

# Häufige CatOS-Fehlermeldungen bei Catalyst Switches der Serien 4500 und 4000

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Fehlermeldungen bei Catalyst Switches der Serien 4500/4000](#)

[%C4K\\_HWPORTMAN-4-BLOCKEDTXQUEUE:Gespernte Übertragungswarteschlange  
HwTxQId\[dec\]on \[char\], count=\[dec\]](#)

[%CDP-4-NVLANMISMATCH: Native VLAN-Diskrepanz auf Port \[dec\]/\[dec\] erkannt](#)

[DTP-1-ILGLCFG: Illegale Konfiguration \(on, isl - on, dot1q\) auf Port \[mod/port\]](#)

[%IP-3-UDP SOCKOVFL:UDP-Socket-Overflow](#)

[%IP-3-UDP BADCKSUM:UDP-Prüfsumme](#)

[%KERNEL-5-UNALIGNACCESS:Korrektur der Ausrichtung vorgenommen](#)

[%MCAST-4-RX\\_JNRANGE:IGMP: Rcvd Report im Bereich](#)

[MGMT-5-LOGIN\\_FAIL:Benutzer konnte sich nicht von der Konsole anmelden.](#)

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

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

[%SYS-3-P2\\_ERROR: 1/Unbekanntes Modul](#)

[%SYS-3-P2\\_ERROR: 1/Habe keine vbufs \(interne Puffer\) mehr](#)

[%SYS-3-P2\\_ERROR: Host xx:xx:xx:xx:xx:xx:xx:xx flapping zwischen Ports](#)

[%SYS-4-P2\\_WARN: 1/Gespernte Warteschlange \(tx\) am Port \[char\]](#)

[%SYS-4-P2\\_WARN: 1/Filtern Ethernet MAC-Adresse im Wert Null](#)

[%SYS-4-P2\\_WARN: 1/Ungültiger CCC, verworfenes Paket, count = xx](#)

[%SYS-4-P2\\_WARN: 1/Ungültiger Datenverkehr von Multicast-Quelladresse](#)

[%SYS-4-P2\\_WARN: 1/Astro\(Mod/Port\)](#)

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

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

[Globaler Prüfsummenfehler](#)

[Zugehörige Informationen](#)

## Einführung

Dieses Dokument enthält eine kurze Erläuterung des allgemeinen Systemprotokolls (Syslog) und der Fehlermeldungen, die auf Switches der Serien Cisco Catalyst 4500/4000 angezeigt werden, auf denen die Catalyst OS (CatOS)-Software ausgeführt wird.

Wenn Sie die Details zu einer bestimmten Fehlermeldung in diesem Dokument nicht finden, verwenden Sie das [Fehlermeldung Decoder](#) (nur [registrierte](#) Kunden) Tool. Dieses Tool zeigt die Bedeutung von Fehlermeldungen an, die von der Cisco IOS® Software und CatOS-Software generiert werden.

**Hinweis:** Das genaue Format des Syslog und der in diesem Dokument beschriebenen Fehlermeldungen kann variieren. Die Variation hängt von der Softwareversion ab, die auf der Switch Supervisor Engine ausgeführt wird.

**Hinweis:** Dies ist die empfohlene Mindestkonfiguration für die Protokollierung der Switches der Serien Catalyst 4500 und 4000:

- Legen Sie das Datum und die Uhrzeit auf dem Switch fest, oder konfigurieren Sie den Switch so, dass er das Network Time Protocol (NTP) verwendet, um das Datum und die Uhrzeit von einem NTP-Server abzurufen. **Hinweis:** Geben Sie den Befehl **set time** ein, um Datum und Uhrzeit auf dem Switch festzulegen.
- Stellen Sie sicher, dass die Protokollierung und Protokollierung der Zeitstempel aktiviert ist (Standardeinstellung).
- Konfigurieren Sie den Switch so, dass er sich möglichst bei einem Syslog-Server anmeldet.

Die Fehlermeldungen in diesem Dokument können bei Catalyst Switches der Serien 4500/4000 und bei Derivaten dieser Switches wie Catalyst Switches der Serien 2948G, 2980G und 4912G auftreten.

## [Voraussetzungen](#)

### [Anforderungen](#)

Für dieses Dokument bestehen keine speziellen Anforderungen.

### [Verwendete Komponenten](#)

Dieses Dokument ist nicht auf bestimmte Software- oder Hardwareversionen beschränkt.

### [Konventionen](#)

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

## [Fehlermeldungen bei Catalyst Switches der Serien 4500/4000](#)

### [%C4K\\_HWPORTMAN-4-BLOCKEDTXQUEUE:Gesperrte Übertragungswarteschlange HwTxQId\[dec\]on \[char\], count=\[dec\]](#)

#### **Problem**

Der Switch generiert `%C4K_HWPORTMAN-4-BLOCKEDTXQUEUE:Blocked Transmit Queue HwTxQId[dec]on[char], count=[dec]` Fehler.

## Beschreibung

Diese Meldung mit begrenzter Übertragungsrates gibt an, dass eine Übertragungswarteschlange an einem Port aus anderen Gründen als "angehalten" blockiert wird. Das heißt, der Datenverkehr an diesem Port wird begrenzt und blockiert. Sie sehen die blockierten Übermittlungswarteschlangen-Meldungen, wenn die Supervisor Engine aufgrund des Empfangs eines besetzten Bits von der Linecard keine Pakete an die Linecard senden kann. Schlechte Hardware oder eine Geschwindigkeit/Duplexungleichheit können dieses Problem verursachen. Die Problemlösung besteht darin, beide Seiten der Verbindung für die automatische Aushandlung auf Geschwindigkeit und Duplex zu konfigurieren. Geben Sie den Befehl **shut/no shutdown** ein, um den Port wiederherzustellen. Wenn das Problem weiterhin besteht, ziehen Sie das verbundene Gerät an einen anderen Anschluss, und prüfen Sie, ob das Problem dort auftritt. Führen Sie als letzte Maßnahme zum Aufheben der Blockierung der Übertragungs-(Tx-)Warteschlange den Befehl **hw-module reset** aus, um den Switch neu zu starten oder die Linecard zurückzusetzen.

## [%CDP-4-NVLANMISMATCH: Native VLAN-Diskrepanz auf Port \[dec\]/\[dec\] erkannt](#)

### Problem

Der Switch generiert häufige %CDP-4-NVLANMISMATCH-Syslog-Meldungen.

### Beschreibung

Dieses Beispiel zeigt die Konsolenausgabe, die angezeigt wird, wenn diese Fehlermeldung auf dem Switch auftritt:

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

Der Switch generiert diese Meldung, wenn der Switch-Port physisch mit einem anderen Switch oder Router verbunden ist. Der Switch generiert diese Meldung, da das konfigurierte native VLAN auf dem Port sich von dem nativen VLAN unterscheidet, das auf dem angeschlossenen Switch oder Router-Port festgelegt ist.

Ein Trunk-Port, den Sie mit IEEE 802.1Q-Tagging konfigurieren, kann getaggten und nicht getaggten Datenverkehr empfangen. Standardmäßig leitet der Switch nicht getaggten Datenverkehr mit dem für den Port konfigurierten nativen VLAN weiter. Wenn ein Paket über dieselbe VLAN-ID wie die native VLAN-ID des ausgehenden Ports verfügt, wird das Paket ohne Tags übertragen. Wenn die VLAN-IDs nicht identisch sind, überträgt der Switch das Paket mit einem Tag.

Stellen Sie sicher, dass das native VLAN für einen 802.1Q-Trunk an beiden Enden der Trunk-Verbindung identisch ist. Wenn sich das native VLAN an einem Ende des Trunks von dem nativen VLAN am anderen Ende unterscheidet, kann der Datenverkehr der nativen VLANs auf beiden Seiten nicht korrekt auf dem Trunk übertragen werden. Dieser Fehler bei der korrekten Übertragung kann zu Verbindungsproblemen in Ihrem Netzwerk führen.

Führen Sie den **Befehl show trunk mod/port** aus, um das auf dem Switch konfigurierte native VLAN zu überprüfen. In diesem Befehl ist *mod/port* der Trunk-Port. Im Folgenden finden Sie eine Beispielausgabe des Befehls:

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

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

```
Port Vlan allowed on trunk
```

```
5/24 1-1005
```

```
Port Vlan allowed and active in management domain
```

```
5/24 1
```

```
Port Vlan in spanning tree forwarding state and not pruned
```

```
5/24
```

```
Console> (enable)
```

Führen Sie den Befehl **set vlan *vlan-id* mod/port** aus, um das für den Trunk-Port konfigurierte native VLAN zu ändern. In diesem Befehl ist *mod/port* der Trunk-Port.

## [DTP-1-ILGLCFG: Illegale Konfiguration \(on, isl - on,dot1q\) auf Port \[mod/port\]](#)

### Problem

Der Switch generiert `DTP-1-ILGLCFG: Illegale Konfigurationsfehler (on, isl - on,dot1q) auf Port [mod/port]`.

### Beschreibung

Diese Meldung kann auftreten, wenn beide Seiten des Trunks auf `on` gesetzt sind, die Kapselungstypen (`isl`, `dot1q`) jedoch nicht übereinstimmen. Wenn die Trunk-Modi auf `wünschenswert` eingestellt sind, wird der Trunk aufgrund dieser Fehlkonfiguration nicht angezeigt. Überprüfen Sie zur Fehlerbehebung die Ausgabe des Befehls **show trunk** auf beiden Seiten. Stellen Sie sicher, dass die Kapselungstypen identisch sind.

## [%IP-3-UDP SOCKOVFL:UDP-Socket-Overflow](#)

### Problem

Der Switch generiert periodische `%IP-3-UDP SOCKOVFL:UDP-Socket-Überlauf-Syslog-Meldungen`.

### Beschreibung

Dieses Beispiel zeigt die Konsolenausgabe, die Sie sehen, wenn dieser Fehler auftritt:

**Hinweis:** Die angezeigte UDP-Socketnummer (User Datagram Protocol) kann unterschiedlich oder einheitlich sein.

```
%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
```

Der Switch generiert diese Syslog-Meldung, wenn der Puffer, der eingehenden Paketen auf dem angegebenen Socket (UDP-Zielport) zugewiesen wird, voll ist. Der Puffer ist voll, da die Datenverkehrsrate, die für diesen Socket bestimmt ist, zu hoch ist. Diese Bedingung kann beispielsweise auftreten, wenn eine Netzwerkmanagementstation eine große Anzahl von SNMP-Abfragen (Simple Network Management Protocol) sendet. Wenn ein UDP-Überlauf auftritt, versuchen Sie, die Anzahl der SNMP-Abfragen zu reduzieren. Führen Sie eine der folgenden Aktionen aus:

- Verlängern Sie das Abfrageintervall auf der Netzwerkmanagementstation.
- Reduzieren Sie die Anzahl der abgefragten MIB-Objekte.

Im Beispiel in diesem Abschnitt erhielt der Switch eine übermäßige Anzahl von Paketen, die für die Switch-IP-Adresse (oder die Broadcast-Adresse) mit dem Ziel-UDP-Socket 2353 bestimmt waren. Da der Eingabepuffer für diesen Socket auf dem Switch voll ist, generiert der Switch eine Syslog-Meldung. Geben Sie den Befehl **show netstat udp ein**, um die Anzahl der Zugriffe des Switches auf den Überlaufzustand anzuzeigen.

Diese Syslog-Meldungen weisen darauf hin, dass eine oder mehrere Stationen einen großen Teil des UDP-Datenverkehrs auf den angegebenen UDP-Ziel-Ports an den Switch senden. Wenn der Switch zu viele dieser Nachrichten generiert, verwenden Sie einen Netzwerkanalyst, um die Quelle des Datenverkehrs zu identifizieren und die Datenverkehrsrate zu reduzieren. Weitere Informationen finden Sie im [Konfigurationsbeispiel für Catalyst Switched Port Analyzer \(SPAN\)](#).

**Hinweis:** Machen Sie sich keine Gedanken über den `port`-Zähler ohne diesen. Dieser Zähler zeigt die Anzahl der UDP-Pakete, die der Switch empfangen hat und für nicht vorhandene Ports bestimmt waren.

## [%IP-3-UDP\\_BADCKSUM:UDP-Prüfsumme](#)

### Problem

Der Switch generiert periodische `%IP-3-UDP_SOCKOVFL:UDP-Socket-Überlauf-Syslog-Meldungen`.

### Beschreibung

Dieses Beispiel zeigt die Konsolenausgabe, die Sie sehen, wenn dieser Fehler auftritt:

**Hinweis:** Die angezeigte UDP-Socketnummer kann unterschiedlich oder einheitlich sein.

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

Der Switch generiert diese Syslog-Meldung, wenn der Switch eine fehlerhafte Prüfsumme für ein UDP-Datagramm, z. B. SNMP-Pakete, erkennt. Der UDP-Datagramm-Header enthält eine Prüfsumme, die das empfangende Netzwerkgerät prüft, um festzustellen, ob das Datagramm während der Übertragung beschädigt wurde. Wenn die empfangene Prüfsumme nicht mit dem Prüfsummenwert im Header übereinstimmt, wird das Datagramm verworfen und eine Fehlermeldung protokolliert. Geben Sie den Befehl **show netstat udp ein**, um die Anzahl der vom Switch erkannten fehlerhaften Prüfsummendatagramme anzuzeigen.

```
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
```

Diese Nachricht dient nur zu Informationszwecken. Ein Netzwerkgerät, das schädliche Pakete an den Switch sendet, verursacht diese Meldung. Verwenden Sie einen Netzwerkanalysator, um die Quelle des Datenverkehrs zu identifizieren. Weitere Informationen finden Sie im [Konfigurationsbeispiel für Catalyst Switched Port Analyzer \(SPAN\)](#).

**Hinweis:** Machen Sie sich keine Gedanken über den `port-Zähler` ohne diesen. Dieser Zähler zeigt die Anzahl der UDP-Pakete, die der Switch empfangen hat und für nicht vorhandene Ports bestimmt waren.

## [%KERNEL-5-UNALIGNACCESS:Korrektur der Ausrichtung vorgenommen](#)

### Problem

Der Switch generiert periodisch `%KERNEL-5-UNALIGNACCESS:Die Alignment-Korrektur` erstellte Syslog-Meldungen.

### Beschreibung

Dieses Beispiel zeigt die Syslog-Ausgabe, die Sie sehen, wenn dieser Fehler auftritt:

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

Diese Syslog-Meldungen weisen darauf hin, dass die Switch-CPU einen Ausrichtungsfehler erkannt und korrigiert hat, als der Switch versucht hat, auf Daten im DRAM zuzugreifen. Diese Meldungen dienen nur zu Informationszwecken. Die Meldungen weisen nicht auf ein Problem mit dem Switch hin und wirken sich nicht auf die Systemleistung aus.

In einigen Fällen sehen Sie eine übermäßige Anzahl dieser Meldungen. Diese Meldungen können beispielsweise die Protokolldatei des Syslog-Servers oder die Switch-Konsole überfluten. Wenn Sie mehr als eine Nachricht erhalten, erwägen Sie ein Upgrade der Switch-Software auf die neueste Wartungsversion für Ihren Software-Release-Train. Oder geben Sie den **Standard-Befehl `set logging level kernel 4 aus`**, um die Protokollierungsebene für die `kernel`-Einrichtung auf 4 oder niedriger zu ändern.

Wenn Sie ein Upgrade auf die neueste Maintenance-Version durchführen, diese Syslog-Meldungen jedoch immer noch erhalten, [erstellen Sie eine Serviceanfrage](#) (nur [registrierte Kunden](#)) beim [technischen Support von Cisco](#).

## [%MCAST-4-RX\\_JNRANGE:IGMP: Rcvd Report im Bereich](#)

### Problem

Auf einem Switch mit aktiviertem IGMP-Snooping (Internet Group Management Protocol) wird `%MCAST-4-RX_JNRANGE:IGMP` angezeigt: `Rcvd Bericht im Bereich 01-00-5e-00-00-xx` Fehlermeldung.

## Beschreibung

Dieses Beispiel zeigt die Syslog-Ausgabe, die Sie sehen, wenn dieser Fehler auftritt:

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

Der Rcvd-Bericht im Bereich der Syslog-Meldung dient nur zur Information. Der Switch generiert diese Meldung, wenn der Switch IGMP-Berichtspakete mit einer Multicast-MAC-Adresse empfängt, die mit 01-00-5e-00-00-xx beginnt. Dieser Layer-2-Adressbereich (L2) entspricht einem Layer-3-Multicast-Adressbereich zwischen 224.0.0.0 und 224.0.0.255. Diese Adressen sind für die Verwendung von Routing-Protokollen und anderen Low-Level-Topologieerkennung- oder Wartungsprotokollen reserviert. Beispiele für diese Protokolle sind die Gateway-Erkennung und die Berichte über Gruppenmitgliedschaften.

Verwenden Sie ein Paket-Erfassungstool, z. B. einen Sniffer, und filtern Sie nach IGMP-Nachrichten, um dieses Problem zu beheben. Darüber hinaus können Sie die Catalyst SPAN-Funktion verwenden, um Pakete von einem Port zu kopieren, von dem Sie vermuten, dass diese Nachrichten von einem Netzwerkgerät empfangen werden. Um diese Meldungen zu unterdrücken, geben Sie den Befehl **set logging level mcast 2 default ein**. Mit diesem Befehl wird die Protokollierungsebene für Multicast-Meldungen auf 2 geändert.

Verwenden Sie die Ports, die der Befehl **show multicast router** anzeigt, sowie alle Uplinks zum Netzwerkkern als SPAN-Quellports. Wenn es sich bei diesen Ports um Trunk-Ports handelt, konfigurieren Sie auch den SPAN-Zielport als Trunk-Port. Geben Sie den Befehl **show trunk ein**, um zu überprüfen, ob es sich bei den Ports um Trunk-Ports handelt.

## [MGMT-5-LOGIN\\_FAIL:Benutzer konnte sich nicht von der Konsole anmelden.](#)

### Problem

Der Switch generiert `MGMT-5-LOGIN_FAIL:Der Benutzer konnte sich aufgrund von Konsolenfehlern nicht anmelden.`

### Beschreibung

Diese Meldung kann auf ein Problem mit dem Terminalserver hinweisen, der an den Konsolenport des Switches angeschlossen ist. Wenn die Switch-Konsole mit einer asynchronen Leitung eines Terminalservers verbunden ist und Sie einen Soft Reset auf dem Switch durchführen, werden Garbage (willkürlicher Text) mehrere Minuten lang über den Bildschirm übertragen. Wenn TACACS auf dem Switch aktiviert ist, können mehrere Minuten in mehrere Tage umgewandelt werden, da TACACS den Müll Stück für Stück puffert und verarbeitet. Die Lösung besteht darin, den Befehl **no exec** auf der asynchronen Leitung auszugeben, mit der der Switch verbunden wird.

**Hinweis:** Auch nachdem Sie den Befehl **no exec** ausgegeben haben, werden die Meldungen fortgesetzt, bis der Puffer leer ist.

**Hinweis:** Wenn Sie die Fehlermeldung `%MGMT-5-LOGIN_FAIL:Benutzer konnte sich nicht über Telnet anmelden.` - Der maximale Versuch wurde erreicht, begrenzen Sie die Anzahl der Benutzer, die Telnet zum Switch nutzen dürfen.

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

## Problem

Der Switch generiert häufige Syslog-Meldungen `%PAGP-5-PORTFROMSTP` und `%PAGP-5-PORTTOSTP`.

## Beschreibung

Dieses Beispiel zeigt die Konsolenausgabe, die Sie sehen, wenn der Switch diese Syslog-Meldungen generiert:

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

Die PAgP-Protokollierung (Port Aggregation Protocol) meldet Ereignisse, die PAgP betreffen. Sie verwenden PAgP, um EtherChannel-Verbindungen zwischen Switches auszuhandeln. Der Switch generiert die Syslog-Meldung `%PAGP-5-PORTFROMSTP` bei Verlust einer Verbindung an einem Switch-Port. Der Switch generiert die Syslog-Meldung `%PAGP-5-PORTTOSTP`, wenn eine Verbindung an einem Switch-Port erkannt wird. Diese Syslog-Meldungen sind normale Informationsmeldungen, die auf das Hinzufügen oder Entfernen eines Ports aus dem Spanning Tree hinweisen.

**Hinweis:** Die Aktivierung der Weiterleitung ist nicht erforderlich, damit diese Nachrichten angezeigt werden.

Im Beispiel in diesem Abschnitt verlor der Switch zunächst die Verbindung an Port 3/3, wodurch der Port aus dem Spanning Tree entfernt wurde. Anschließend erkannte der Switch erneut die Verbindung am Port, die den Port wieder in den Spanning Tree einfügte.

Wenn Sie diese Meldungen häufig für einen bestimmten Port sehen, blinkt der Link, was bedeutet, dass der Link ständig verloren geht und wiederhergestellt wird. Untersuchen Sie die Ursache. Typische Ursachen für das Flapping von Verbindungen auf einen Switch-Port sind:

- Unstimmigkeit bei Geschwindigkeit/Duplex
- Fehlerhaftes Kabel
- Fehlerhafte Netzwerkschnittstellenkarte (NIC) oder ein anderes Problem mit der Endstation
- Fehlerhafter Switch-Port
- Andere Fehlkonfiguration

Wenn Sie diese Syslog-Meldungen unterdrücken möchten, geben Sie den Befehl **set logging level pagp 4 default** ein, um die Protokollierungsebene für die PAgP-Einrichtung auf 4 oder niedriger zu ändern. Die Standardprotokollierungsstufe für PAgP ist 5.

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

## Problem

Der Switch generiert periodische `%SPANTREE-3-PORTDEL_FAILNOTFOUND`-Syslog-Meldungen.

## Beschreibung

Dieses Beispiel zeigt die Syslog-Ausgabe, die Sie sehen, wenn dieser Fehler auftritt:



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

Diese Syslog-Meldungen weisen darauf hin, dass der PAgP versucht hat, einen Port aus dem Spanning Tree für das angegebene VLAN zu entfernen. Der Port war jedoch nicht in der Spanning Tree-Datenstruktur für dieses VLAN enthalten. In der Regel wurde der Port bereits durch einen anderen Prozess, z. B. das Dynamic Trunking Protocol (DTP), aus dem Spanning Tree entfernt.

Diese Meldungen begleiten in der Regel `%PAGP-5-PORTFROMSTP`-Nachrichten. Die Meldungen dienen Debugzwecken. Die Meldungen weisen nicht auf ein Problem mit dem Switch hin und wirken sich nicht auf die Switching-Leistung aus. Darüber hinaus werden diese Meldungen nur protokolliert, wenn Sie die standardmäßige `SPANTREE`-Einrichtungsprotokollkonfiguration geändert haben. Die Standardprotokollierungsstufe für `SPANTREE` ist 2.

In einigen Fällen sehen Sie eine übermäßige Anzahl dieser Meldungen. Diese Meldungen können beispielsweise die Switch-Konsole überfluten. Wenn Sie mehr als eine Nachricht erhalten, erwägen Sie ein Upgrade der Switch-Software auf die neueste Wartungsversion für Ihren Software-Release-Train. Spätere Softwareversionen unterdrücken diese Meldungen in den meisten Fällen.

## [%SYS-3-P2\\_ERROR: 1/Unbekanntes Modul](#)

### Problem

Der `%SYS-3-P2_FEHLER: 1/Bei der Installation eines neuen Switching-Moduls in einem Catalyst Switch der Serien 4500 und 4000 wird eine Fehlermeldung für ein unbekanntes Modul angezeigt.`

### Beschreibung

Dieses Beispiel zeigt die Konsolenausgabe, die Sie sehen, wenn dieser Fehler auftritt:

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

Der `%SYS-3-P2_FEHLER: 1/Unbekannter Modulfehler tritt auf, wenn die Software-Image-Version, die derzeit auf der Supervisor Engine ausgeführt wird, die eingesetzte Hardwarekomponente nicht unterstützt.`

Im Beispiel wird ein 1000BASE-X Server-Switching-Modul mit 18 Ports (WS-X4418) in einen Catalyst 4500/4000-Switch eingefügt, auf dem die CatOS-Softwareversion 4.4(1) ausgeführt wird. Für das WS-X4418-Modul ist eine Softwareversion von mindestens 4.5(1) erforderlich.

Die Lösung besteht darin, die Supervisor Engine-Softwareversion auf eine Softwareversion zu aktualisieren, die die Hardware unterstützt. In den [Versionshinweisen für Catalyst Switches der Serie 4500](#) finden Sie eine Liste der Mindestsoftwareversionen für jedes Modul.

## [%SYS-3-P2\\_ERROR: 1/Habe keine vbufs \(interne Puffer\) mehr](#)

### Problem

Der Switch generiert `%SYS-3-P2_FEHLER: 1/Wenn mehrere Hosts gleichzeitig oder rund um die Uhr eingeschaltet sind, sind keine vbufs-Meldungen vorhanden.`

## Beschreibung

Dieses Beispiel zeigt die Konsolenausgabe, die Sie sehen, wenn der Fehler auftritt:

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

Der %SYS-3-P2\_FEHLER: 1/Habe keine vbufs(interne Puffer) Fehler können auftreten, wenn mehrere Hosts gleichzeitig hochgefahren werden. Nach dem Einschalten der Hosts werden die Fehler nicht mehr angezeigt.

Diese Fehler führen nicht zu einer Unterbrechung der Catalyst-Fähigkeit, den Datenverkehr zu verändern. Die Nachrichten sind nur informativ.

## [%SYS-3-P2\\_ERROR: Host xx:xx:xx:xx:xx:xx flapping zwischen Ports](#)

### Problem

Der Switch generiert %SYS-3-P2\_FEHLER: Host xx:xx:xx:xx:xx:xx flapping zwischen Ports... Nachrichten, wobei xx:xx:xx:xx:xx:xx eine MAC-Adresse ist.

### Beschreibung

Dieses Beispiel zeigt die Konsolenausgabe, die Sie sehen, wenn dieser Fehler auftritt:

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

Verwenden Sie die Schritte und Richtlinien in diesem Abschnitt, um die Ursache dieser Fehlermeldung zu verstehen und zu beheben.

Die Meldung weist darauf hin, dass der Catalyst Switch der Serien 4500 und 4000 eine MAC-Adresse erhalten hat, die bereits in der Tabelle mit dem adressierbaren Speicher (CAM) auf einem anderen Port als dem ursprünglichen vorhanden ist. Dieses Verhalten tritt wiederholt über kurze Zeiträume auf, d. h. es gibt Adressflapping zwischen Ports.

Wenn die Meldung für mehrere MAC-Adressen angezeigt wird, ist das Verhalten nicht normal. Dieses Verhalten weist auf ein mögliches Netzwerkproblem hin, da die MAC-Adressen vor der standardmäßigen Alterungszeit schnell von einem Port zu einem anderen Port verschoben werden. Das Problem kann das Schleifen des Datenverkehrs im Netzwerk sein. Typische Symptome sind:

- Hohe CPU-Auslastung
- Langsamer Datenverkehr im gesamten Netzwerk
- Hohe Backplane-Nutzung auf dem Switch

Informationen zur Identifizierung und Behebung von Problemen mit Spanning Tree finden Sie unter [Spanning Tree Protocol-Probleme und zugehörige Designüberlegungen](#).

Wenn die Fehlermeldung für eine oder zwei MAC-Adressen angezeigt wird, suchen Sie diese MAC-Adressen, um die Ursache zu bestimmen. Geben Sie den Befehl **show cam mac\_addr ein**, um zu ermitteln, von wo aus diese MAC-Adressen abgerufen wurden. In diesem Befehl ist *mac\_addr* die MAC-Adresse, die der Fehler als Flapping meldet.

Nachdem Sie ermittelt haben, zwischen welchen Ports diese MAC-Adresse Flapping aufzeigt, können Sie die MAC-Adresse nachverfolgen. Stellen Sie eine Verbindung zu den zwischengeschalteten Geräten zwischen dem Catalyst 4500/4000 und dem Gerät her, das die Problem-MAC-Adresse hat. Führen Sie diese Schritte aus, bis Sie die Quelle und die Art der Verbindung dieses Geräts mit dem Netzwerk identifizieren können.

**Hinweis:** Da die MAC-Adresse zwischen zwei Ports wechselt, müssen beide Pfade nachverfolgt werden.

Dieses Beispiel zeigt, wie Sie beide Pfade verfolgen, über die diese MAC-Adresse abgerufen wurde:

**Hinweis:** Nehmen Sie an, Sie haben diese Nachricht erhalten und damit begonnen, sie zu untersuchen.

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

Gehen Sie wie folgt vor, um festzustellen, wie diese MAC-Adresse von beiden Ports empfangen wurde:

1. Betrachten Sie zuerst Port 1/2 und geben Sie den Befehl **show cam dynamic 1/2** ein. Wenn Sie die MAC-Adresse 00:50:0f:20:08:00 in der Liste der MAC-Adressen sehen, die an diesem Port gelernt wurden, stellen Sie fest, ob es sich um einen einzelnen Host handelt, der verbunden ist, oder ob es mehrere Hosts gibt, die an diesem Port registriert sind.
2. Untersuchen Sie das Gerät je nachdem, ob es einen oder mehrere Hosts gibt: Wenn ein einzelner Host (00:50:0f:20:08:00) verbunden ist, überprüfen Sie den anderen registrierten Port, und prüfen Sie, ob der Host doppelt an den Switch angeschlossen ist. In diesem Beispiel ist der andere Port Port 4/39. Wenn der Host über Verbindungen zu anderen Geräten verfügt, die letztendlich zu diesem Switch zurückkehren können, versuchen Sie, die zwischengeschalteten Geräte nachzuverfolgen. Führen Sie bei Cisco Geräten den Befehl **show cdp neighbors mod/port detail** aus. Die Ausgabe liefert Informationen über zwischengeschaltete Geräte. Hier eine Beispielausgabe:

```
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. Richten Sie eine Telnet-Sitzung mit dem Gerät ein, und folgen Sie dem Pfad der MAC-Adresse. In diesem Beispiel ist die IP-Adresse 172.16.1.1. Wiederholen Sie das Verfahren für alle MAC-Adressen, die die Fehlermeldung als Flapping meldet.
4. Erstellen Sie ein einfaches Diagramm des Quellgeräts mit dieser MAC-Adresse und der physischen Verbindungen (Catalyst 4500/4000-Ports), von denen und zu denen diese MAC-Adresse flapping. Mithilfe des Diagramms können Sie feststellen, ob es sich um einen gültigen Port und Pfad für Ihr Netzwerklayout handelt. Wenn Sie überprüfen, dass beide Ports, an denen die MAC-Adresse flapping ist, einen Pfad zu diesem Netzwerkknoten darstellen, besteht die Möglichkeit, dass ein Spanning-Tree-Fehler vorliegt. Informationen zur Isolierung und Behebung dieser Schleife finden Sie unter [Spanning Tree Protocol-Probleme und zugehörige Entwurfsüberlegungen](#). In großen Netzwerken, in denen mehrere Hosts verschiedener Anbieter miteinander verbunden sind, kann es bei der Suche nach dem Host mit nur der MAC-Adresse zu Problemen kommen. Verwenden Sie das Suchdienstprogramm für die [IEEE OUI- und Company id-Zuweisungen](#), um diese MAC-Adressen nachzuverfolgen. Diese Liste ist das Front-End der Datenbank, in der IEEE alle MAC-Adressen registriert hat, die allen Anbietern zugewiesen wurden. Geben Sie die ersten drei Oktette der MAC-Adresse in die **Suche nach:** um den Anbieter zu finden, der diesem Gerät zugeordnet ist. Die ersten drei Oktette im Beispiel sind 00:50:0f.

Dies sind andere Probleme, die dazu führen können, dass diese Meldung angezeigt wird:

- **Server NIC Redundancy Problem** - Es gibt einen Server mit zwei Netzwerkkarten, der sich falsch verhält und nicht den Standards entspricht. Der Server verwendet für beide Ports, die mit demselben Switch verbunden sind, die gleiche MAC-Adresse.
- **Hot Standby Router Protocol (HSRP)-Flapping** - Flapping mit HSRP kann dazu führen, dass diese Meldungen in der Supervisor Engine-Konsole angezeigt werden. Wenn Sie bemerken, dass die HSRP-Implementierung in Ihrem Netzwerk instabil ist, lesen Sie [Informationen zur Behebung von HSRP-Problemen in Catalyst Switch Networks](#), um das Problem zu beheben.
- **EtherChannel-Fehlkonfiguration** - Eine falsch konfigurierte EtherChannel-Verbindung kann diese Symptome ebenfalls verursachen. Wenn Ports, die die Flapping-Meldungsberichte enthalten, Mitglieder derselben Channel-Gruppe sind, überprüfen Sie Ihre EtherChannel-Konfiguration, und lesen Sie zur Fehlerbehebung die Informationen zu [EtherChannel Load Balancing und Redundanz auf Catalyst Switches](#).
- **Host reflektiert Pakete zurück ins Netzwerk** - Die Reflektion von Paketen, die von einem Host ins Netzwerk zurückgeleitet werden, kann auch Flapping verursachen. In der Regel ist die Ursache für diese Paketreflexion eine defekte NIC oder ein Ausfall der physischen Schnittstelle des Hosts, der mit dem Port verbunden ist. Wenn die Reflektion von Paketen durch den Host Ihre Wurzel ist, rufen Sie eine Sniffer-Trace ab, und untersuchen Sie den Datenverkehr, der zu und von den Ports geht, auf denen die Meldungen aufgetreten sind. Wenn ein Host Pakete reflektiert, werden in der Regel doppelte Pakete in der Ablaufverfolgung angezeigt. Die doppelten Pakete sind ein mögliches Symptom dieser Flapping der MAC-Adresse. Weitere Informationen zur Konfiguration eines Ports für die Verwendung mit einem Sniffer finden Sie unter [Konfigurieren von SPAN und RSPAN](#).
- **Software- oder Hardwarefehler:** Wenn Sie versucht haben, die Flapping-Meldung mit den Anweisungen in diesem Abschnitt zu beheben, das Problem aber dennoch feststellen, wenden Sie sich an den [technischen Support von Cisco](#). Erwähnen Sie unbedingt die Informationen, die Sie während der Ausführung der Schritte gesammelt haben, und

dokumentieren Sie diese. Diese Informationen beschleunigen und optimieren die weitere Fehlerbehebung.

## [%SYS-4-P2\\_WARN: 1/Gesperrte Warteschlange \(tx\) am Port \[char\]](#)

### Problem

Der Switch generiert blockierte Warteschlangen (tx) auf Port [char]-Nachrichten.

### Beschreibung

Dieses Beispiel zeigt die Syslog-Ausgabe, die Sie sehen, wenn der Fehler auftritt:

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

Diese Fehler weisen auf ein Hardwareproblem oder eines der folgenden Probleme hin:

- Duplex-Ungleichgewicht
- Fehlerhaftes Kabel
- Kabel Typ 1
- Fehlerhafte Ports
- Hardwareproblem eines externen angeschlossenen Geräts

Die häufigste Ursache dieser Fehler ist ein Problem mit der physischen Schicht. Das Problem führt dazu, dass ein erheblicher Teil des Datenverkehrs auf den internen K1-Gigaports gesichert wird. ASICs (Application-Specific Integrated Circuits) sind die Hauptchips, die den Switch steuern. Im Allgemeinen erhöht sich die Anzahl der blockierten Tx-Warteschlangen aufgrund eines Konfigurationsproblems oder einer beschädigten Verkabelung.

In einer normalen Umgebung kann die Tx-Warteschlange nur etwa 20 Sekunden lang blockiert werden. Eine längere Blockade weist auf ein erhebliches Problem hin. Daher wird die Anzahl der blockierten Tx-Warteschlangen erhöht, wenn die Tx-Warteschlange für den Gigaport nicht in 35 Sekunden abgelaufen ist.

Wenden Sie sich bei Bedarf an den [technischen Support von Cisco](#), um festzustellen, ob das Modul ausgetauscht werden muss. Setzen Sie zunächst das Modul wieder ein, und prüfen Sie, ob die Fehlermeldung noch vorhanden ist.

Führen Sie die folgenden Schritte aus, um die blockierte Catalyst 4000/2948G/2980G-Warteschlange auf Gigaport <Gigaport\_number> den Switch-Ports auf der Vorderseite zuzuordnen, die neu eingesetzt werden muss.

### Beispielfehlermeldungen:

```
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 )
```

Diese Fehlermeldung weist darauf hin, dass ein Konfigurationsfehler vorliegt, der

höchstwahrscheinlich auf ein Problem mit der physischen Schicht oder eine Duplexungleichheit im Zusammenhang mit Gigaport 29 zurückzuführen ist. Um herauszufinden, welche Ports sich auf Gigabit Port 29 beziehen, sehen Sie sich diese Tabellen an. Die Tabellen variieren und hängen von der Supervisor Engine ab.

## WS-X4013 Gigabit-Kirky-Port-Zuordnung

### K1-A (Gigabit-Ports 0-11)

Gigaport 0	Uplink 0 (Port 1/1) oder Internal Interconnect K1-C
Gigaport 1	Steckplatz 6 - Gigabit-Interconnect 5
Gigaport 2	Steckplatz 5 - Gigabit-Interconnect 5
Gigaport 3	Steckplatz 2 - Gigabit-Interconnect 5
Gigaport 4	Steckplatz 3 - Gigabit-Interconnect 5
Gigaport 5	Steckplatz 4 - Gigabit-Interconnect 5
Gigaport 6	Steckplatz 4 - Gigabit-Interconnect 4
Gigaport 7	Steckplatz 3 - Gigabit-Interconnect 4
Gigaport 8	Steckplatz 2 - Gigabit-Interconnect 4
Gigaport 9	Steckplatz 5 - Gigabit-Interconnect 4
Gigaport 10	Steckplatz 6 - Gigabit-Interconnect 4
Gigaport 11	Interner Interconnect K1-B

### K1-B (Gigaports 12-23)

Gigaport 12	Interner Interconnect K1-A
Gigaport 13	Steckplatz 6 - Gigabit-Interconnect 3
Gigaport 14	Steckplatz 5 - Gigabit-Interconnect 3
Gigaport 15	Steckplatz 2 - Gigabit-Interconnect 3
Gigaport 16	Steckplatz 3 - Gigabit-Interconnect 3
Gigaport 17	Steckplatz 4 - Gigabit-Interconnect 3
Gigaport 18	Steckplatz 4 - Gigabit-Interconnect 2
Gigaport 19	Steckplatz 3 - Gigabit-Interconnect 2
Gigaport 20	Steckplatz 2 - Gigabit-Interconnect 2
Gigaport 21	Steckplatz 5 - Gigabit-Interconnect 2
Gigaport 22	Steckplatz 6 - Gigabit-Interconnect 2
Gigaport 23	Interner Interconnect K1-C

### K1-C (Gigaports 24-35)

Gigaport 24	Interne Verbindung zu K1-B
Gigaport 25	Steckplatz 6 - Gigabit-Interconnect 1
Gigaport 26	Steckplatz 5 - Gigabit-Interconnect 1
Gigaport 27	Steckplatz 2 - Gigabit-Interconnect 1
Gigaport 28	Steckplatz 3 - Gigabit-Interconnect 1

Gigaport 29	Steckplatz 4 - Gigabit-Interconnect 1
Gigaport 30	Steckplatz 4 - Gigabit-Interconnect 0
Gigaport 31	Steckplatz 3 - Gigabit-Interconnect 0
Gigaport 32	Steckplatz 2 - Gigabit-Interconnect 0
Gigaport 33	Steckplatz 5 - Gigabit-Interconnect 0
Gigaport 34	Steckplatz 6 - Gigabit-Interconnect 0
Gigaport 35	Uplink 1 (Port 1/2) oder Interner Interconnect zu K1-A

Jeder K1 ASIC verfügt über 12 Gigabit-Verbindungen. Diese Gigabit-Verbindungen werden zwischen den Linecards und der Supervisor Engine als serielle Point-to-Point-Verbindungen verwendet. Jede Line Card des Catalyst 4000 ist mit 6 der 12 Gigabit-Verbindungen verbunden. Die Gigabit-Interconnects werden von 0 bis 5 referenziert und in umgekehrter Reihenfolge verbunden. Auf einer 4148-Linecard beispielsweise ist die Gigabit-Verbindung 5 mit den Ports 1-8 verbunden, die Gigabit-Verbindung 4 mit den Ports 9-16.

### Zuordnung der Line Module Interconnect-Ports

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

Ports	Gigabit-Verbindung
1 bis 8	5
9 bis 16	4
17-24	1
25-32	2
33-40	1
41-48	0

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

Ports	Gigabit-Verbindung
1	5
2	4
3 bis 10	1
11 bis 18	2
19-26	1
27-34	0

WS-X4418 GB

Ports	Gigabit-Verbindung
1	5
2	4
3-6	1
7 bis 10	2
11 bis 14	1

15 bis 18	0
-----------	---

### WS-X4124-FX-MT

Ports	Gigabit-Verbindung
1 bis 4	5
5-8	4
9 bis 12	1
13 bis 16	2
17 bis 20	1
21-24	0

### WS-X4306 GB

Ports	Gigabit-Verbindung
1	5
2	4
1	1
4	2
5	1
6	0

### WS - X4412-2GB-TX

Ports	Gigabit-Verbindung
1-2	5
3-4	4
5-6	1
7-8	2
9 bis 10	1
11 bis 12	0

### Beispiel für das Auffinden verdächtiger Ports

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

1



```
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 bezieht sich auf Steckplatz 3, Gigabit Interconnect 3. Da Steckplatz 3 ein WS-X4232-L3 ist, bezieht sich Gigabit-Interconnect 3 auf die Ports 3-10. Prüfen Sie bei der Fehlerbehebung für diese Ports, ob Fehler und/oder Duplexungleichgewichte auftreten, die den **Port** anzeigen, **MAC-** und Zählerbefehle **anzeigen**. Es kann auch nützlich sein, einen **Dump 1** abzurufen und festzustellen, ob mit Ports Hardwarefehler verbunden sind. Ein bemerkenswerter Verweis in der Ausgabe von Dump 1 ist das CSCTimeout, das dem Leitungsmodul ASIC für die entsprechende Verbindung zugeordnet ist. Der Wert von **cscTimeout** muss **0** sein.

## [%SYS-4-P2\\_WARN: 1/Filtern Ethernet MAC-Adresse im Wert Null](#)

### Problem

Der Switch generiert gefilterte Ethernet-MAC-Adresse mit Wert 0 (null) Nachrichten.

### Beschreibung

Dieses Beispiel zeigt die Syslog-Ausgabe, die Sie sehen, wenn dieser Fehler auftritt:

```
%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
```

Der Switch generiert die gefilterte Ethernet-MAC-Adresse mit dem Wert 0, syslog, wenn der Switch Pakete mit der Quell-MAC-Adresse 00-00-00-00-00-00 empfängt. Diese MAC-Adresse ist eine ungültige Quell-MAC-Adresse.

Die Syslog-Meldung weist darauf hin, dass der Switch sich weigert, die ungültige Adresse zu ermitteln. Der Switch leitet jedoch Datenverkehr weiter, der von einer reinen Nullen-MAC-Adresse stammt.

Die Problemlösung besteht darin, die Endstation zu identifizieren, die Frames mit einer rein nullen Quell-MAC-Adresse erzeugt. In der Regel überträgt eines dieser Geräte solche Frames:

- Ein Datenverkehrsgenerator, z. B. Spirent SmartBits
- Bestimmte Servertypen, z. B. IBM WebSphere-Server mit Lastenausgleich
- Ein falsch konfigurierter Router oder eine falsch konfigurierte Endstation, z. B. ein Gerät, das alle Nullen-Broadcasts überträgt
- Eine fehlerhafte Netzwerkkarte

## [%SYS-4-P2\\_WARN: 1/Ungültiger CCC, verworfenes Paket, count = xx](#)

### Problem

Der Switch mit der Supervisor Engine II (WS-X4013=) generiert die Meldung, dass dieser Abschnitt angezeigt wird und dass die Netzwerkverbindung teilweise oder vollständig unterbrochen wird. Der Verbindungsverlust kann sich nur auf einen Teil der Switch-Ports auswirken und die Uplink-Ports beinhalten.

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

### Beschreibung

Dieses Beispiel zeigt die Syslog- oder Konsolenausgabe, die Sie sehen, wenn dieser Fehler auftritt:

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

Manchmal sehen Sie auch die folgende Meldung:

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

**Hinweis:** Wenn Sie nur %SYS-4-P2\_WARN erhalten: 1/Astro(3/4) - Zeitüberschreitungsmeldung für Verwaltungsanfragen, siehe [%SYS-4-P2\\_WARN: 1/Astro\(Mod/Port\)](#) Abschnitt dieses Dokuments.

**Hinweis:** Wenn diese Meldungen angezeigt werden, können Netzwerkverbindungsprobleme auftreten.

Führen Sie die folgenden Schritte zur Fehlerbehebung durch, und erfassen Sie die Ausgabe der Befehle in jedem Schritt:

**Hinweis:** Wenden Sie sich an den [technischen Support von Cisco](#), um Hilfe bei der Fehlerbehebung zu erhalten.

1. Geben Sie folgende Befehle ein:**show logging buffer -1023Technischer Support anzeigenGesundheit anzeigen 1Speicherauszug 1**
2. Stellen Sie einen dieser Befehle fünf Mal in unregelmäßigen Abständen aus, und beobachten Sie den `InvalidPacketBufferCrcs`-Zähler:**show nvramenv 1 - CatOS-Softwareversion 6.1(1) oder höher**

```
Cat4k> (enable) show nvramenv 1
```

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

**show env 1 - CatOS-Softwareversion 5.5(19) oder frühere Version**Wenn Sie den Befehl wiederholen, stellen Sie fest, ob der `InvalidPacketBufferCrcs`-Zähler um hohe Werte schnell

zunimmt.

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

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

**Hinweis:** Wenn Sie eine kleine Anzahl von InvalidPacketBufferCrcs in der Ausgabe sehen und eine CatOS-Softwareversion ausgeführt wird, die älter als 5.5.10, 6.2.3 oder 6.3.1 ist, aktualisieren Sie auf eine neuere Version. Es besteht die Möglichkeit, dass Sie auf die Cisco Bug ID [CSCdu48749](#) (nur registrierte Kunden) und [CSCdt80707](#) (nur registrierte Kunden) gestoßen sind. Siehe [Problemhinweis: Catalyst 4000-Ports verlieren den aktiven VLAN-Status, was zu Paketverlusten führt](#) für weitere Informationen [führt](#).

3. Wenn der Zähler InvalidPacketBufferCrcs mit hoher Geschwindigkeit zunimmt, führen Sie den Befehl **reset** aus, um das Zurücksetzen des Switches einzustellen. **Hinweis:** Die Erfassung der Ausgabe in diesem Schritt ist von kritischer Bedeutung.

```
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"
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC#####
Starting Off-line Diagnostics
Mapping in TempFs
Board type is WS-X4013
DiagBootMode value is "post"
Loading diagnostics...
```

```
Power-on-self-test for Module 1: WS-X4013
Status: (. = Pass, F = Fail)
uplink port 1: .       uplink port 2: F       eobc port: .
processor: .          cpu sdram: .           eprom: .
nvram: .              flash: .             enet console port: .
switch 0 port 0: .    switch 0 port 1: .    switch 0 port 2: .
switch 0 port 3: .    switch 0 port 4: .    switch 0 port 5: .
switch 0 port 6: .    switch 0 port 7: .    switch 0 port 8: .
switch 0 port 9: .    switch 0 port 10: .   switch 0 port 11: .
switch 0 registers: . switch 0 sram: .      switch 1 port 0: .
switch 1 port 1: .    switch 1 port 2: .    switch 1 port 3: .
switch 1 port 4: .    switch 1 port 5: .    switch 1 port 6: .
switch 1 port 7: .    switch 1 port 8: .    switch 1 port 9: .
switch 1 port 10: .   switch 1 port 11: .   switch 1 registers: .
```

```

switch 1 sram: .      switch 2 port 0: F      switch 2 port 1: F
switch 2 port 2: F    switch 2 port 3: F      switch 2 port 4: F
switch 2 port 5: F    switch 2 port 6: F      switch 2 port 7: F
switch 2 port 8: F    switch 2 port 9: F      switch 2 port 10: F
switch 2 port 11: F   switch 2 registers: .    switch 2 sram: F
Module 1 Failed

```

Exiting Off-line Diagnostics

**Failed Module Bringup Process**

Use 'show test 1' to see results of tests.

*!--- Output suppressed.*

4. Wenn der Switch wieder online ist, führen Sie den Befehl **show test 1 aus**.
5. Wenn die Befehlsausgabe Diagnosefehler aufweist, schalten Sie den Switch aus und wieder ein (hartes Zurücksetzen).
6. Wenn der Switch wieder in Betrieb ist, führen Sie den Befehl **show test 1** erneut aus, und prüfen Sie, ob die Diagnostesttests für den Switch fehlgeschlagen sind.
7. Wenden Sie sich aufgrund Ihrer Beobachtung an den [technischen Support](#) von [Cisco](#): Wenn der Switch die Diagnostesttests erneut nicht bestanden hat, ist die Supervisor Engine höchstwahrscheinlich ausgefallen. Weitere Anweisungen erhalten Sie [beim technischen Support](#) von [Cisco](#). Wenn die Diagnose für das Zurücksetzen des Switches nicht fehlschlägt, wenden Sie sich an den [technischen Support](#) von [Cisco](#) mit den Informationen, die Sie in den anderen Schritten dieses Verfahrens gesammelt haben. **Hinweis:** Wenn der technische Support von Cisco während der Fehlerbehebung nicht involviert war, müssen Sie die Informationen in der Reihenfolge bereitstellen, in der sie dokumentiert wurden.

Nachdem Sie das Zurücksetzen der Festplatte durchgeführt haben, sollte die Netzwerkverbindung wiederhergestellt werden.

## [%SYS-4-P2\\_WARN: 1/Ungültiger Datenverkehr von Multicast-Quelladresse](#)

### Problem

Der Switch generiert ungültigen Datenverkehr aus Multicast-Quelladressennachrichten.

### Beschreibung

Dieses Beispiel zeigt die Syslog-Ausgabe, die Sie sehen, wenn dieser Fehler auftritt:

```

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

```

Der Switch generiert den ungültigen Datenverkehr aus der Syslog-Multicast-Quelladresse, wenn der Switch Pakete mit einer Multicast-MAC-Adresse als Quell-MAC-Adresse empfängt. Die Verwendung einer Broadcast- oder Multicast-MAC-Adresse als Quell-MAC für einen Frame ist nicht standardkonform. Der Switch leitet jedoch weiterhin Datenverkehr weiter, der von einer Multicast-MAC-Adresse stammt.

Die Syslog-Meldung gibt die Multicast-MAC-Adresse im Quell-MAC-Feld des Frames sowie den Port an, an dem der Datenverkehr empfangen wurde.

Die Problemumgehung besteht darin, die Endstation zu identifizieren, die Frames mit einer

Multicast-Quell-MAC-Adresse erzeugt. In der Regel überträgt eines dieser Geräte solche Frames:

- Ein Datenverkehrsgenerator, z. B. SmartBits
- Geräte von Drittanbietern, die eine Multicast-MAC-Adresse gemeinsam nutzen, z. B. Firewall-Lastenausgleich oder Serverprodukte

## [%SYS-4-P2\\_WARN: 1/Astro\(Mod/Port\)](#)

### Problem

Der Switch generiert `%SYS-4-P2_WARN: 1/Astro(6/6)...` Nachrichten

### Beschreibung

Diese Fehlermeldung weist darauf hin, dass die Supervisor Engine die Kommunikation mit einer Komponente auf einer Linecard verloren hat. Die Supervisor Engine überwacht alle Timeouts, die mit dieser Kommunikation verbunden sind. Es gibt viele mögliche Ursachen für diesen Zustand. Weitere Informationen zu dieser Fehlermeldung und möglichen Ursachen finden Sie unter [Understanding and Troubleshooting Astro/Lemans/NiceR Timeouts on Catalyst Switches der Serien 4000/4500](#)

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

Der Switch generiert `%SYS-4-P2_WARN: 1/Tag 0...` Nachrichten

Dieses Beispiel zeigt die Syslog-Ausgabe, die Sie sehen, wenn dieser Fehler auftritt:

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

Diese Meldung weist darauf hin, dass ein 802.1Q-getaggtes Paket auf einem Nicht-Trunk-Port empfangen wurde. Das vom Paket-Tag abgeleitete VLAN unterscheidet sich vom nativen Port-VLAN. In der Fehlermeldung:

- Das `Tag [dec]` ist die VLAN-Kennung des Pakets.
- Der `[Ether]` ist die Host-MAC-Adresse.
- Der `Port [Chars]` ist die Port-ID.
- Der zweite `[dec]` ist die native VLAN-Nummer.

Es besteht die Möglichkeit, dass der lokale Port fälschlicherweise als Access-Port anstatt als Trunk-Port konfiguriert wurde. Alternativ kann die Remote-Seite als Trunk-Port anstelle eines Access-Ports konfiguriert worden sein.

Stellen Sie sicher, dass der lokale Port nicht fälschlicherweise als Access-Port anstatt als Trunk-Port konfiguriert wurde. Stellen Sie außerdem sicher, dass die Remote-Seite nicht als Trunk-Port statt als Access-Port konfiguriert ist.

## [convert\\_post\\_SAC\\_CiscoMIB:Nvram block \[#\] nicht konvertierbar](#)

### Problem

Der Switch generiert periodisch `convert_post_SAC_CiscoMIB: Syslog-Meldungen`.

## Beschreibung

Dieses Beispiel zeigt die Konsolenausgabe, die Sie sehen, wenn diese Meldung auftritt:

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

Der Switch generiert diese Konsolenmeldungen häufig, wenn Sie CatOS-Codeversionen aktualisieren oder herabsetzen. Der Fehler kann auch auftreten, wenn Sie eine Switch-Konfiguration laden, die von einem anderen Switch generiert wird, oder wenn Sie eine Switch-Konfiguration aus einer anderen Codeversion verwenden. Ein Failover auf die Standby-Supervisor Engine kann diese Meldungen ebenfalls generieren.

Verschiedene Codeversionen enthalten Variablen, die im NVRAM gespeichert werden. Wenn der Switch anfänglich zu einer späteren oder früheren Version von CatOS startet, konvertiert der Switch die vorherige Konfiguration in eine Version, die vom aktuellen Boot-Image verwendet werden kann. Während dieses Vorgangs wird ein bestimmter Speicherblock, der nicht notwendig oder in der aktuellen Form nicht verwendbar ist, dereserviert und nicht konvertiert. Diese interne Funktion erzeugt die Fehlermeldung.

Diese Nachricht dient in der Regel nur zur Information. Vergleichen Sie die vorherige Konfiguration mit der aktuellen Konfiguration, um sicherzustellen, dass alle Konfigurationsinformationen korrekt konvertiert wurden.

Wenn diese Meldungen angezeigt werden, wenn keine Code-Upgrades, Konfigurationsänderungen oder Supervisor Engine-Ausfallsicherungen durchgeführt wurden, [erstellen Sie eine Serviceanfrage](#) (nur [registrierte](#) Kunden) beim [technischen Support von Cisco](#).

## Globaler Prüfsummenfehler

### Problem

Diese Fehlermeldung kann auf Catalyst Switches der Serien 4000/4500 und 6000/6500 angezeigt werden, auf denen die Catalyst OS-Systemsoftware ausgeführt wird.

Die Fehlermeldung `Globale Prüfsumme fehlgeschlagen` kann in der Ausgabe des Befehls `show version` angezeigt werden.

```
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

Eine verwandte Meldung, NVRAM: F, kann in der Ausgabe des Befehls **show test** angezeigt werden.

```
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.*

## Beschreibung

Der globale Prüfsummenfehler bedeutet, dass der NVRAM beim nächsten erneuten Laden des Felds höchstwahrscheinlich aufgrund einer CRC-Prüfsumme verloren geht, die beim Lesen der Konfiguration fehlschlug. Dies ist normalerweise kein Hardwarefehler, aber der Switch korrigiert sich selbst. Dies hat keine Auswirkungen auf einen betrieblichen Switch, es sei denn, es werden Konfigurationsänderungen vorgenommen, während sich der Switch in diesem Zustand befindet. Meistens löst ein Zurücksetzen jedoch den Ausfall der Prüfsumme, wenn diese neu berechnet wird. Dieses Problem ist in der Cisco Bug-ID [CSCdx87646](#) dokumentiert (nur [registrierte](#) Kunden).

## Lösung

Führen Sie die folgenden Schritte aus, um den Switch aus diesem Fehlerstatus wiederherzustellen:

1. Sichern Sie die Konfiguration des Switches. Weitere Informationen zur [Sicherung der Konfiguration](#) finden Sie unter [Hochladen von Konfigurationsdateien auf einen TFTP-Server](#).
2. Setzen Sie das Supervisor-Modul zurück, indem Sie den Befehl **reset supervisor\_module\_#** eingeben.
3. Sobald der Switch hochgefahren ist, führen Sie die **show version** aus und zeigen Testbefehle

an, um zu überprüfen, ob die Ausgabe normal ist.

4. Überprüfen Sie die auf dem Switch vorhandene Konfiguration, und stellen Sie ggf. die Sicherung wieder her.

## Zugehörige Informationen

- [Catalyst-Switches der System Message Guide, 7.4](#)
- [Konfigurieren der Protokollierung von Systemmeldungen](#)
- [Häufige CatOS-Fehlermeldungen bei Catalyst Switches der Serien 5000 und 5500](#)
- [Häufige CatOS-Fehlermeldungen bei Catalyst Switches der Serien 6500 und 6000](#)
- [Fehlermeldung Decoder \(nur registrierte Kunden\)](#)
- [Support-Seiten für LAN-Produkte](#)
- [Support-Seite für LAN-Switching](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)