O switch gera mensagens do Syslog %SPANTREE-3-PORTDEL\_FAILNOTFOUND periódicas.

### Descrição

Este exemplo mostra a saída do Syslog exibida quando este erro ocorre:

```
%SPANTREE-3-PORTDEL_FAILNOTFOUND:9/5 in vlan 10 not found (PAgP_Group_Rx)
```

Essas mensagens de syslog indicam que o PAgP tentou remover uma porta da extensão de árvore do VLAN especificado, mas a porta não estava na estrutura de dados de extensão de árvore daquele VLAN. Em geral, outro processo, como o Dynamic Trunking Protocol (DTP), já removeu a porta da spanning tree.

Essas mensagens normalmente acompanham as mensagens %PAGP-5-PORTFROMSTP. As mensagens destinam-se à depuração. Elas não indicam um problema no switch e não afetam o desempenho do switching. Além disso, essas mensagens não serão registradas a menos que você tenha alterado a configuração padrão de log do recurso SPANTREE. O nível de log padrão de SPANTREE é 2.

Em alguns casos, um número excessivo dessas mensagens pode ser exibido. Por exemplo,



essas mensagens podem inundar o console do seu switch. Se você receber mensagens em excesso, considere atualizar o software do switch para o release de manutenção mais recente da sua linha de release de software. Versões mais recentes do software suprimem essas mensagens na maioria dos casos.

## [%SYS-3-P2\\_ERROR: 1/Módulo desconhecido](#)

### Problema

Os erros `%SYS-3-P2_ERROR: 1/Unknown module` é exibida quando você instala um novo switching module em um Catalyst 4500/4000 Series Switch.

### Descrição

Este exemplo mostra a saída do console que você vê quando este erro ocorre:

```
%SYS-3-P2_ERROR: 1/Unknown module (fru minor type 304) in slot 3
```

Os erros `%SYS-3-P2_ERROR: 1/Unknown module` ocorre quando a versão da imagem do software em execução no Supervisor Engine não oferece suporte ao componente de hardware inserido.

No exemplo, um switching module de servidor de 18 portas 1000BASE-X (WS-X4418) foi inserido em um Catalyst 4500/4000 Switch com o CatOS Software Release 4.4(1). O módulo WS-X4418 necessita no mínimo do software release 4.5(1).

A solução é atualizar a versão do software Supervisor Engine para uma versão que suporte o hardware. Consulte [Release Notes dos Catalyst 4500 Series Switches](#) para obter uma lista das versões mínimas de software para cada módulo.

## [%SYS-3-P2\\_ERROR: 1/Tiver ficado sem vbufs \(buffers internos\)](#)

### Problema

O switch gera mensagens `%SYS-3-P2_ERROR: 1/Have run out of vbufs` quando vários hosts são ligados simultaneamente ou quase ao mesmo tempo.

### Descrição

Este exemplo mostra a saída do console exibida quando este erro ocorre:

```
%SYS-3-P2_ERROR: 1/Have run out of vbufs(internal buffers)
```

Os erros `%SYS-3-P2_ERROR: 1/Have run out of vbufs(internal buffers)` podem ocorrer quando vários hosts são ligados simultaneamente. Depois que os hosts são ligados, os erros não aparecem mais.

Esses erros não causam nenhuma interrupção na capacidade de o Catalyst de comutar o tráfego. As mensagens são de natureza meramente informativa.

## [%SYS-3-P2\\_ERROR: Host xx:xx:xx:xx:xx:xx is flapping between ports](#)

## Problema

O switch gera mensagens %SYS-3-P2\_ERROR: Host xx:xx:xx:xx:xx:xx is flapping between ports..., onde xx:xx:xx:xx:xx:xx é um endereço MAC.

## Descrição

Este exemplo mostra a saída do console que você vê quando este erro ocorre:

```
%SYS-4-P2_WARN: 1/Host 00:50:0f:20:08:00 is flapping between port 1/2 and port 4/39
```

Use os passos e as diretrizes desta seção para compreender e fazer o troubleshooting da causa dessa mensagem de erro.

A mensagem indica que o Catalyst 4500/4000 Switch reconheceu um endereço MAC já existente na tabela de memória de conteúdo endereçável (CAM) em uma porta diferente da original. Esse comportamento ocorre repetidamente após pequenos intervalos de tempo, o que significa que o endereço está oscilando entre portas.

Se a mensagem for exibida para vários endereços MAC, o comportamento não é normal. Esse comportamento indica um possível problema de rede, pois os endereços MAC se movem rapidamente de uma porta para outra antes do tempo de validade padrão. O problema pode ser o tráfego em loop na rede. Os sintomas típicos incluem:

- Alto uso de CPU
- Tráfego lento em toda a rede
- Alto uso do backplane do switch

Para obter mais informações sobre como identificar e fazer o troubleshooting de problemas relativos à spanning tree, consulte [Problemas do Spanning Tree Protocol e Considerações de Design Relacionadas](#).

Se a mensagem de erro for exibida para um ou dois endereços MAC, localize esses endereços para determinar a causa. Execute o comando **show cam mac\_addr para identificar de onde esses endereços MAC foram aprendidos**. Nesse comando, *mac\_addr* é o endereço MAC que a mensagem de erro informou que está oscilando.

Após determinar entre quais portas esse endereço MAC está oscilando, rastreie o endereço MAC. Conecte-se aos dispositivos intermediários entre seu Catalyst 4500/4000 e o dispositivo que apresenta o problema com o endereço MAC. Faça isso até que você seja capaz de identificar a origem e a forma com a qual esse dispositivo se conecta à rede.

**Nota: Como o endereço MAC oscila entre duas portas, rastreie por ambos os caminhos.**

Este exemplo mostra como rastrear os dois caminhos a partir dos quais esse endereço MAC foi aprendido:

**Nota: Considere que você recebeu essa mensagem e começou a investigá-la.**

```
%SYS-4-P2_WARN: 1/Host 00:50:0f:20:08:00 is flapping between port 1/2 and port 4/39
```

Para rastrear como esse endereço MAC foi aprendido por ambas as portas, conclua estas etapas:

1. Considere a porta 1/2 primeiro e, em seguida, execute o comando **show cam dynamic 1/2**. Se você vir o endereço MAC 00:50:0f:20:08:00 na lista de endereços MAC que foram aprendidos por essa porta, determine se ele é relativo a um único host conectado ou se há diversos hosts registrados nessa porta.
2. Com base em há um único ou vários hosts, investigue o dispositivo: Se houver um único host (00:50:0f:20:08:00) conectado, verifique a outra porta registrada e veja se o host está duplamente conectado ao switch. Neste exemplo, a outra porta é a porta 4/39. Se o host possuir conexões a outros dispositivos que podem acabar direcionando-o de volta a este switch, tente rastrear os dispositivos intermediários. Em dispositivos Cisco, execute o comando **show cdp neighbors mod/port detail**. A saída fornece informações sobre dispositivos intermediários. Aqui está o exemplo de saída:

```
Cat4K> (enable) show cdp neighbors 1/2 detail
```

```
Port (Our Port): 1/2
Device-ID: brigitte
Device Addresses:
IP Address: 172.16.1.1
Novell address: aa.0
Holdtime: 171 sec
Capabilities: ROUTER
Version:
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(7)T, RELEASE SOFTWARE (fc2)
```

```
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Mon 06-DEC-99 17:10 by phanguye
Platform: cisco 2500
Port-ID (Port on Neighbors's Device): Ethernet0
VTP Management Domain: unknown
Native VLAN: unknown
Duplex: half
System Name: unknown
System Object ID: unknown
Management Addresses: unknown
Physical Location: unknown
```

```
Cat4K> (enable)
```

3. Estabeleça uma sessão de Telnet com o dispositivo e siga o caminho do endereço MAC. Neste exemplo, o endereço IP é 172.16.1.1. Repita o procedimento para todos os endereços MAC relatados como oscilantes pela mensagem de erro.
4. Crie um diagrama simples do dispositivo de origem com esse endereço MAC e das conexões físicas (as portas do Catalyst 4500/4000) de e para onde esse endereço MAC está oscilando. O diagrama permite que você determine se essa é uma porta e um caminho válido dentro do layout da sua rede. Se você verificar que ambas as portas onde o endereço MAC oscila fornecem um caminho em direção a esse nó da rede, é possível que haja um problema de falha de spanning tree. Consulte [Problemas do Spanning Tree Protocol e Considerações de Design Relacionadas](#) para isolar e resolver esse loop. Em redes grandes onde diversos hosts de vários fornecedores estão interconectados, algumas dificuldades surgem quando você tenta rastrear o host somente com o uso do endereço MAC. Use o utilitário de pesquisa para o [IEEE OUI e Atribuições Company id](#) para rastrear esses endereços MAC. Essa lista é o front-end do banco de dados no qual o IEEE registrou todos os endereços MAC atribuídos a todos os fornecedores. Insira os primeiros três octetos do endereço MAC no campo **Search for:** dessa página para localizar o fornecedor associado a esse dispositivo. Os primeiros três octetos no exemplo são 00:50:0f.

Estes são outros problemas que podem fazer com que esta mensagem apareça:

- **Problema de redundância de NIC de servidor** — Quando há um servidor com uma NIC duplamente conectada com comportamento que não segue os padrões. O servidor usa o mesmo endereço MAC para ambas as portas que se conectam ao mesmo switch.
- **Oscilação de Hot Standby Router Protocol (HSRP)** — O HSRP oscilante pode causar o surgimento dessas mensagens no console do Supervisor Engine. Se você constatar que a implementação do HSRP de sua rede é instável, consulte [Compreensão e Troubleshooting de Problemas de HSRP em Redes de Catalyst Switches](#) para resolver o problema.
- **Configuração incorreta do EtherChannel** — Uma conexão incorreta do EtherChannel também pode causar esses sintomas. Se as portas relatadas como oscilantes pela mensagem forem membros do mesmo grupo de canal, verifique sua configuração de EtherChannel e consulte [Entendendo o Balanceamento de Carga do EtherChannel e a Redundância nos Catalyst Switches](#) para fazer o troubleshooting da configuração.
- **O host reflete pacotes de volta para a rede** — A reflexão de pacotes de volta para a rede por um host também pode causar oscilação. Normalmente, a causa principal dessa reflexão de pacotes é uma NIC defeituosa ou qualquer outra falha na interface física do host conectado à porta. Se a reflexão de pacotes por esse host for sua causa principal, obtenha um rastreamento de sniffer e examine o tráfego de e para as portas para as quais a mensagem foi exibida. Se um host refletir pacotes, em geral haverá pacotes duplicados no rastreamento. Os pacotes duplicados são um possível sintoma dessa oscilação de endereço MAC. Consulte [Configurando o SPAN e o RSPAN](#) para obter detalhes sobre como configurar uma porta para uso com um sniffer.
- **Defeito de software ou hardware** — Se você tiver tentado fazer o troubleshooting da mensagem oscilante com as instruções desta seção, mas ainda constatar o problema, procure ajuda adicional do [Suporte Técnico da Cisco](#). Certifique-se de mencionar e fornecer a documentação das informações coletadas durante a execução das etapas. Essas informações tornarão o troubleshooting adicional mais rápido e eficiente.

## [%SYS-4-P2\\_AVISO: 1/Fila bloqueada \(tx\) na porta \[char\]](#)

### Problema

O switch gera mensagens Blocked queue (tx) on port [char].

### Descrição

Este exemplo mostra a saída do Syslog exibida quando este erro ocorre:

```
%SYS-4-P2_WARN: 1/Blocked queue (tx) on port 3/3
%SYS-4-P2_WARN: 1/Blocked queue on gigaport 3, ( 8671 : 0)
```

Esses erros indicam um problema de hardware ou um destes problemas:

- Incompatibilidade duplex
- Cabo defeituoso
- Cabeamento tipo 1
- Portas defeituosas

- Problema de hardware de um dispositivo externo conectado

A causa mais comum desses erros é um problema da camada física. O problema causa uma quantidade considerável de tráfego para backup nas gigaports K1 internas. Os Application-Specific Integrated Circuits (ASICs) K1 são os chips principais que controlam o switch. Em geral, o contador da fila de Tx bloqueada é incrementado devido a um problema de configuração ou a um cabo danificado.

Em um ambiente normal, a fila de Tx somente pode ser bloqueada por aproximadamente 20 segundos. Um bloqueio mais longo indica um problema significativo. Como resultado, o contador da fila de Tx bloqueada será incrementado se a fila de Tx não for drenada pela gigaport em 35 segundos.

Se necessário, entre em contato com o [Suporte Técnico da Cisco](#) para determinar se o módulo necessita ser substituído. No entanto, reinicialize primeiro o módulo e veja se a mensagem de erro ainda persiste.

Aqui estão as etapas para mapear a fila bloqueada do Catalyst 4000/2948G/2980G em gigaport <gigaport\_number> para as portas do switch do painel frontal, que precisam ser recolocadas.

### Exemplo de mensagens de erro:

```
2000 Aug 25 12:22:48 cet +02:00 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 29, (331 : 0 )
2000 Aug 25 12:23:41 cet +02:00 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 29, (332 : 0 )
2000 Aug 25 12:25:42 cet +02:00 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 29, (333 : 0 )
2000 Aug 25 12:46:42 cet +02:00 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 29, (334 : 0 )
2000 Aug 25 12:48:41 cet +02:00 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 29, (335 : 0 )
2000 Aug 25 12:57:42 cet +02:00 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 29, (336 : 0 )
```

Essa mensagem de erro indica que há um erro de configuração que resulta mais provavelmente de um problema de camada física ou de uma incompatibilidade duplex relacionada ao gigaport 29. Para descobrir quais portas estão relacionadas ao gigaport 29, consulte essas tabelas. As tabelas variam e dependem do Supervisor Engine.

### Mapeamento de porta Gigabit Kirky WS-X4013

K1-A (gigaports 0-11)

Gigaport 0	Uplink 0 (Porta 1/1) ou Interconexão interna K1-C
Gigaport 1	Slot 6 - Interconexão Gigabit 5
Gigaport 2	Slot 5 - Interconexão Gigabit 5
Gigaport 3	Slot 2 - Interconexão Gigabit 5
Gigaport 4	Slot 3 - Interconexão Gigabit 5
Gigaport 5	Slot 4 - Interconexão Gigabit 5
Gigaport 6	Slot 4 - Interconexão Gigabit 4
Gigaport 7	Slot 3 - Interconexão Gigabit 4
Gigaport 8	Slot 2 - Interconexão Gigabit 4
Gigaport 9	Slot 5 - Interconexão Gigabit 4
Gigaport 10	Slot 6 - Interconexão Gigabit 4
Gigaport 11	Interconexão interna K1-B

## K1-B (gigaports 12-23)

Gigaport 12	Interconexão interna K1-A
Gigaport 13	Slot 6 - Interconexão Gigabit 3
Gigaport 14	Slot 5 - Interconexão Gigabit 3
Gigaport 15	Slot 2 - Interconexão Gigabit 3
Gigaport 16	Slot 3 - Interconexão Gigabit 3
Gigaport 17	Slot 4 - Interconexão Gigabit 3
Gigaport 18	Slot 4 - Interconexão Gigabit 2
Gigaport 19	Slot 3 - Interconexão Gigabit 2
Gigaport 20	Slot 2 - Interconexão Gigabit 2
Gigaport 21	Slot 5 - Interconexão Gigabit 2
Gigaport 22	Slot 6 - Interconexão Gigabit 2
Gigaport 23	Interconexão interna K1-C

## K1-C (gigaports 24-35)

Gigaport 24	Interconexão interna com K1-B
Gigaport 25	Slot 6 - Interconexão Gigabit 1
Gigaport 26	Slot 5 - Interconexão Gigabit 1
Gigaport 27	Slot 2 - Interconexão Gigabit 1
Gigaport 28	Slot 3 - Interconexão Gigabit 1
Gigaport 29	Slot 4 - Interconexão Gigabit 1
Gigaport 30	Slot 4 - Interconexão Gigabit 0
Gigaport 31	Slot 3 - Interconexão Gigabit 0
Gigaport 32	Slot 2 - Interconexão Gigabit 0
Gigaport 33	Slot 5 - Interconexão Gigabit 0
Gigaport 34	Slot 6 - Interconexão Gigabit 0
Gigaport 35	Uplink 1 (Porta 1/2) ou Interconexão Interna para K1-A

Cada ASIC K1 tem interconexões de 12 gigabits. Essas interconexões gigabit são usadas entre as placas de linha e o Supervisor Engine como links seriais ponto-a-ponto. Cada placa de linha no Catalyst 4000 se conecta a 6 das interconexões de 12 gigabits. As interconexões gigabit são referenciadas de 0 a 5 e conectadas em ordem inversa. Por exemplo, em uma placa de linha 4148, a interconexão de gigabit 5 se conecta às portas 1-8, a interconexão de gigabit 4 se conecta às portas 9-16.

## Mapeamento de porta de interconexão do módulo de linha

WS-X4148-RJ, WS-X4148-RJ45V, WS-X4148-RJ21

Portas	Interconexão Gigabit
1-8	5
9-16	4
17-24	3

25-32	2
33-40	1
41-48	0

WS-X4232-RJ-32, WS-X4232-L3

Portas	Interconexão Gigabit
1	5
2	4
3-10	3
11-18	2
19-26	1
27-34	0

WS-X4418-GB

Portas	Interconexão Gigabit
1	5
2	4
3-6	3
7-10	2
11-14	1
15-18	0

WS-X4124-FX-MT

Portas	Interconexão Gigabit
1-4	5
5-8	4
9-12	3
13-16	2
17-20	1
21-24	0

WS-X4306-GB

Portas	Interconexão Gigabit
1	5
2	4
3	3
4	2
5	1
6	0

WS—X4412-2GB-TX

Portas	Interconexão Gigabit
1-2	5
3-4	4
5-6	3
7-8	2
9-10	1
11-12	0

## Exemplo de localização de portas suspeitas

```
4006-2b1> en
```

```
Enter password:
```

```
4006-2b1> (enable) sh mod
```

```
Mod Slot Ports Module-Type          Model          Sub Status
-----
1  1    2    1000BaseX Supervisor  WS-X4013      no  ok
2  2   48    10/100BaseTx Ethernet  WS-X4148      no  ok
3  3   34    Router Switch Card  WS-X4232-L3   no  ok
6  6   24    100BaseFX Ethernet  WS-X4124-FX-MT no  ok
```

```
Mod Module-Name          Serial-Num
-----
```

```
1          JAB0438020C
2          JAB0234036Q
3          JAB041705GE
6          JAB0410096R
```

```
Mod MAC-Address (es)          Hw    Fw    Sw
-----
1  00-01-96-62-cc-00 to 00-01-96-62-cf-ff 2.0    5.4 (1)    5.5 (6)
2  00-50-73-0a-30-e0 to 00-50-73-0a-31-0f 1.0
3  00-01-42-06-72-98 to 00-01-42-06-72-b9 1.0    12.0 (7)W5 ( 12.0 (7)W5 (15d)
6  00-d0-06-01-68-30 to 00-d0-06-01-68-47 1.0
```

```
4006-2b1> (enable)
```

```
2000 Aug 25 12:48:41 cet +02:00 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 16, (335 : 0 )
```

```
2000 Aug 25 12:57:42 cet +02:00 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 16, (336 : 0 )
```

Gigaport 16 refere-se ao slot 3, interconexão gigabit 3. Como o slot 3 é um WS-X4232-L3, a interconexão de gigabit 3 se refere às portas 3-10. Ao solucionar problemas dessas portas, verifique se há erros e/ou incompatibilidades duplex que usam os comandos **show port**, **show mac** e **show counters**. Também pode ser útil obter um **dump 1** e ver se há erros de hardware associados às portas. Uma referência notável na saída de dump 1 é o `cscTimeout` associado ao módulo de linha ASIC para a interconexão correspondente. O valor de `cscTimeout` deve ser **0**

[%SYS-4-P2\\_AVISO: 1/endereço MAC de Ethernet de filtragem com valor zero](#)

## Problema

O switch gera mensagens Filtering Ethernet MAC address of value zero.

## Descrição



Este exemplo mostra a saída do Syslog exibida quando este erro ocorre:

```
%SYS-4-P2_WARN: 1/Filtering Ethernet MAC address of value zero
from agent host table interface
%SYS-4-P2_WARN: 1/Filtering Ethernet MAC address of value zero
from agent host table interface
```

O switch gera a mensagem `Filtering Ethernet MAC address of value zero` syslog quando o switch recebe pacotes com um endereço MAC origem 00-00-00-00-00-00. Esse endereço MAC é um MAC de origem inválido.

The syslog message indicates that the Switch refuses to learn the invalid address. Entretanto, o switch reencaminha o tráfego originado de endereços MAC completamente nulos.

A solução alternativa é tentar identificar a estação terminal que está gerando frames com um endereço MAC de origem completamente nulo. Em geral, um destes dispositivos transmite tais frames:

- Um gerador de tráfego, como o Spirent SmartBits
- Certos tipos de servidores, tais como os servidores de balanceamento de carga IBM WebSphere
- Um roteador ou estação terminal mal configurada, tal como um dispositivo que transmite broadcasts somente com zeros
- Uma NIC defeituosa

## [%SYS-4-P2\\_AVISO: 1/crc inválido, pacote descartado, contagem = xx](#)

### Problema

O switch com o Supervisor Engine II (WS-X4013=) está gerando a mensagem mostrada nesta seção e você está enfrentando uma perda parcial ou total de conectividade de rede. The loss of connectivity may affect only a portion of the Switch ports and may include the uplink ports.

```
%SYS-4-P2_WARN: 1/Invalid crc, dropped packet, count = xx
```

### Descrição

Este exemplo mostra a saída do Syslog ou console exibida quando este erro ocorre:

```
%SYS-4-P2_WARN: 1/Invalid crc, dropped packet, count = 590073
%SYS-4-P2_WARN: 1/Invalid crc, dropped packet, count = 594688
```

Às vezes, você também vê esta mensagem:

```
%SYS-4-P2_WARN: 1/Astro(3/4) - management request timed out
```

**Nota:** Se você receber apenas a mensagem `%SYS-4-P2_WARN: 1/Astro(3/4) - management request timed out`, consulte a seção [%SYS-4-P2\\_WARN: 1/Astro\(mod/port\)](#) deste documento.

**Nota:** Você poderá experimentar problemas de conectividade de rede quando essas mensagens surgirem.

Siga estes passos de troubleshooting e capture a saída dos comandos em cada passo:

**Nota:Contate o Suporte Técnico da Cisco para obter assistência para o troubleshooting.**

1. Execute estes comandos:**show logging buffer -1023show tech-supportshow health 1dump 1**
2. Execute um destes comandos cinco vezes, em intervalos aleatórios, e observe o contador InvalidPacketBufferCrcs:**show nvramenv 1** — CatOS Software Release 6.1(1) ou posterior  
Cat4k> (enable) **show nvramenv 1**

```
PS1="rommon ! >"
?="0"
DiagBootMode="post"
MemorySize="64"
ResetCause="20"
AutobootStatus="success"
InvalidPacketBufferCrcs="82325"
```

**show env 1** — CatOS Software Release 5.5(19) ou anteriorÀ medida que repete o comando, observe se o contador InvalidPacketBufferCrcs é incrementado rapidamente por altos valores.

```
cat4k> (enable) show nvramenv 1
```

```
PS1="rommon ! >"
?="0"
DiagBootMode="post"
MemorySize="64"
ResetCause="20"
AutobootStatus="success"
InvalidPacketBufferCrcs="82763"
```

**Nota:Se você vir um pequeno número de InvalidPacketBufferCrcs na saída e estiver executando uma versão do CatOS Software anterior à 5.5.10, 6.2.3 ou 6.3.1, faça o upgrade para uma versão posterior. É possível que você tenha encontrado os bugs da Cisco IDs [CSCdu48749](#) (somente clientes [registrados](#)) e [CSCdt80707](#) (somente clientes [registrados](#)). Consulte [Field Notice: Portas do Catalyst 4000 Perdem o Estado de VLAN Ativa Resultando em Perda de Pacotes](#) para obter mais informações.**

3. Se você achar que o contador InvalidPacketBufferCrcs está sendo incrementado a uma taxa alta, execute o comando **reset** para reinicializar o switch por software.**Observação:** a captura da saída nesta etapa é crítica.

```
cat4k> (enable) reset
```

```
This command will reset the system.
Do you want to continue (y/n) [n]? y
```

```
nodcsw0nm1> (enable)
WS-X4013 bootrom version 5.4(1), built on 2000.02.17 18:28:09
H/W Revisions: Crumb: 5 Rancor: 8 Board: 2
Supervisor MAC addresses: 00:0a:8a:6d:92:00 through 00:0a:8a:6d:95:ff
(1024 addresses)
Installed memory: 64 MB
Testing LEDs... done!
The system will autoboot in 5 seconds.
Type control-C to prevent autobooting.
```

```
rommon 1 >
The system will now begin autobooting.
Autobooting image: "bootflash:cat4000-k9.6-3-9.bin"
```



Este exemplo mostra a saída do Syslog exibida quando este erro ocorre:

```
SYS-4-P2_WARN: 1/Invalid traffic from multicast source address
                81:00:01:00:00:00 on port 2/1
%SYS-4-P2_WARN: 1/Invalid traffic from multicast source address
                81:00:01:01:00:00 on port 2/1
```

O switch gera a mensagem do Syslog Invalid traffic from multicast source address ao receber pacotes com um endereço MAC de multicast como MAC de origem. A utilização de um endereço MAC de broadcast ou multicast como o MAC de origem para um frame não é um comportamento compatível com os padrões. No entanto, o switch ainda encaminhará o tráfego proveniente de um endereço MAC de multicast.

A mensagem do Syslog indica o endereço MAC de multicast no campo de MAC de origem do frame, bem como a porta em que o tráfego foi recebido.

A alternativa é tentar identificar a estação final que gera os frames com um endereço MAC de origem de multicast. Em geral, um destes dispositivos transmite tais frames:

- Um gerador de tráfego, como SmartBits
- Dispositivos de terceiros que compartilham um endereço MAC de multicast, como produtos de firewall de balanceamento de carga ou de servidores

## [%SYS-4-P2 AVISO: 1/Astro\(mod/port\)](#)

### Problema

O switch gera mensagens %SYS-4-P2\_WARN: 1/Astro(6/6)...

### Descrição

Essa mensagem de erro indica que o Supervisor Engine perdeu a comunicação com um componente ou placa de linha. O Supervisor Engine mantém o controle sobre quaisquer timeouts associados a essa comunicação. Há várias causas possíveis para essa condição. Para obter mais informações sobre essa mensagem de erro e suas possíveis causas, consulte [Compreensão e Troubleshooting de Timeout de Astro/Lemans/NiceR nos Catalyst 4000/4500 Series Switches](#)

## [%SYS-4-P2 AVISO: 1/Tag 0](#)

O switch gera mensagens %SYS-4-P2\_WARN: 1/Tag 0...

Este exemplo mostra a saída do Syslog exibida quando este erro ocorre:

```
%SYS-4-P2_WARN: 1/Tag [dec] on packet from [ether] port [chars],
                but port's native vlan is [dec]
```

Essa mensagem indica que um pacote com marca 802.1Q foi recebido em uma porta que não é de tronco. A VLAN derivada da marca do pacote é diferente da VLAN nativa da porta. Na mensagem de erro:

- Tag [dec] é o identificador da VLAN do pacote.
- [ether] é o endereço MAC do host.
- port [chars] é o identificador da porta.
- O segundo [dec] é o número da VLAN nativa.

Há uma possibilidade de que a porta local esteja configurada incorretamente como uma porta de acesso em vez de porta de tronco. Alternativamente, o lado remoto pode ter sido configurado como uma porta de tronco, em vez de porta de acesso.

Verifique se a porta local não está incorretamente configurada como porta de acesso em vez de porta de tronco. Verifique também se o lado remoto não está configurado como porta de tronco, em vez de porta de acesso.

## [convert\\_post SAC CiscoMIB:Nvram block \[#\] unconvertible](#)

### Problema

O switch gera mensagens do Syslog `convert_post_SAC_CiscoMIB:` periódicas.

### Descrição

Este exemplo mostra a saída do console que você vê quando esta mensagem ocorre:

```
convert_post_SAC_CiscoMIB:Nvram block 0 unconvertible: )
convert_post_SAC_CiscoMIB:Nvram block 1 unconvertible: )
convert_post_SAC_CiscoMIB:Nvram block 2 unconvertible: )
```

O switch gera essas mensagens de console com frequência quando você faz upgrade ou downgrade de versões do código do CatOS. O erro também pode ocorrer durante o carregamento de uma configuração de switch gerada por outro switch ou quando uma configuração de switch de outra versão de código é usada. Um failover para o Supervisor Engine em standby também pode gerá-las.

Versões diferentes de código contêm variáveis que são armazenadas em NVRAM. Quando o switch inicializa em uma versão mais recente ou mais antiga do CatOS, ele converte a configuração anterior em uma versão utilizável pela imagem de inicialização atual. Durante esse processo, um bloco de memória específico que não é necessário ou utilizável na forma atual é desalocado em vez de convertido. Essa função interna gera a mensagem de erro.

Esta mensagem é geralmente apenas informativa. Compare a configuração anterior com a atual para verificar se todas as informações de configuração foram corretamente convertidas.

Se essas mensagens surgirem sem que tenha havido nenhuma atualização de código, alteração de configuração ou failover de Supervisor Engine, [crie uma solicitação de serviço](#) (somente clientes [registrados](#)) no [Suporte Técnico da Cisco](#).

## [Global checksum failed error](#)

### [Problema](#)

Essa mensagem de erro pode surgir nos Catalyst 4000/4500 e 6000/6500 Series Switches que

executam o Catalyst OS System Software.

A mensagem de erro Global checksum failed pode se exibida na saída do comando **show version**.

```
4000-Switch> (enable) show version
WS-C4006 Software, Version NmpSW: 7.6(2)
Copyright (c) 1995-2003 by Cisco Systems, Inc.
NMP S/W compiled on Jun 25 2003, 23:00:25
GSP S/W compiled on Jun 25 2003, 17:11:56
```

```
System Bootstrap Version: 5.4(1)
```

```
Hardware Version: 3.2 Model: WS-C4006 Serial #: FOX053701JY
```

Mod	Port	Model	Serial #	Versions
1	2	WS-X4013	JAB054207A0	Hw : 3.2 Gsp: 7.6(2.0) Nmp: 7.6(2)
2	48	WS-X4148-RJ45V	JAB05410EQF	Hw : 1.6
3	48	WS-X4148-RJ45V	JAB05410ES5	Hw : 1.6
4	48	WS-X4148-RJ45V	JAB0541070L	Hw : 1.6
5	48	WS-X4148-RJ45V	JAB05410ESC	Hw : 1.6

Module	DRAM			FLASH			NVRAM		
	Total	Used	Free	Total	Used	Free	Total	Used	Free
1	65536K	40935K	24601K	16384K	10543K	5841K	480K	198K	282K

**Global checksum failed.**

Uptime is 306 days, 8 hours, 0 minute

Uma mensagem relacionada, NVRAM: F, pode ser exibida na saída do comando **show test**.

```
6000-Switch> show test 1
```

```
Diagnostic mode: complete (mode at next reset: complete)
```

```
Module 1 : 2-port 1000BaseX Supervisor
Network Management Processor (NMP) Status: (. = Pass, F = Fail, U = Unknown)
ROM: . Flash-EEPROM: . Ser-EEPROM: . NVRAM: F EOBC Comm: .
```

```
Line Card Status for Module 1 : PASS
```

```
Port Status :
Ports 1 2
-----
```

```
!--- Output is suppressed.
```

## Descrição

O erro de soma de verificação global indica que, na próxima vez que o equipamento for recarregado, a NVRAM provavelmente será perdida devido a uma falha na soma de verificação de CRC durante a leitura da configuração. Normalmente, esse não é um erro de hardware, mas o switch se corrigirá automaticamente. Isso não terá qualquer impacto em um switch operacional, a menos que sejam feitas alterações na configuração enquanto o switch estiver nessa condição.

Contudo, na maioria das vezes, uma reinicialização solucionará a falha de soma de verificação, uma vez que seu valor será recalculado. Este problema está documentado no bug da Cisco ID [CSCdx87646](#) (somente clientes [registrados](#)).

## Solução

Execute estes passos para recuperar o switch desse estado de erro:

1. Faça backup da configuração do switch. Consulte [Carregando Arquivos de Configuração em um Servidor TFTP](#) para obter mais informações sobre como fazer o backup da configuração.
2. Reinicie o módulo Supervisor executando o comando **reset** *número\_do\_módulo\_do\_supervisor*.
3. Depois que o switch for inicializado, execute os comandos **show version** e **show test** para verificar se a saída está normal.
4. Verifique a configuração existente no switch e faça a restauração a partir do backup, se necessário.

## Informações Relacionadas

- [Guia de Mensagens do Sistema Switches da Família Catalyst, 7.4](#)
- [Configurando o registro de mensagens do sistema](#)
- [Mensagens de erro comuns de CatOS em Switches da série Catalyst 5500 ou 5000](#)
- [Mensagens de erro comuns do CatOS em Switches Catalyst 6500/6000 Series](#)
- [Decodificador de Mensagens de Erro \(somente clientes registrados\)](#)
- [Páginas de Suporte de Produtos de LAN](#)
- [Página de suporte da switching de LAN](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)